Declaración de Prácticas de Certificación

Servicios de confianza

Evicertia
Marzo de 2023

Público

Índice

1 Introducción

1.1 Presentación

Este documento declara las prácticas de certificación para los servicios de confianza de Evicertia, S.L., en lo sucesivo Evicertia.

1.2 Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Certificación de los servicios de confianza de Evicertia" en lo sucesivo "DPC".

1.3 Participantes en los servicios de certificación

1.3.1 Prestador de servicios de certificación

El Prestador de Servicios Electrónicos de Certificación, en adelante "PSC" es la persona, física o jurídica, que presta uno o más servicios de confianza.

Evicertia es un prestador de servicios electrónicos de confianza, 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.

1.3.2 Autoridad de registro

La Autoridad de Registro, en adelante "RA" (del término en inglés Registry Authority), son las personas físicas o jurídicas a las que Evicertia encomienda la identificación y verificación de la identidad de los suscriptores de los servicios de confianza.

Podrán actuar como RA de Evicertia.

- La propia matriz de Evicertia.
- Cualquier entidad autorizada por Evicertia.

Para poder actuar como RA será necesario formalizar contractualmente la relación existente entre Evicertia y la entidad autorizada.

Entre las funciones de estas RA, que actúan por cuenta de Evicertia se encuentran:

- La comprobación de la identidad del suscriptor validando entre otras las circunstancias personales de la persona que conste como firmante del contrato.
- Verificar la información suministrada por el suscriptor en la formalización del contrato de prestación de servicios.
- Custodiar dicha información relativa a la identificación y suscripción del interesado con referencia los servicios de confianza de Evicertia.
- Hacer entrega de la información necesaria para poder utilizar los servicios de confianza como pueden ser certificados, procedimientos para activar las cuentas de uso, ...

1.3.3 Autoridad de sellado de tiempo

La autoridad de sellado de tiempo, en lo sucesivo "TSA" (del término en inglés Time-Stamp Authority), es el tercero de confianza que presta el servicio de expedición de sellos de tiempo electrónicos cualificados.

Evicertia es el prestador de servicios de TSA cualificada que actúa como autoridad de sellado tiempo para la expedición de sellos de tiempo electrónicos cualificados.

1.3.4 Autoridad de entrega cualificada

La autoridad de entrega cualificada, en lo sucesivo "AEC", es el tercero de confianza que presta el servicio de entrega cualificada "QERDS" (del término en inglés *Qualified Electronic Registered Delivery Services*).

Evicertia es el prestador de servicios de entrega cualificada que actúa como autoridad de entrega para mensajes cuya entrega sea cualificada.

1.3.5 Suscriptores del servicio de certificación

Los suscriptores son los usuarios finales de los servicios de confianza operados por Evicertia. Los suscriptores del servicio pueden ser:

- 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.
- Las personas físicas que solicitan el servicio para sí mismas.

El suscriptor de los servicios electrónicos de confianza son, por tanto, los clientes del PSC.

1.3.6 Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben certificados, firmas electrónicas, sellos de tiempo, mensajes cuya entrega será cualificada o cualquier otro de los servicios de confianza del PSC.

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

1.3.7 Emisor y receptor

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

1.4 Uso de los servicios de confianza

La información sobre los usos permitidos y los límites y prohibiciones se indica en la declaración de prácticas y política de cada perfil de certificados, o de los servicios de confianza

1.5 Administración de la política

1.5.1 Organización que administra el documento

Los datos de la sociedad son los siguiente:

- Evicertia, S.L. (Evicertia)
- NIF: ESB86021839
- Registro Mercantil de Madrid Tomo: 28127, Libro: 0, Folio 11, Sección 8, Hoja M-506734, Inscripción 1.

1.5.2 Datos de contacto de la organización

Los datos de contacto de Evicertia, S.L., son los siguientes:

- Web: https://www.evicertia.com
- Email: info@evicertia.com
- Teléfono: +34914237080
- Fax: +34911410144
- Domicilio postal: c/ Lagasca, 95. 28006, Madrid

1.5.3 Procedimientos de gestión del documento

El sistema documental y de organización de Evicertia garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

2 Control de versiones

Ver.	Fecha	Observaciones
1.0	12/05/2021	Se aprueba la primera versión de este documento.
1.1	04/04/2022	• Se adecua la plantilla del documento y los logos. • Pequeñas correcciones gramaticales o lingüísticas en el documento.
1.2	13/03/2023	• Pequeñas correcciones gramaticales o lingüísticas en el documento.

3 Publicación y preservación

3.1 Depósito

Evicertia dispone de un Depósito, en el que se publican las informaciones relativas al servicio de confianza. El depósito de publicación se puede consultar en https://www.evicertia.com/.

Dicho servicio 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.

3.2 Publicación de información del prestador de servicios de certificación

Evicertia publicará las siguientes informaciones, en su depósito:

- La Declaración de Prácticas de Certificación (DPC).
- La declaración de prácticas y política de cada perfil de certificados, o de los servicios de confianza.
- Las listas de certificados revocados.
- Los textos de divulgación, en lo sucesivo "TD" (del término en inglés *Policy Disclosure Statements*) correspondientes.
- Las claves públicas de los certificados de sello de tiempo electrónico.
- Las claves públicas de los certificados utilizados para la entrega cualificada.

3.3 Frecuencia de publicación

La información del PSC, incluyendo la DPC, se publica en cuanto se encuentra disponible.

Los cambios en la DPC cualificada se rigen por lo establecido en el procedimiento de gestión de este documento y de acuerdo a la normativa de aplicación.

3.4 Control de acceso

Evicertia no limita el acceso de lectura a las informaciones establecidas en la sección "Publicación de información del prestador de servicios de certificación", pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información.

Evicertia emplea sistemas fiables para el depósito, de modo tal que:

- Únicamente las personas autorizadas pueden hacer anotaciones y modificaciones.
- Puede comprobarse la autenticidad de la información.
- Puede detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

4 Identificación y autenticación

La información sobre la identificación y autenticación de cada perfil de certificados o de los servicios de confianza de Evicertia se indica en su correspondiente declaración de prácticas y política de cada perfil de certificados, o de los servicios de confianza

5 Requisitos operacionales

La información sobre los requisitos operacionales se indica en la declaración de prácticas y política de cada perfil de certificados, o de los servicios de confianza

6 Controles de seguridad física, de gestión y de operaciones

6.1 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, los propios sistemas y los equipamientos empleados para las operaciones para la prestación de los servicios electrónicos de confianza.

En concreto, la política de seguridad de Evicertia aplicable a los servicios electrónicos de confianza 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 prestan los servicios electrónicos de confianza, 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.

6.2 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.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos principal cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

Evicertia dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

6.2.1 Acceso físico

Evicertia dispone de tres niveles de seguridad física en el CPD principal (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 llevan a cabo procesos de certificación 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 del mismo.
- 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.

6.2.2 Electricidad y aire acondicionado

Las instalaciones del CPD principal 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.

6.2.3 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.

6.2.4 Prevención y protección de incendios

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

6.2.5 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 Centro de Proceso de Datos principal.

6.2.6 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.

6.2.7 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 Centro de Proceso de Datos principal.

6.3 Controles de procedimientos

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 sus servicios.

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

6.3.1 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 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 Sistemas**: 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.

6.3.2 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.

6.3.3 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.

6.4 Controles de personal

6.4.1 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.

6.4.2 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, reflejada en el Reglamento Europeo nº 2016/679 General de Protección de Datos y en general cualquier normativa nacional que resulte de aplicación.

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.

6.4.3 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 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.

6.4.4 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.

6.4.5 Secuencia y frecuencia de rotación laboral

N/A

6.4.6 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.

6.4.7 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 Declaración de Prácticas de Certificación, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la Prestador de Servicios de Confianza será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto a Evicertia.

6.4.8 Suministro de documentación al personal

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

6.5 Procedimientos de auditoría de seguridad

6.5.1 Tipos de eventos registrados

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

- 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 a los servicios de confianza a través de la red.
- 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 de los servicios de confianza.
- Cambios en los detalles de los servicios de confianza 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.

6.5.2 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.

6.5.3 Período de conservación de registros de auditoría

Evicertia almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

6.5.4 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.

6.5.5 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.

6.5.6 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.

6.5.7 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.

6.5.8 Análisis de vulnerabilidades

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.

6.6 Archivos de informaciones

6.6.1 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.

6.6.2 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.

6.6.3 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.

6.6.4 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.

6.6.5 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.

6.6.6 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.

6.7 Renovación de claves

Las claves y certificados de los servicios de confianza están únicamente asociadas con el sistema que presta dicho servicio. Con anterioridad al uso de las claves privadas de los servicios de confianza, se realizará un cambio de claves o revocación de las actuales.

6.8 Compromiso de claves y recuperación de desastre

6.8.1 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.

6.8.2 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.

6.8.3 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.

6.8.4 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.

6.9 Terminación del servicio

Evicertia asegura que las posibles interrupciones a los suscriptores de los servicios y a terceras partes son 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 Declaración de Prácticas de Certificación.

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

Antes de terminar sus servicios, Evicertia desarrolla 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 Suscriptores del servicio, Tercero que confían y en general cualquier tercero 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 de los servicios de confianza.
- 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 al Órgano Supervisor Español correspondiente, 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.

7 Controles de seguridad técnica

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.

7.1 Generación e instalación del par de claves

La información sobre la generación e instalación del par de claves de cada perfil de certificados o de los servicios de confianza de Evicertia se indica en su correspondiente declaración de prácticas y política de cada perfil de certificados, o de los servicios de confianza

7.2 Protección de las claves privadas

7.2.1 Estándares de módulos criptográficos

Los módulos que gestionan claves de Evicertia cumplen con la certificación *Common Criteria EAL4+* o equivalente.

7.2.2 Control sobre las claves privada

La gestión de acceso a las claves privadas de los certificados de los servicios de confianza se realiza según los controles establecidos por el HSM donde se custodian. Asimismo, los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

7.2.3 Copia de respaldo de las claves privada

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 las mismas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

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

7.2.4 Introducción de las claves privadas en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción de Evicertia donde se almacenan cifradas.

7.2.5 Método de activación de las claves privada

Las claves privadas de Evicertia se activan mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico.

7.2.6 Método de desactivación de las claves privada

Para la desactivación de las claves privadas de Evicertia se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

7.2.7 Método de destrucción de las claves privada

Para la destrucción de las claves privadas se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

Con anterioridad a la destrucción de las claves, se emitirá una 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.

7.3 Controles de seguridad informática

Evicertia emplea sistemas fiables para ofrecer sus servicios de certificación. Evicertia ha realizado controles y auditorías informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, Evicertia aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de Evicertia, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Requerimientos de tráfico de red.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

7.4 Controles técnicos del ciclo de vida

7.4.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e 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.

7.4.2 Controles de gestión de seguridad

Evicertia desarrolla actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

Evicertia exige medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios electrónicos de confianza.

7.4.2.1 Clasificación y gestión de información y bienes

Evicertia mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de Evicertia detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, USO INTERNO y CONFIDENCIAL.

7.4.2.2 Operaciones de gestión

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.

7.4.2.3 Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

7.4.2.4 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.

7.4.2.5 Reportes de incidencias y respuesta

Evicertia dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación del proceso de resolución de la incidencia.

7.4.2.6 Procedimientos operacionales y responsabilidades

Evicertia define actividades, asignadas a personas con un rol de confianza, distintas de las actividades asignadas a personas que no tienen ese rol. Dichas actividades no tienen carácter confidencial.

7.4.2.7 Gestión del sistema de acceso

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.

7.4.2.8 Gestión del ciclo de vida del hardware criptográfico

Evicertia asegura que el hardware criptográfico usado para la firma de certificados o los servicios de confianza no se manipula durante su transporte mediante la inspección del material entregado.

En particular:

- El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.
- Evicertia registra toda la información pertinente del dispositivo para añadir al catálogo de activos.
- El uso del hardware criptográfico requiere de al menos dos empleados de confianza.
- Evicertia realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.
- El dispositivo hardware criptográfico solo es manipulado por personal confiable.
- Las claves privadas de los certificados de Evicertia almacenadas en el hardware criptográfico se eliminarán una vez se haya retirado el dispositivo.
- La configuración del sistema de Evicertia, así como sus modificaciones y actualizaciones son documentadas y controladas.
- Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

7.5 Controles de seguridad de red

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.

7.6 Controles de ingeniería de módulos criptográficos

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a la que están destinados.

Todas las operaciones criptográficas de Evicertia son realizadas en módulos con las certificación *Common Criterial 4 EAL+* o equivalentes.

7.7 Fuentes de Tiempo

El servicio de sellado cualificado de tiempo de Evicertia se basa en el uso del protocolo TSP (*Time-Stamp Protocol*) sobre HTTP, definido en la norma RFC 3161 "*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*".

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, como pueden ser el Real Observatorio de la Armada, RedIris o los *pooles* de servidores de tiempo del proyecto NTP (http://www.ntp.org/).

8 Perfiles de certificados y revocación de los mismos

La información sobre los perfiles de los certificados emitidos o utilizados por Evicertia se indica en su correspondiente declaración de prácticas y política de cada perfil de certificados, o de los servicios de confianza.

9 Auditoría de conformidad

Evicertia ha comunicado el inicio de su actividad como prestador de servicios de certificación por el Órgano Supervisor Nacional, y se encuentra sometida a las revisiones de control que este organismo considere necesarias.

9.1 Frecuencia de la auditoría de conformidad

Evicertia lleva a cabo una auditoría de conformidad anualmente, 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.

9.2 Identificación y calificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

9.2.1 Relación del auditor con la entidad auditada

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con Evicertia.

9.3 Listado de elementos objeto de auditoría

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 Declaración de Prácticas de Certificación y otra documentación vinculada con la emisión de los distintos certificados digitales.
- Que la Declaración de Prácticas de Certificación y demás documentación jurídica vinculada, se ajusta a lo acordado por Evicertia y con lo establecido en la normativa vigente.
- Que la entidad gestiona de forma adecuada sus sistemas de información

9.4 Acciones a emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta las medidas correctivas que solucionen dichas deficiencias.

Si Evicertia es incapaz de desarrollar y/o ejecutar las medidas correctivas o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Dirección de Evicertia que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Solicitar la revocación de las claves de los certificados de los servicios de confianza y regenerar la infraestructura.
- Terminar el servicio de confianza afectado,
- Otras acciones complementarias que resulten necesarias.

9.5 Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Seguridad de Evicertia en un plazo máximo de 15 días tras la ejecución de la auditoría.

10 Requisitos comerciales y legales

10.1 Tarifas

10.1.1 Tarifa de los servicios de confianza

Evicertia puede establecer una tarifa por el uso de sus servicios de confianza, de la que, en su caso, se informará oportunamente a los suscriptores.

10.1.2 Política de reintegro

Sin estipulación.

10.2 Capacidad financiera

Evicertia dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI EN 319 401-1 7.12 c), en relación a la gestión de la finalización de los servicios y plan de cese.

10.2.1 Cobertura de seguro

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.

10.2.2 Otros activos

Sin estipulación.

10.2.3 Cobertura de seguro para suscriptores y terceros que confían en los servicio de confianza

Evicertia dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, para los servicios electrónicos de confianza, con un mínimo asegurado de 3.000.000 €.

10.3 Confidencialidad

10.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por Evicertia:

- Las solicitudes del servicio, así como toda otra información personal obtenida para la prestación del mismo, excepto las informaciones indicadas en la sección siguiente.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa.
- Planes de continuidad de negocio y de emergencia.
- Planes de seguridad.
- Documentación de operaciones, archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

10.3.2 Divulgación legal de información

Evicertia no divulgará la información confidencial excepto en los casos legalmente previstos.

10.4 Protección de datos personales

Evicertia garantiza el cumplimiento de la normativa vigente en materia de protección de datos personales, reflejada en el Reglamento Europeo 2016/679 General de Protección de Datos y en general cualquier normativa nacional que resulte de aplicación.

En cumplimiento de la misma, Evicertia ha documentado en esta Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad y organizativos, con el fin de garantizar que todos los datos personales a los que tenga acceso son protegidos ante su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado.

A continuación, se detalla toda la información necesaria con respecto al tratamiento de datos personales realizado por Evicertia:

10.4.1 Responsable del tratamiento

El Responsable del tratamiento de datos de carácter personal va a ser:

- Evicertia, S.L. (Evicertia)
- NIF: ESB86021839
- Registro Mercantil de Madrid Tomo: 28127, Libro: 0, Folio 11, Sección 8, Hoja M-506734, Inscripción 1.

10.4.2 Datos de contacto de la organización

Los datos de contacto del delegado de protección de datos son:

- https://support.evicertia.com (principal)
- Email: support+gdpr@evicertia.com
- Domicilio postal: c/ Lagasca, 95. 28006, Madrid. ESPAÑA.
- Teléfono: 914237080
- Fax: 911410144

10.4.3 Finalidades del tratamiento

Evicertia tiene el deber de informar a los usuarios, que todos sus datos de carácter personal facilitados se tratan para las siguientes finalidades:

- **Prestación de Servicios Electrónicos de Confianza**. Los datos son recabados mediante el contrato oportuno y son tratados con la finalidad de llevar a cabo los servicios electrónicos solicitados y contratados por los usuarios, todo ello en base a lo establecido en la presente Declaración de Prácticas de Certificación de Sellado de Tiempo.
- **Soporte para la prestación de los servicios**. Mantenimiento de datos de contacto para facilitar la gestión de peticiones e incidencias relacionadas con la prestación de los Servicios. Por ejemplo, el CLIENTE o directamente el Usuario, puede facilitar sus datos de contacto, para intentar resolver una incidencia relacionada con problemas en los servicios ofertados por Evicertia.
- **Relación mercantil**. Mantenimiento de datos de contacto de empleados del CLIENTE para facilitar la gestión comercial, facturación, seguimiento y gestión de los Servicios.

Evicertia informa que los datos personales facilitados únicamente se tratarán para las finalidades anteriormente descritas y no serán tratados de manera incompatible con las mismas.

10.4.4 Legitimación del tratamiento

De acuerdo con las finalidades de tratamiento indicadas, la base legal para el tratamiento de los datos personales de los usuarios es:

- La legitimación del tratamiento para la Prestación de Servicios Electrónicos de Confianza es la ejecución del contrato de los servicios solicitados, donde el usuario es parte del mismo, el cual presta expresa e inequívocamente, mediante acción positiva y previa al uso del servicio, al aceptar las condiciones y la política de privacidad.
- La legitimación del tratamiento para atender las consultas y solicitudes se basa en el interés legítimo, por ejemplo, para atender al destinatario de una comunicación o para validar un documento firmado, resultado de la prestación de los servicios.

El consentimiento para el tratamiento puede ser retirado en cualquier momento mediante una solicitud en https://support.evicertia.com o por correo electrónico a la dirección email especificada en el apartado Datos de contacto de la organización.

El usuario garantiza que los datos aportados son verdaderos, exactos, completos y actualizados, siendo responsable de cualquier daño o perjuicio, directo o indirecto, que pudiera ocasionarse como consecuencia del incumplimiento de tal obligación.

10.4.5 Datos tratados y conservación

Las categorías de datos personales tratados por Evicertia, a título enunciativo pero no limitativo, comprenden datos identificativos (nombre, apellidos y los propios de identidad) y datos de contacto (dirección postal, correo electrónico y teléfono), y algún dato adicional como la dirección IP.

Los datos personales se conservarán mientras sean necesarios para dar respuesta a las consultas y solicitudes, hasta la finalización de la relación contractual y posteriormente, durante los plazos legalmente exigidos acorde a cada caso, tal y como se encuentran definidos en la presente Declaración de Prácticas de Certificación. En caso de imperativo legal, ésta permanecerá bloqueada, exclusivamente a disposición de jueces y tribunales, los periodos de tiempo legalmente establecidos.

10.4.6 Cesión y transferencia internacional de datos

Los datos personales no se divulgan ni se ceden a terceros salvo:

- Obligación legal
- Interés legítimo sobre los datos, como puede ser, el destinatario de las comunicaciones o los firmantes de los documentos, objeto de los Servicios Electrónicos de Confianza, que contengan dichos datos
- Para atender un requerimiento judicial o de cualquier autoridad administrativa competente que así lo requiera
- Terminación de los servicios

No se realizarán transferencias internacionales fuera de la Unión Europea o del Espacio Económico Europeo (EEE).

10.4.7 Derechos de los usuarios

- **Confirmación**. Todos los usuarios tienen derecho a obtener confirmación sobre si Evicertia está tratando datos personales que les concierne.

- **Acceso y rectificación**. Los usuarios tienen derecho a acceder a todos sus datos personales, así como solicitar la rectificación de aquellos que sean inexactos o erróneos.
- Supresión / cancelación. Los usuarios podrán solicitar la supresión/cancelación de los datos cuando, entre otros motivos, éstos no sean necesarios para los fines para los que fueron recogidos.
- **Limitación y oposición**. El usuario podrá solicitar la limitación del tratamiento para que sus datos personales no se apliquen en las operaciones que correspondan. En determinadas circunstancias y por motivos relacionados con su situación particular, el usuario podrá oponerse al tratamiento de datos, estando Evicertia obligada a dejar de tratarlos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.
- **Portabilidad**. Los interesados podrán solicitar que sus datos personales les sean enviados o bien se transmitan a otro responsable, en un formato electrónico estructurado y de uso habitual.

Para ejercer sus derechos, los usuarios pueden realizar una solicitud en https://support.evicertia.com o por escrito mediante correo electrónico o carta postal a la dirección contacto especificada en el apartado **Datos de contacto de la organización**. En dicha petición, deberán adjuntar copia de su documento de identidad e indicar claramente cuál es el derecho que se desea ejercer.

10.5 Derechos de propiedad intelectual

Evicertia goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

10.6 Obligaciones y responsabilidad civil

10.6.1 Obligaciones de Evicertia

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

Evicertia presta los servicios electrónicos de confianza conforme con esta Declaración de Prácticas de Certificación.

Evicertia informa al suscriptor de los términos y condiciones relativos a la prestación del servicio de confianza, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor que incorpora por referencia los textos de divulgación (TD) del servicio.

El documento de texto de divulgación, también denominado TD, cumple con lo indicado en las normas ETSI correspondientes, documento el cual puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

Evicertia vincula a los suscriptores y terceros que confían en certificados, mediante dicho texto de divulgación o TD, 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 servicios de confianza.
- Información sobre cómo validar un sello de tiempo, 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 el certificado.

- 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 Prestador de Servicios de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.

10.6.2 Obligaciones de terceros en el soporte de servicios al PSC

Las obligaciones de terceros en el soporte de los servicios que ofrece el PSC deben proporcionar, en líneas generales, las siguientes garantías:

- Cumplir y facilitar el cumplimiento de todo lo estipulado en esta DPC y en las políticas de certificación del PSC.
- Los servicios cuya infraestructura esté desplegada en terceros deben ofrecer los mismos niveles de seguridad y fiabilidad como si estuvieran desplegados en las infraestructuras del PSC.
- El tercero deberá conocer y seguir lo establecido en esta DPC y en las políticas de certificación, siendo de obligado cumplimiento como si del propio PSC se tratara.
- En el caso en el que el tercero, además, tenga que archivar información y datos, lo hará en las mismas condiciones y plazos que marcan la DPC y las políticas de certificación.
- El tercero deberá informar al PSC de cualquier cambio que se vaya a llevar en la infraestructura o en los procedimientos con el fin de someterlo a evaluación por parte del PSC. En cualquier caso, dichos cambios deberán garantizar lo estipulado en esta DPC y en las políticas de certificación.

10.6.3 Obligaciones de los suscriptores

Las obligaciones de los suscriptores con respecto a los servicios de confianza de Evicertia son:

- Respetar lo dispuesto en esta DPC, así como en las prácticas y políticas de Evicertia.
- Formalizar un contrato de prestación de servicios de confianza con Evicertia.
- Utilizar los servicios de confianza de Evicertia de acuerdo con los procedimientos y, si es necesario, los componentes técnicos suministrados por Evicertia, de conformidad con lo que se establece en la Declaración de Prácticas de Certificación (en adelante DPC) y en la documentación de Evicertia.
- Verificar las firmas electrónicas y los sellos de tiempos electrónicos, incluyendo la validez del certificado usado en los diferentes servicios de confianza de Evicertia.
- Notificar cualquier incidente o hecho que afecte a los servicios de confianza de Evicertia.

10.6.4 Garantías ofrecidas a suscriptores y terceros que confían

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 servicios de confianza cumplen con todos los requisitos materiales establecidos en esta Declaración de Prácticas de Certificación, así como las normas de referencia.

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

10.6.5 Rechazo de otras garantías

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

10.6.6 Limitación de responsabilidades

Evicertia limita su responsabilidad a la prestación de los servicios de confianza, 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 servicios de confianza.

10.6.7 Caso fortuito y fuerza mayor

Evicertia incluye en el texto de divulgación o TD, cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

10.6.8 Jurisdicción aplicable

Evicertia establece, en el contrato con el suscriptor y/o en el texto de divulgación o TD, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley española.

10.6.9 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

Evicertia establece, en el contrato de suscriptor, y/o en el texto de divulgación o TD, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones **Obligaciones y responsabilidad**, **Auditoría de conformidad** y **Confidencialidad,** continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

10.6.10 Cláusula de jurisdicción competente

Evicertia establece, en el contrato de suscriptor y en el texto de divulgación o TD, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

10.6.11 Resolución de conflictos

Evicertia establece, en el contrato de suscriptor, y en el texto de divulgación o TD, los procedimientos de mediación y resolución de conflictos aplicables.

11 Anexo I - Acrónimos

A continuación se muestran los acrónimos utilizados en la presente Declaración de Prácticas de Certificación.

- AC: Autoridad de Certificación. También se puede utilizar CA (Certification Authority).
- CN: Common Name
- CP: Certificate Policy
- CPD: Centro de Procesamiento de Datos
- CSR: Certificate Signing Request. Petición de firma de certificado
- DCCF: Dispositivo Cualificado de Creación de Firma. También se puede utilizar QSCD: (Qualified Signature Creation Device).
- DES: Data Encryption Standard. Estándar de cifrado de datos
- DN: Distinguished Name. Nombre distintivo dentro del certificado digital
- DPC: Declaración de Prácticas de Certificación. También se puede utilizar CPS (Certification Practice Statement).
- DPPSEC: Declaración de Prácticas y Políticas del Servicio de Entrega Cualificada
- DPPSST: Declaración de Prácticas y Políticas del Servicio de Sellado de Tiempo
- DSA: Digital Signature Algorithm. Estándar de algoritmo de firma
- ETSI: European Telecommunications Standards Institute o Instituto Europeo de Normas de Telecomunicaciones
- FIPS: Federal Information Processing Standard Publication.
- ISO: International Organization for Standardization. Organismo Internacional de Estandarización
- LDAP: Lightweight Directory Access Protocol. Protocolo de acceso a directorios
- LRC: Listas de Revocación de Certificados. También se puede utilizar CRL (Certificate Revocation List).
- NTP: Network Time Protocol
- OCSP: On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
- OID: Object Identifier. Identificador de objeto
- PA: Policy Authority. Autoridad de Políticas
- PC: Política de Certificación
- PIN: Personal Identification Number. Número de identificación personal
- PKCS: Public-Key Cryptography Standards
- PKI: Public Key Infrastructure. Infraestructura de clave pública

- PSC: Prestador de Servicios Electrónicos de Certificación / Confianza
- QERDS: Qualified Electronic Registered Delivery Services)
- RA: Autoridad de Registro.
- RSA: Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
- SHA: Secure Hash Algorithm. Algoritmo seguro de Hash
- SSL: Secure Sockets Layer
- TCP/IP: Transmission Control. Protocol/Internet Protocol
- TD: Texto de divulgación. También se puede utilizar su término en inglés PDS o Practice Disclosure Statement,
- TSA: Autoridad de Sellado de Tiempo
- TSU: Unidad de Sellado de Tiempo