Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos

It-SecurityServices

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	1.2
Fecha edición:	29/10/2025
Fichero:	PSADE-1-DPAC_ITSS_v1.2
Código:	PSADE-1-

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Cargo: Responsable SGSI Fecha: 29/10/2025	Cargo: Responsable de Seguridad Fecha: 29/10/2025	Cargo: CEO Fecha: 30/10/2025

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	Resp. SGSI	09/12/2024
1.1	General	Revisión general del documento, mediante corrección de erratas, ampliación de la información de los servicios.	Resp. SGSI	06/03/2025
1.2	1.6 y 9.8	Actualización de la dirección y teléfono	Resp. SGSI	29/10/2025

Índice

1. Introducción

1.1. Presentación

El presente documento describe la Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos de **IT Security Services, S.A. de C.V.**, en adelante "***ITSS***", en calidad de Proveedor de Servicios de Almacenamiento de Documentos Electrónicos conforme lo establecido en la Ley de Firma Electrónica (Decreto Legislativo No 133) y el Reglamento de la Ley de Firma Electrónica (Decreto Legislativo No 60) en El Salvador.

Esta Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos expone y describe la forma en que ITSS provee los distintos servicios de almacenamiento, asegurando el cumplimiento de la normativa y estándares aplicables.

Los servicios de almacenamiento ofrecidos por ITSS son los siguientes:

- **Procesamiento y Almacenamiento de mensajes de datos y documentos electrónicos.** Conforme el estándar ETSI TS 102 573.

- **Archivo y conservación de mensajes de datos y documentos electrónicos**. Conforme los estándares ETSI TS 119 511 y ETSI TS 119 512.

1.2. Nombre del documento e identificación

El presente documento establece la Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos de ITSS, en lo sucesivo "*DPAC*".

1.3. Identificadores de los servicios

Con el fin de identificar los Servicios de Almacenamiento y Conservación de documentos electrónicos, ITSS ha asignado a cada una de sus modalidades un identificador de objeto (OID) único.

Número OID	Tipo de servicios
1.3.6.1.4.1.61909.1.2	Procesamiento y Almacenamiento de mensajes de datos y documentos electrónicos.
1.3.6.1.4.1.61909.1.3	Archivo y conservación de mensajes de datos y documentos electrónicos.

El servicio de procesamiento y almacenamiento de mensajes de datos y documentos electrónicos se identificará en adelante como "*Servicio de Almacenamiento*".

El servicio de archivo y conservación de mensajes de datos y documentos electrónicos se identificará en lo sucesivo como "*Servicio de Conservación*".

Ambos servicios, podrán ser identificados conjuntamente como "*Servicios de Almacenamiento y Conservación*".

En caso de contradicción entre esta DPAC y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos.

1.4. Participantes en los servicios de almacenamiento y conservación

1.4.1. Proveedor de servicios de almacenamiento de documentos electrónicos

El Proveedor del Servicio de Almacenamiento de Documentos Electrónicos (en lo sucesivo denominado "*PSADE*") es la persona natural o jurídica, que presta servicios de procesamiento y almacenamiento de mensajes de datos y documentos electrónicos, desmaterialización de documentos físicos, archivo y conservación de mensajes de datos y de documentos electrónicos, así como otros servicios relacionados con el tratamiento y preservación de archivos y documentos electrónicos.

ITSS es un Proveedor del Servicio de Almacenamiento de Documentos Electrónicos, que actúa de acuerdo con la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento, Decreto 534 de Ley

de Acceso a la Información Pública, así como las normas técnicas aplicables a la provisión de Servicios de Almacenamiento y Conservación.

Asimismo, ITSS se encuentra acreditado como Proveedor de Servicios de Almacenamiento de Documentos Electrónicos, para el Servicio de Desmaterialización de documentos.

1.4.2. Suscriptor del servicio

Los suscriptores de los Servicios de Almacenamiento y Conservación son las personas naturales y/o jurídicas que adquieren los servicios de Procesamiento y Almacenamiento de mensajes de datos y documentos electrónicos y/o los servicios de Archivo y conservación de mensajes de datos y documentos electrónicos de ITSS (directamente o a través de un tercero).

1.4.3. Tercero que confía

Los terceros que confían son las personas naturales y/o jurídicas que confían en los servicios prestados por ITSS, esto es que reciben documentos procesados por los servicios de almacenamiento y/o conservación.

1.4.4. Proveedores

La prestación de los servicios de ITSS se apoya en distintos servicios ofrecidos por terceros, que se identifican a continuación:

1.4.4.1. Autoridad de Sellado de Tiempo

La Autoridad de Sellado de Tiempo (TSA) es el tercero de confianza que presta el servicio de expedición de sellos de tiempo electrónicos. La TSA es la encargada de expedir sellos de tiempo con el fin de probar que una serie de datos han existido y no han sido alterados a partir de un instante específico en el tiempo.

ITSS utiliza servicios de Prestadores de Servicios de Certificación que cumplen con las políticas de certificación conforme lo establecido en la norma ETSI EN 319 421 o equivalente.

1.4.4.2. Proveedor de Servicios Electrónicos de Certificación

El Proveedor de Servicios electrónicos de certificación es la persona natural o jurídica, que expide y gestiona certificados electrónicos para entidades finales, empleando una Entidad de Certificación (CA), y/o que presta otros servicios relacionados con la firma electrónica.

ITSS utiliza servicios de Prestadores de Servicios de Certificación que cumplen con las políticas de certificación conforme lo establecido en la norma ETSI EN 319 411 o equivalente.

1.4.4.3. Proveedor de la infraestructura tecnológica

Los proveedores de la infraestructura tecnológica son aquellas entidades que prestan servicios de “infraestructura como servicio” para el alojamiento y ejecución de sistemas y aplicaciones. Asimismo para la gestión y carga de los distintos módulos que conforman el servicio para las funcionalidades de: carga/recepción de documentos, procesado y devolución, gestión de flujos, etc.

ITSS utiliza servicios de prestadores que garanticen la seguridad y disponibilidad de sus operaciones, mediante certificaciones en seguridad y/o procedimientos análogos.

1.4.4.4. Proveedor de la infraestructura de conservación

El Proveedor de la infraestructura de conservación es la persona natural o jurídica que constituye y gestiona la plataforma para la custodia a largo plazo de documentos electrónicos.

ITSS utiliza servicios de prestadores que cumplen lo establecido en la norma ETSI TS 119 511.

1.5. Límites de uso del servicio

La Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos, Políticas de almacenamiento y demás documentos que se establezcan para los servicios de almacenamiento y conservación de ITSS, constituyen los documentos que determinan los usos y limitaciones de cada servicio, los cuales se encuentran publicados en: https://itss.sv/politicas-practicas.

1.5.1. Usos permitidos para los servicios

Sin perjuicio de lo anterior, a continuación se establecen los usos permitidos con carácter general para los Servicios de Almacenamiento y Conservación de ITSS.

1.5.1.1. Servicio de Almacenamiento

El servicio de Procesamiento y Almacenamiento de mensajes de datos y documentos electrónicos es una solución destinada a garantizar la integridad, autenticidad y legibilidad de objetos de datos, estableciendo formatos y aplicando tecnologías para producir y mantener de manera confiable los documentos electrónicos.

El Servicio de Almacenamiento permite la conservación de documentos electrónicos por cuenta propia asegurando la disponibilidad del documento para su consulta, la integridad de la información, manteniéndose el documento electrónico legible, completo y sin alteraciones.

Este servicio dispone del OID 1.3.6.1.4.1.61909.1.2.

1.5.1.2. Servicio de Conservación

El servicio de archivo y conservación de mensajes de datos y documentos electrónicos es una solución destinada a garantizar la integridad, autenticidad y legibilidad de objetos de datos, aplicando diferentes tecnologías de almacenamiento y criptografía por tal de mantener el estado de validez del documento durante largos períodos de tiempo.

El Servicio de Conservación garantiza la disponibilidad, integridad y confidencialidad de los documentos electrónicos conservados directamente por ITSS durante periodos de preservación a largo plazo.

Este servicio dispone del OID 1.3.6.1.4.1.61909.1.3.

1.5.2. Límites y prohibiciones de uso de los servicios

Los Servicios de Almacenamiento y Conservación de ITSS se utilizarán exclusivamente para la función y finalidad que tengan establecida en el presente documento, políticas y términos y condiciones que sean de aplicación, debiendo respetar en todo momento la normativa vigente.

Los usos que contravengan lo dispuesto en la presente DPAC, tendrán la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a ITSS, en función de la legislación vigente, de todas las responsabilidades que provengan del uso indebido de los mismos, ya sea realizado directa o indirectamente por el suscriptor.

1.6. Administración del documento

1.6.1. Organización que administra el documento

IT Security Services, Sociedad Anónima de Capital Variable

Dirección fiscal: 89 Avenida Norte y Calle El Mirador Colonia Escaló, Edificio WTC, Torre I, Piso 2, Local 201-A, Colonia Escalón, San Salvador. Código postal 1101

NIT: 0623-290424-104-0

NRC: 343908-4

1.6.2. Datos de contacto de la organización

IT Security Services, Sociedad Anónima de Capital Variable

Dirección fiscal: 89 Avenida Norte y Calle El Mirador Colonia Escaló, Edificio WTC, Torre I, Piso 2, Local 201-A, Colonia Escalón, San Salvador. Código postal 1101

Correo electrónico: comercial@it-securityservices.com

Web: https://www.itss.sv/

Teléfono: +503 2254 6777

1.6.3. Procedimientos de gestión del documento

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

2. Publicación y repositorio de la información

2.1. Repositorio

Se dispone de un repositorio público en el que se publican las informaciones relativas a los Servicios de Almacenamiento y Conservación de ITSS.

El repositorio se encuentra disponible en https://itss.sv/politicas-practicas.

Dicho repositorio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema se realizarán sus mejores esfuerzos para que el servicio se encuentre disponible en la mayor brevedad posible.

2.2. Publicación de información del PSADE

En el repositorio serán publicadas las siguientes informaciones:

- Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos.
- Política de almacenamiento de documentos electrónicos.
- Política de Seguridad de la Información.
- Si procede, términos y condiciones de los distintos Servicios de Almacenamiento y Conservación.

2.3. Frecuencia de publicación

La información del PSADE, incluyendo las políticas y la Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos se rigen por lo establecido en la sección 1.6.3 de este documento.

2.4. Control de acceso al repositorio

ITSS no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del repositorio, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

Se emplean sistemas fiables para el repositorio, de modo tal que:

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

3. Descripción de los servicios

3.1. Procedimiento funcional del Servicio de Almacenamiento

El Servicio de Procesamiento y Almacenamiento de mensajes de datos y documentos electrónicos es una solución destinada a garantizar la integridad, autenticidad y legibilidad de objetos de datos, estableciendo formatos y aplicando tecnologías para producir y mantener de manera confiable los documentos electrónicos.

El procedimiento del servicio de almacenamiento de documentos electrónicos de ITSS es el siguiente:

1. El Suscriptor previo al inicio del servicio debe aceptar y firmar el contrato de prestación de servicios de almacenamiento y conservación.

2. Una vez contratado, ITSS facilita al Suscriptor o a quien éste designe, las instrucciones y acceso a la Plataforma de Almacenamiento de Documentos de ITSS.

3. El Suscriptor a través de canales seguros remite a la plataforma los documentos electrónicos que desea almacenar de manera segura.

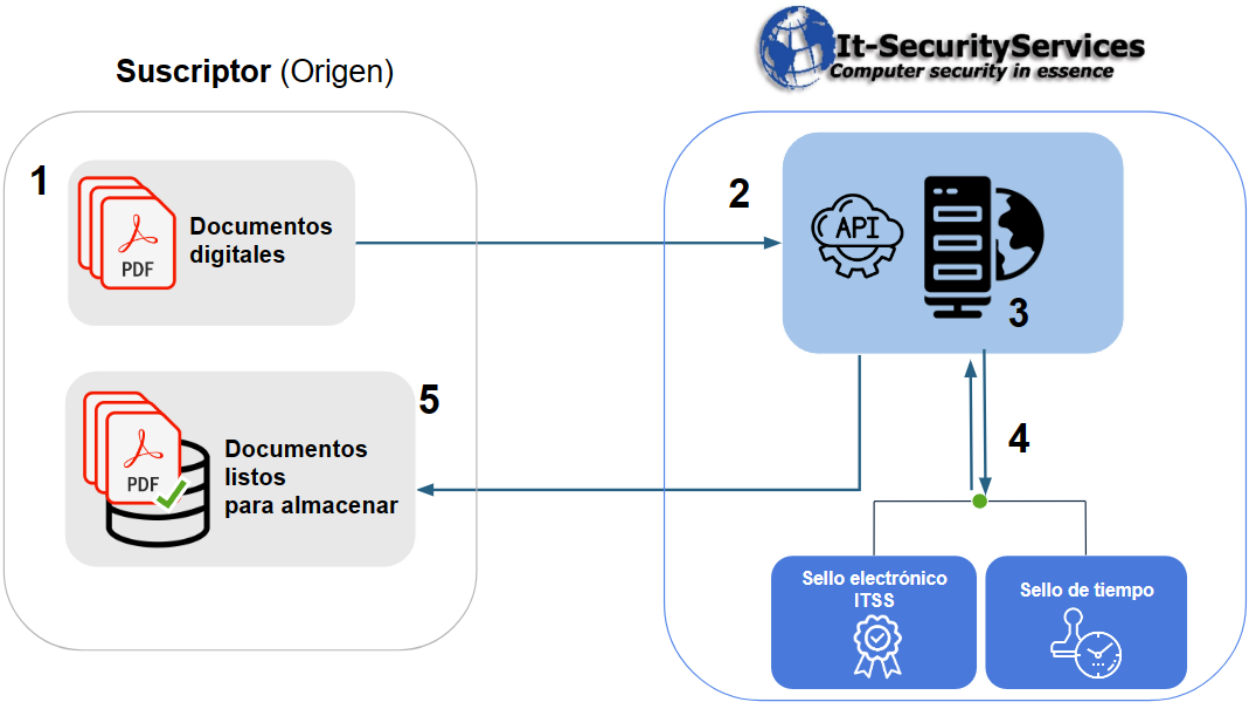
4. La plataforma de ITSS realiza la verificación de los documentos por tal de evidenciar que se ajustan a los formatos aceptados por el servicio. En caso que los documentos no puedan ser recibidos o no se ajusten a los requisitos definidos, estos serán rechazados, informando al Suscriptor.

5. Una vez evaluada la conformidad de los documentos electrónicos, se procede al sellado electrónico por parte de ITSS. Para ello se utilizará un certificado electrónico de sello propio de ITSS, expedido por un Proveedor de Servicios electrónicos de certificación conforme lo establecido en el presente documento.

6. Seguidamente al sellado del documento, se procederá a añadirle un sello de tiempo expedido por una Autoridad de Sellado de Tiempo conforme lo establecido en el presente documento.

7. El documento electrónico resultante será un fichero debidamente firmado en formato attached con nivel de firma -T. Éste contiene el archivo original más la correspondiente firma y sellado de tiempo. El formato de las evidencias de almacenamiento dependerá del formato/extensión del archivo de entrada: PAdES-T para PDF (recomendado), XAdES-T para XML y CAdES-T para el resto.

8. El documento electrónico se pondrá a disposición del Suscriptor para que proceda a su conservación por cuenta propia. La entrega se realizará directamente en los sistemas del Suscriptor. ITSS únicamente almacenará el documento electrónico durante el tiempo que dura el procesado del documento y hasta la puesta en disposición en los sistemas del Suscriptor (recepción, creación de evidencias de conservación y devolución).



3.2. Procedimiento funcional del Servicio de Conservación

El Servicio de Archivo y Conservación de mensajes de datos y documentos electrónicos consiste en una solución destinada a garantizar la integridad, autenticidad y legibilidad de objetos de datos, aplicando diferentes tecnologías de almacenamiento y criptografía por tal de mantener el estado de validez del documento durante largos períodos de tiempo.

El servicio de conservación ofrecido por ITSS está basado en la especificación OAIS (Open Archival Information System) estándar ISO 14721. Los acrónimos utilizados en el siguiente procedimiento forman parte de dicha especificación.

El procedimiento del servicio de conservación de documentos electrónicos de ITSS es el siguiente:

1. El Suscriptor previo al inicio del servicio debe aceptar y firmar el contrato de prestación de servicios de almacenamiento y conservación.

2. Una vez contratado, ITSS facilita al Suscriptor o a quien éste designe, las instrucciones y acceso a la Plataforma de Conservación de Documentos de ITSS.

3. El Suscriptor a través de canales seguros remite a la plataforma los documentos electrónicos que desea conservar de manera segura y duradera en el tiempo. El proceso de conservación de documentos se puede iniciar periódicamente y de manera automática según la tipología de documentos y las reglas de conservación definidas, acordadas previamente con el Suscriptor.

4. La plataforma de ITSS realiza la verificación de los documentos por tal de evidenciar que se ajustan a los formatos aceptados por el servicio. En caso que los documentos no puedan ser recibidos o no se ajusten a los requisitos definidos, estos serán rechazados, informando al Suscriptor.

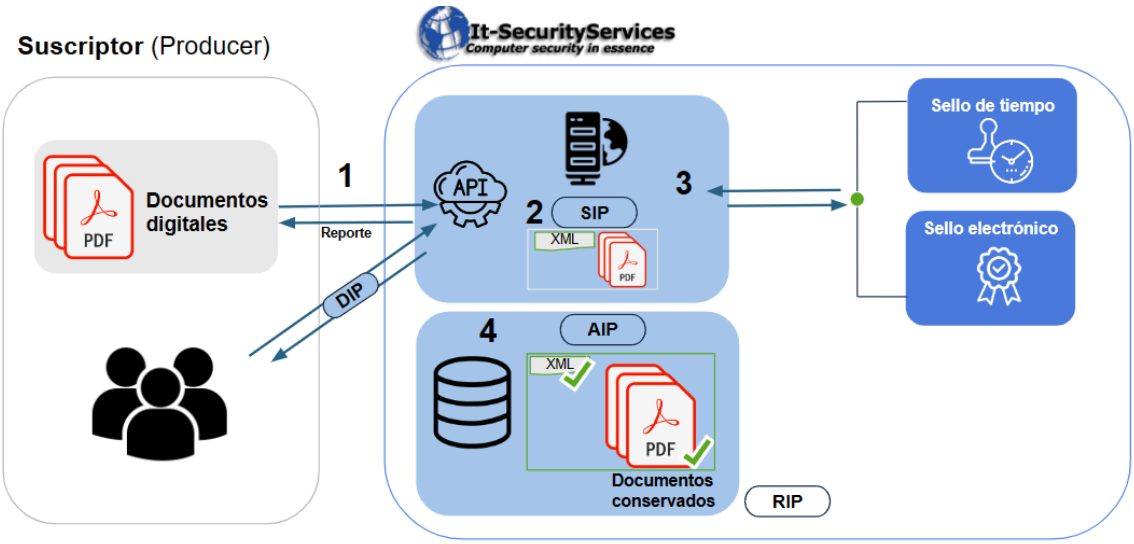
5. Una vez evaluada la conformidad de los documentos electrónicos, se crea un Paquete de Depósito (SIP - Submission Information Package) conteniendo dichos documentos, junto con un archivo XML incluyendo un índice/identificador como referencia de este paquete.

6. Una vez el paquete de depósito se encuentra listo, se procede a aplicar una firma electrónica y un sello de tiempo, utilizando certificados expedidos por un Proveedor de Servicios electrónicos de certificación conforme lo establecido en el presente documento.

7. Asegurada la integridad a través de la firma electrónica y habiendo añadido una referencia temporal de confianza, dicho paquete queda convertido en un Paquete de Conservación (AIP - Archival Information Package). Dicho paquete queda listo para su conservación en las bases de datos seguras de ITSS durante el periodo de tiempo que corresponda. Dicho proceso crea una trazabilidad que queda registrada tanto en el AIP como en los registros seguros del sistema.

8. Si durante el tiempo que dura la conservación, los Paquetes de Conservación requieren una actualización o extensión de las evidencias de conservación, el servicio puede hacer uso de los Paquetes de Revisión (RIP - Revision Information Package), los cuales permiten una actualización de un Paquete de Depósito (SIP) previo. Dicha revisión a través de un RIP siempre se realiza referenciando al SIP anterior e indicando el motivo por el cual ha sido requerido. Esto garantiza la integridad y la autenticidad de los archivos y evidencias durante el periodo de conservación correspondiente.

   Cabe destacar que el Suscriptor (Producer) recibe un reporte (Submission Report) con identificadores únicos una vez los documentos han sido validados y cargados de forma correcta en el sistema de conservación. El Suscriptor o a quién este autorice puede consultar los datos y el estado de cualquier archivo conservado y de sus evidencias cuando sea requerido a través de Paquetes de Consulta (DIP - Dissemination Information Packages).


Suscriptor (Producer)
It-SecurityServices
Computer security in essence
Documentos digitales
PDF
1
Reporte
DIP
API
2
SIP
XML
PDF
3
Sello de tiempo
Sello electrónico
4
AIP
XML
PDF
Documentos conservados
RIP

4. Requisitos operacionales de los servicios

4.1. Formato y conversión de los documentos electrónicos

Los Servicios de Almacenamiento y Conservación de documentos electrónicos de ITSS aceptan los objetos de datos o documentos electrónicos descritos en la siguiente tabla:

Formato	Extensión	Visor	Mime-Type
PDF	.pdf	Adobe Reader	application/pdf
PDF/A	.pdf	Adobe Reader	application/pdf
XML	.xml	Navegador Web	application/xml
TXT	.txt	Varios	text/xml
TIFF	.tiff	Varios	image/tiff
JPG	.jpg/.jpeg	Varios	image/jpeg
OOXML	.docx, .xlsx, .pptx	Varios	
P7M	.p7m	Varios	
ZIP	.zip	Varios	application/zip

El servicio aceptará archivos que ya puedan incluir una firma electrónica o un sello de tiempo incorporados (en las extensiones .pdf, .xml o .p7m).

ITSS no procederá a la conversión, transformación y/o cualquier modificación del formato de los documentos enviados por el Suscriptor. No obstante lo anterior, el Suscriptor podrá contratar los servicios de desmaterialización de documentos, los cuales se regirán por lo dispuesto en el Plan de Desmaterialización aprobado por ITSS así como los términos y condiciones propios de dicho servicio.

Para los objetos de datos aceptados descritos anteriormente, ITSS podrá solicitar información adicional y una serie de requisitos para asegurar que los mismos pueden ser procesados y preparados para su almacenamiento o conservación. Estos requisitos

pueden incluir: que el contenido de los documentos se encuentre en formatos interoperables o la definición de formatos de codificación.

Corresponde al Suscriptor entregar todos los documentos electrónicos en dichos formatos y con la correspondiente fiabilidad de los mismos. ITSS rechazará cualquier documento electrónico no disponga de la correspondiente fiabilidad.

ITSS tendrá preferencia por archivos de tipo PDF, dada su interoperabilidad, estandarización y facilidad de firma, visualización y revisión por parte del Suscriptor.

4.2. Sellado electrónico de los documentos electrónicos

ITSS en la prestación de los Servicios de Almacenamiento y Conservación de documentos electrónicos, procederá al sellado electrónico de todos los documentos electrónicos u objetos de datos con su propio certificado de sello electrónico, sin perjuicio que el documento electrónico enviado por el Suscriptor se encuentre previamente firmado electrónicamente.

En el presente apartado se definen todos los requisitos y características propias del proceso de sellado electrónico de los documentos del servicio.

4.2.1. Tipo de firma electrónica

Las firmas y/o sellos electrónicos utilizados por ITSS serán como mínimo firma electrónica avanzada "*AdES*", garantizando así la autenticidad e integridad durante la vida del documento electrónico.

Las firmas electrónicas empleadas utilizan los siguientes estándares:

- CAdES, de acuerdo al estándar ETSI EN 319 122.
- XAdES de acuerdo al estándar ETSI EN 319 132.
- PAdES de acuerdo al estándar ETSI EN 319 142.

4.2.2. Tipo de certificado electrónico

El certificado electrónico utilizado será un certificado de sello electrónico basado como mínimo en una política de certificación normalizada (N). Este será expedido por un Prestador de Servicios de Certificación que garantice de manera confiable las claves públicas y el estado de revocación, durante todo el periodo de conservación de los documentos electrónicos conservados.

4.2.3. Uso de la clave privada

La clave privada del certificado electrónico empleado para el sellado de la documentación electrónica se mantendrá bajo el control exclusivo de ITSS, de acuerdo con los procesos y medidas de seguridad adoptadas por el Prestador de Servicios de Certificación, conforme lo estipulado en su Declaración de Prácticas y Políticas de Certificación.

4.2.4. Registro del titular y gestión del ciclo de vida del certificado

ITSS únicamente empleará certificados electrónicos expedidos por Prestadores de Servicios de Certificación que acrediten su conformidad con el estándar ETSI EN 319 411-1, garantizando así la confiabilidad de todos los procesos de identificación, autenticación y registro del suscriptor y su titular, la debida entrega del certificado y sus claves, así como la correcta gestión del ciclo de vida del mismo, entendiéndose esta como su emisión, suspensión, reactivación, revocación y renovación.

4.2.5. Política de validación de firmas

Se aplicará la política de validación de firmas definida en la Declaración de Prácticas de Certificación del Prestador de Servicios de Certificación que expida el certificado electrónico, todo ello conforme lo establecido en el estándar ETSI EN 319 411-1.

La validación se realizará a través del estado de validez del certificado empleado, utilizando las Listas de Revocación de Certificados (CRL) o por medio del Protocolo de Verificación de Certificados en Línea (OCSP). Toda la información requerida para la validación está disponible en el documento electrónico sellado.

Los Suscriptores, bajo demanda, podrán solicitar a ITSS información relativa a la política de validación de firmas.

4.3. Sellado de tiempo electrónico de los documentos electrónicos

ITSS en la prestación de los Servicios de Almacenamiento y Conservación, procederá al sellado de tiempo electrónico de todos los documentos electrónicos u objetos de datos por tal de garantizar el momento en que ese documento electrónico existía y que el certificado empleado era válido.

ITSS únicamente utilizará servicios de sellado de tiempo ofrecidos por Prestadores de Servicios de Certificación que acrediten su conformidad con el estándar ETSI EN 319 421.

Los sellos de tiempo se realizarán conforme lo estipulado por los estándares IETF RFC 3161 y 5816. Asimismo se seguirá el protocolo y perfiles definidos en el estándar ETSI EN 319 422.

4.4. Política de evidencias electrónicas

Los Servicios de Almacenamiento y Conservación de ITSS generan evidencias a los documentos electrónicos transmitidos por el Suscriptor. Estas se crean a través del sellado electrónico de los documentos y la aplicación del sello de tiempo.

El algoritmo de firma utilizado tanto para el sellado como para el sello de tiempo es:

- RSA SHA-256

Los formatos de las evidencias de preservación para los servicios de almacenamiento y conservación se definen a continuación.

4.4.1. Servicio de Almacenamiento

El Servicio de Almacenamiento de ITSS crea las siguientes evidencias de preservación para que posteriormente el Suscriptor las almacene y conserve por cuenta propia.

Tipo de documento	Formato de firma	Evidencias de conservación	Formato de las evidencias
PDF	PAdES-T	Documento original incluyendo las evidencias de conservación en formato adjunto (attached).	.pdf
XML	XAdES-T	Archivo original incluyendo las evidencias de conservación en formato adjunto (attached).	.xml
Resto de tipo de archivos definidos en la sección "4.1. Formato y conversión de los documentos electrónicos".	CAdES-T	Archivo original incluyendo las evidencias de conservación en formato adjunto (attached).	.p7m

4.4.2. Servicio de Conservación

El Servicio de Conservación de ITSS crea las siguientes evidencias de preservación para posteriormente conservarlas.

Las evidencias generadas forman parte del Paquete de Conservación, definido por el estándar OAIS, bajo el tipo de objeto AIP - Archival Information Package. Open Archival Information System (OAIS) es un modelo conceptual destinado a la gestión, al archivo y a la preservación a largo plazo de documentos.

Dicho paquete contiene:

- los objetos a preservar (documentos y/o metadatos de los documentos);
- el índice del Paquete de Conservación (AIPindex), como representación de la información a conservar y de las evidencias de conservación.

El hash de los objetos se crea a partir de una función resumen que emplea el algoritmo robusto SHA 256.

El índice AIP es la evidencia de preservación producida en formato XML asociada a cada AIP en la que se detalla la estructura de datos. Sobre dicho índice se aplica un sello electrónico y un sello de tiempo.

Un AIP puede contener varios SIPs. Cada AIP y SIP contiene un número de versión. Cuándo se requiere realizar una revisión de la versión de cierto paquete de conservación, se actualiza dicha versión y los cambios quedan registrados. Un paquete de revisión permite modificar un SIP ya enviado creando un nuevo SIP con el Id de referencia del original. Para ser aceptado, debe incluir el tipo de cambio solicitado:

- Corrección: Modificación o ajuste de un acto o condición previa.
- Complemento: Adición de información a un acto o condición previa.
- Nota: Resumen con fines administrativos o disciplinarios.

También se usa cuando es necesario agregar una nueva firma o sello de tiempo sobre las evidencias de preservación.

Las evidencias no contienen información respecto de los Servicios de Almacenamiento y Conservación de ITSS, no obstante se incluye información respecto de los servicios de sellado y sellado de tiempo.

Los certificados de sello electrónico utilizados han sido expedidos por un Prestador de Servicios de Certificación conforme el estándar ETSI EN 319 411-1. Los servicios de sellado de tiempo utilizados son provistos por un Prestador de Servicios de Certificación conforme el estándar ETSI EN 319 421.

El aumento de las evidencias de conservación se consigue a través de la extensión/revisión conforme lo estipulado en el presente documento. El proceso de extensión/revisión dependerá de los servicios contratados por el Suscriptor.

La validación de las evidencias se realiza a través del estado de validez del certificado empleado tanto para el sello como para el sellado de tiempo, utilizando las Listas de

Revocación de Certificados (CRL) o por medio del Protocolo de Verificación de Certificados en Línea (OCSP) ofrecidos por los correspondientes Prestadores de Servicios de Certificación.

La duración de las evidencias generadas por ITSS en los Servicios de Almacenamiento y Conservación vienen determinadas por el estándar ETSI TS 119 312.

5. Conservación de documentos electrónicos

5.1. Perfil y modelo de conservación

El Servicio de Conservación de ITSS de conformidad con el estándar ETSI TS 119 511 sigue un modelo de "Servicio de preservación con conservación (WST)", identificado con el OID: 1.3.6.1.4.1.61909.1.3.

El esquema de conservación viene definido por la URI:

```
http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers
```

ITSS tramitará los documentos electrónicos enviados por los Suscriptores conforme al Servicio de Conservación descrito en el presente documento, generando las evidencias correspondientes.

Posteriormente conservará los documentos y evidencias el tiempo necesario según lo acordado con el Suscriptor.

El modelo de conservación se mantendrá inalterable durante todo el periodo de preservación.

No obstante lo anterior, el Servicio de Almacenamiento de ITSS no conservará ni custodiará ningún documento y/o evidencia, siendo el único responsable el Suscriptor.

5.2. Metas de conservación

El Servicio de Conservación de ITSS tiene las siguientes metas funcionales:

a) Preservación general de datos [PGD]. Aportación de pruebas de la existencia durante largos períodos de tiempo de datos generales, ya sea que estos datos estén firmados o no.

   http://uri.etsi.org/19512/goal/pgd

b) Preservación de firmas digitales [PDS]. La preservación, durante largos períodos de tiempo, de la capacidad de validar una firma digital, mantener su estado de validez y obtener una prueba de existencia de los datos firmados asociados.

   http://uri.etsi.org/19512/goal/pds

c) Augmentation [AUG]. Aumento de las pruebas de conservación presentadas al servicio de conservación. Dicho aumento se procederá cuando sea necesario acorde a lo definido en el presente documento y/o haya sido contratado por el Suscriptor.

   http://uri.etsi.org/19512/goal/aug

El objetivo principal del servicio es producir evidencia de que los datos o documentos electrónicos no han sido alterados y han existido en un momento determinado, así como conservarlos en el tiempo de manera segura.

5.3. Acceso a la documentación electrónica

En el Servicio de Conservación, la documentación electrónica será custodiada por ITSS, para ello se han implementado controles de acceso que garantizan que únicamente el personal autorizado por el Suscriptor puede acceder a la documentación electrónica.

El acceso a la documentación se realizará de manera remota mediante el empleo de credenciales robustas y a través de protocolos de comunicación seguros como SSL / TLS.

Sin perjuicio de lo anterior, ITSS podrá conceder acceso temporal a terceros ajenos al Suscriptor como consecuencia de procedimientos judiciales, legales, policiales o administrativos, en general a cualquier organismo de acuerdo con lo establecido en la normativa actual.

5.4. Autenticidad e integridad de la documentación electrónica

ITSS dispone de un sistema de eventos que monitoriza los sistemas por tal de garantizar la autenticidad, validez e integridad de los documentos electrónicos.

La aplicación de una firma electrónica avanzada garantiza la autenticidad de los sellos electrónicos utilizados, así como la integridad de la documentación.

Cuando corresponda, se aplicará la extensión de las evidencias de conservación, garantizando el mantenimiento de la misma durante el periodo de conservación.

ITSS únicamente permite el acceso y la descarga de la documentación electrónica por parte de personal autorizado.

5.5. Legibilidad

ITSS garantiza que los documentos electrónicos son legibles por humanos o máquinas durante todo el proceso de conservación. Los Servicios de Almacenamiento y Conservación de documentos electrónicos de ITSS, únicamente aceptan documentos electrónicos y/u objetos de datos en formato PDF.

Cuando exista el riesgo de que el formato de los documentos electrónicos o sistema de visualización específico se vuelva obsoleto, ITSS actualizará sus Servicios de Almacenamiento y Conservación a un nuevo formato de datos o sistema de visualización vigente.

Respecto los documentos electrónicos conservados por ITSS, cuando el formato o sistema de visualización de los mismos se vuelva obsoleto, todos los documentos afectados se copiarán de manera confiable manteniendo su semántica sin cambios, a un nuevo formato de datos o sistema de visualización vigente. ITSS elaborará una declaración confiable e independiente que dé fe de la correspondencia del contenido y la semántica del nuevo objeto de datos con el anterior.

5.6. Tipo de medio de almacenamiento

ITSS utiliza soportes de almacenamiento que garantizan la conservación segura de los documentos durante la prestación del Servicio de Conservación.

ITSS dispone de un sistema de gestión de seguridad de la información por el que se garantiza la utilización de medios y/o activos confiables, haciendo uso de proveedores y/o productos certificados.

En el Servicio de Conservación, los documentos y evidencias se encuentran almacenados en objetos de tipo S3 y buckets dedicados, basados en AWS. Dichos contenedores se encuentran dentro de una red perimetral protegida y monitorizada por el equipo de Proveedor, dentro de los centros de datos de Amazon Web Services. Estos centros de datos cumplen con la mayoría de estándares de seguridad internacionales y en particular, ISO 27001, 27017 y 27018.

5.7. Requisitos de separación y confidencialidad

ITSS garantiza la confidencialidad de toda la información procesada y conservada a través de su Servicio de Conservación.

La documentación electrónica se procesa y se conserva de manera individualizada para cada Suscriptor, siendo imposible que estos accedan a documentación de otros suscriptores o viceversa. A través de un fuerte control de acceso y un aislamiento lógico, se asegura el acceso a la información únicamente por las personas autorizadas.

Para cada Suscriptor, se permite la configuración de políticas de conservación. Cada objeto de datos enviado a conservar cuenta con un identificador único y exclusivo del Suscriptor propietario de dichos datos, restringiendo el acceso únicamente por personal autorizado por el Suscriptor.

En los casos en lo que el Suscriptor lo demande y previo acuerdo con ITSS, se permitirá el cifrado de datos con clave bajo control del Suscriptor para añadir una capa adicional de confidencialidad (ej. tratamiento de datos altamente sensible).

El acceso e intercambio de la documentación electrónica conservada por ITSS, corresponde exclusivamente al Suscriptor o a quien éste designe mediante autorización expresa.

No obstante lo anterior y de conformidad con lo establecido por la legislación aplicable, ITSS podrá otorgar el acceso a la documentación electrónica a terceros distintos del Suscriptor, como consecuencia de procedimientos judiciales, legales, policiales o administrativos.

En cualquier caso, el acceso se realizará de acuerdo con las medidas de seguridad de acceso definidos en el presente documento, debiendo identificar y autenticar al tercero que requiere el acceso, otorgarle unas credenciales y acceder a través de los protocolos de comunicación seguros provistos por ITSS.

5.8. Mantenimiento de la validez del documento electrónico durante el periodo de conservación

ITSS ha establecido los medios para que todos los documentos electrónicos resultantes de aplicar el Servicio de Conservación, mantengan su validez durante todo período de conservación requerido por el Suscriptor.

Para ello, ha adoptado distintas medidas técnicas y organizativas por tal de asegurar que todos los sellos electrónicos incluidos en los documentos electrónicos conservados, se pueda verificar su validez durante todo el periodo correspondiente.

5.8.1. Medidas técnicas

Todas las firmas realizadas por ITSS incluyen la información necesaria que permite realizar la validación de los sellos electrónicos. Ello se consigue a través de los puntos y/o enlaces de validación para consultar el estado de revocación, ya sea a través de las Listas de Revocación de Certificados (CRL) o por medio del protocolo OCSP.

Asimismo cada documento electrónico incluye un indicador de confianza realizado en el momento del sellado del mismo, concretamente se aplica un sello de tiempo por un prestador de servicios de certificación acreditado por tal de garantizar el momento en que ese documento electrónico existía y era válido el certificado empleado.

La duración del documento electrónico así como de las evidencias vendrá determinado por lo estipulado en el estándar ETSI TS 119 312. Con el fin de garantizar la conservación de los documentos electrónicos almacenados por un tiempo superior al tiempo de vida de los algoritmos criptográficos, longitudes de clave empleadas y validez de los certificados electrónicos utilizados, ITSS ha establecido un proceso de extensión de las evidencias de conservación.

En el Servicio de Conservación, la extensión de las evidencias de conservación consiste en la revisión de las evidencias anteriores para extender su validez, a través de la aplicación de un nuevo sello electrónico junto con un nuevo sello de tiempo cuando sea necesario, asegurando la fiabilidad de las evidencias de conservación durante el periodo de tiempo requerido.

5.8.2. Medidas organizativas

ITSS dispone de un sistema de gestión de la seguridad de la información por el que se han adoptado y evaluado políticas, procesos y procedimientos que garantizan la seguridad y confiabilidad de los sistemas y productos.

5.9. Disponibilidad de los documentos electrónicos

En el Servicio de Conservación de ITSS todos los documentos gestionados se almacenan en la plataforma de conservación, cuya disponibilidad se garantiza a través de un servicio diseñado en alta disponibilidad y a través de varias interfaces (acceso panel web o vía servicio web API), manteniendo no obstante fuertes mecanismos de control de acceso para asegurar el acceso a la información únicamente por personal autorizado designado por el Suscriptor.

Cabe destacar que el Suscriptor (Producer) recibe un reporte (Submission Report) con identificadores únicos una vez los documentos han sido validados y cargados de forma

correcta en el sistema de conservación. El Suscriptor o a quién este autorice puede consultar los datos y el estado de cualquier archivo conservado y de sus evidencias cuando sea requerido a través de Paquetes de Consulta (DIP - Dissemination Information Packages).

En el Servicio de Almacenamiento de ITSS, todos los documentos electrónicos gestionados a través del mismo serán puestos a disposición del Suscriptor a través de la propia plataforma del servicio, permitiendo su descarga o bien la entrega directa en los sistemas del Suscriptor a través de integración / punto de acceso.

5.10. Importación y exportación de documentos

ITSS ofrece la posibilidad de la exportación e importación de los documentos electrónicos y evidencias respecto de su Servicios de Conservación.

Para la exportación e importación se utilizarán formatos estandarizados conforme lo descrito en los estándares: (i) ETSI TS 119 512 (estándar OAIS).

El formato de paquetes para la importación, definido como SIP (del inglés, Submission Information Package - Paquete de presentación/envío de información) es un archivo ZIP sin comprimir que contiene documentos sujetos a preservación, los cuales pueden estar firmados digitalmente. Incluye un archivo de índice SIP (XML) que describe el objeto de preservación, identifica al propietario y al productor del SIP, y proporciona metadatos de los documentos. También especifica la aplicación que generó el SIP y los mensajes del administrador de preservación. Contiene detalles como nombres de archivos, hashes y otros datos relevantes. Finalmente, el archivo de índice es firmado digitalmente por ITSS.

El formato de paquete para la exportación, definido como DIP (del inglés Dissemination Information Package - Paquete de difusión de información) es un paquete generado por el sistema de preservación para garantizar la interoperabilidad y transferencia a otros proveedores según normativas y estándares. Puede solicitarse en como resultado de la búsqueda de un documento único, de múltiples documentos (incluyendo los de distintos AIPs) o en respuesta a la terminación del servicio, agrupando AIPs por tipo de documento y año.

El DIP es un archivo ZIP que contiene los documentos solicitados, el índice del SIP, y uno o más índices AIP firmados y sellados de tiempo. También incluye un archivo de índice DIP (XML) con los hashes de los AIPs y documentos. Además, el DIP Index almacena datos sobre su generación, propietario, solicitante, gestor de preservación y lista de archivos entregados.

Las solicitudes de exportación e importación se tramitarán a través de una petición expresa por parte del Suscriptor a través de los métodos de contacto facilitados por ITSS, ya sea a través del Acuerdo de Nivel de Servicio o en el presente documento.

La petición de exportación e importación deberá ser realizada por el propio Suscriptor y/o representante legal debidamente autorizado y/o apoderado. ITSS únicamente entregará el paquete de datos para la exportación al propio suscriptor del servicio o persona autorizada por este.

ITSS mantendrá un registro de todas las solicitudes de importación y/o exportación por el que se indicará la fecha del evento y los criterios que se han utilizado para seleccionar el conjunto de objetos de conservación que se han incluido en el paquete de exportación-importación.

5.11. Extensión / Revisión de documentos electrónicos (Augmentation)

ITSS asegura que los documentos electrónicos tramitados a través del Servicio de Conservación puedan lograr el objetivo de preservación correspondiente.

Si durante el tiempo que dura la conservación, los Paquetes de Conservación requieren una actualización o extensión de las evidencias de conservación, el servicio puede hacer uso de los Paquetes de Revisión (RIP - Revision Information Package), los cuales permiten una actualización de un Paquete de Depósito (SIP) previo. Dicha revisión a través de un RIP siempre se realiza referenciando al SIP anterior e indicando el motivo por el cual ha sido requerido. En esta revisión se aplica un nuevo sello electrónico y un sello de tiempo. Esto garantiza la integridad y la autenticidad de los archivos y evidencias durante el periodo de conservación correspondiente.

No obstante lo anterior, si durante el periodo de preservación temporal existe riesgo respecto de la seguridad de los algoritmos y/o procedimientos criptográficos utilizados en la prestación del servicio de almacenamiento, ITSS procederá a resellar la documentación electrónica antes de que esta no pueda ser utilizada y logre el objetivo o periodo de conservación correspondiente.

5.12. Protocolos de conservación y notificación

5.12.1. Protocolo de conservación

ITSS asegura los canales seguros de comunicación entre sus sistemas y los del Suscriptor, garantizando la confidencialidad de todos los datos a través del uso de cifrado mediante el protocolo HTTPS. Asimismo, se establecen controles de seguridad para que únicamente pueda ser utilizado por el personal autorizado por parte del Suscriptor.

Se ha definido un protocolo de conservación para el servicio de Preservación de datos a Largo Plazo que sigue las operaciones definidas por el estándar ETSI TS 119 512:

- RetrieveInfo
  - Obtención de información acerca del Servicio de Conservación.
- PreservePO
  - Envío de documentos/objetos a conservar a través de un Paquete de Depósito (SIP).
- RetrievePO
  - Obtención de evidencias de conservación y objetos a través de Paquetes de Consulta (DIP).
- UpdatePO
  - Actualización/revisión de objetos de conservación a través de Paquetes de Revisión (RIP).
- RetrieveTrace
  - Obtención de registros relativos a la conservación de un objeto en el sistema.
- DeletePO

- Eliminación de objetos conservados a través de la creación de un Paquete de Eliminación (Discard Information Package) como registro.

- Search
  - Búsqueda y filtrado avanzado de objetos en el sistema.

El proceso de validación de los paquetes de información y de los documentos incluye:

- control de correspondencia de documentos: verificación/matching entre los documentos reales presentes en el Servicio de Conservación y el número de registros provistos para un propietario específico (e.g. DIPs provistos);
- control de integridad de las medidas de conservación aplicadas a los documentos y a los Índices de los paquetes: verificación de la firma y del sello de tiempo en un porcentaje elegido del número total de documentos e índices XML del AIP presentes en el Servicio de Conservación para un suscriptor específico.
  - cálculo y comparación de hashes para asegurar la integridad de los documentos.
  - validación de certificado y emisor utilizado en la firma y sellado de tiempo, asegurando que los mismos pertenecen y son/han sido emitidos y utilizados por y para el Servicio de Conservación.

Se permite la recepción de Paquetes de Depósito a través de servicio web (panel web o API - proceso síncrono) o de sFTP (proceso asíncrono).

- En la opción síncrona, se hace uso del protocolo HTTPS, implementado algoritmos seguros y certificados emitidos por emisores reconocidos para la emisión de certificados TLS/SSL.
- En la opción asíncrona, se hace uso del protocolo SSH-2 para aportar la protección y cifrado de la información compartida a través de sFTP.

Una vez transcurrido el período de conservación acordado entre ITSS y el Suscriptor para cierto objeto/documento, el sistema implementa el procedimiento de descarte del Paquete de Conservación.

El sistema notifica (vía correo electrónico) al Suscriptor del inicio del proceso de descarte de los Paquetes de Conservación correspondiente, dando aviso y proporcionando la

información necesaria para que el Suscriptor evalúe la posible solicitud de ampliación del plazo de conservación.

Si se excede el plazo preestablecido y no se realiza ninguna solicitud de extensión, se activa el procedimiento de descarte, produciendo un Paquete de Descarte relacionado con los objetos pertinentes. La operación es registrada en el sistema y se genera un índice para el Paquete de Descarte, que es firmado electrónicamente.

Como norma general, se adecuarán los documentos conservador de acuerdo con el procedimiento de exportación de datos para proceder a entregárselo al suscriptor.

En el caso de que el suscriptor solicite la eliminación de los documentos conservados por ITSS antes de finalizar el periodo de conservación, se requerirá que la solicitud sea formulada por una persona autorizada por el suscriptor y que facilite el correspondiente justificante.

5.12.2. Protocolo de notificación

Cuando un Paquete de Depósito es aceptado por el Servicio de Conservación, éste genera un Reporte de Entrega incluyendo todas las comprobaciones realizadas en dicho paquete antes de su aceptación. Esto permite formalizar la recepción y aceptación de los datos a conservar. El reporte puede contener referencias a uno o más Paquetes de Depósito.

El Suscriptor puede optar por recibir dichos Reportes de Entrega a través de varios medios:

- Vía correo electrónico como notificación.
- A través del servicio web API.
- A través del acceso al panel web.

Todos los Reportes de Entrega generados por el sistema se mantienen disponibles dentro del Servicio de Conservación para cualquier posible consulta por parte del Suscriptor.

El Suscriptor también puede recibir notificaciones vía correo electrónico cuando un Paquete de Conservación está llegando al fin de su periodo de conservación y entra en el proceso de descarte.

5.13. Monitoreo criptográfico

ITSS emplea algoritmos criptográficos seguros.

Listado de algoritmos utilizados:

- El algoritmo de firma de. En este caso el algoritmo utilizado es el RSA (sha256WithRSAEncryption 1.2.840.113549.1.1.11).
- El identificador del algoritmo de hash utilizado para generar la huella de la evidencia es el sha256 (Algoritmo hash seguro 256bit OID: 2.16.840.1.101.3.4.2.1).

En caso de que uno de los algoritmos o parámetros utilizados se vuelva menos seguro o que la validez los certificados electrónicos empleados vaya a caducar, ITSS actualizará los mismos con antelación suficiente, con el fin de evitar el compromiso de los documentos electrónicos enviados a los Servicios de Almacenamiento y Conservación.

En caso de que uno de los algoritmos o parámetros utilizados en el Servicio de Conservación se vuelva menos seguro o que algunos de los certificados utilizados en el proceso de creación de evidencias deba ser actualizado, ITSS procederá a la revisión y posible extensión de las evidencias de conservación de los documentos electrónicos por tal de garantizar la preservación del documento o evidencia durante el periodo de conservación correspondiente.

5.14. Periodo de preservación

ITSS procederá a la conservación de los documentos electrónicos, así como las evidencias de preservación durante los plazos establecidos con el Suscriptor, mediante el contrato de prestación de servicios. Las evidencias de preservación se conservarán durante los periodos legalmente establecidos, siendo estos de 15 años desde la finalización del servicio.

En caso que el Suscriptor decida dar por terminado el contrato, independientemente de la causa, ITSS procederá a la exportación de toda la documentación electrónica

custodiada de acuerdo con lo identificado en el presente documento y la pondrá a disposición del Suscriptor. El plazo para la exportación, así como la manera de entregar la información se definirá caso por caso, en atención a las necesidades del Suscriptor, la magnitud y/o cantidad de documentación custodiada.

6. Controles de seguridad

6.1. Controles de seguridad física

Se han 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 de Almacenamiento y Conservación.

ITSS asegura que la infraestructura y sistemas que permiten la prestación de los Servicios de Almacenamiento y Conservación se encuentran alojados en proveedores que garanticen la seguridad a través de certificaciones internacionalmente reconocidas.

El proveedor de infraestructura para ambos servicios es Amazon Web Services. Los centros de AWS datos cumplen con la mayoría de estándares de seguridad internacionales y en particular, ISO 27001, 27017 y 27018.

6.2. Controles de seguridad de red

ITSS 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 basados en TLS/SSL o a través de redes virtuales privadas VPN con autenticación por doble factor.

6.3. Controles de seguridad informática

Se emplean sistemas fiables para ofrecer sus Servicios de Almacenamiento y Conservación. Para atender a este fin, se han 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, ITSS aplica los controles del esquema de certificación ETSI EN 319 401.

Los sistemas usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas 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 copias de seguridad y recuperación.
- Configuración de antivirus.
- Requerimientos de tráfico de red.

Asimismo se incluyen las siguientes funcionalidades:

- Control de acceso a los Servicios de Almacenamiento y Conservación, así como y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial de los suscriptores, servicios de almacenamiento y conservación, así como datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Evaluaciones de vulnerabilidades relacionadas con los Servicios de Almacenamiento y Conservación.

6.4. Controles de seguridad técnica

Se emplean sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica de los Servicios de Almacenamiento y Conservación.

6.4.1. Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por ITSS 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.

6.4.2. Controles de gestión de seguridad

ITSS desarrolla las 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.

ITSS exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores relativas a los Servicios de Almacenamiento y Conservación.

6.4.2.1. Clasificación y gestión de información y bienes

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

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

Los documentos están catalogados en cuatro niveles:

- SIN CLASIFICAR: Se considerará la clasificación de seguridad: “Sin clasificar” cuando el documento o información se encuentra en un estado inicial, que no permite discernir sobre la clasificación de seguridad correspondiente. Sin perjuicio de lo anterior, ante la duda del nivel de clasificación, si se prevé que pudiera contener información sensible o personal, deberá ser clasificado como Confidencial y una vez finalizado el mismo aplicar una reclasificación acorde a este documento

- PÚBLICO: Se considerará la clasificación de seguridad: “Público” cuando el documento o información está disponible para todo el público, tanto para internos como para externos.

- USO INTERNO: Se considerará la clasificación de seguridad: “Uso interno” cuando el documento o información está disponible para un grupo específico de empleados o terceros ajenos a la organización debidamente autorizados.

- CONFIDENCIAL: Se considerará la clasificación de seguridad: “Confidencial”: cuando el documento o información está disponible únicamente a ciertos de empleados o terceros ajenos a la organización debidamente autorizados.

6.4.2.2. Operaciones de gestión

Se 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 se desarrolla en detalle el proceso de gestión de incidencias.

ITSS 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.

6.4.2.3. 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.

6.4.2.4. Gestión del sistema de acceso

ITSS emplea medidas de seguridad físicas y lógicas para asegurar el acceso a los recursos de sus servicios únicamente por el personal autorizado.

En particular:

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- ITSS dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- ITSS 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 es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

6.5. Procedimientos de auditoría de seguridad

6.5.1. Tipos de eventos registrados

ITSS diferencia entre dos tipos de registros:

- los relacionados con el funcionamiento y ejecución a bajo nivel de las aplicaciones/sistemas;
- aquellos relativos a las acciones y operaciones de los Servicios de Almacenamiento y Conservación (incluidos eventos relativos a la seguridad y control de acceso).

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 de registro.

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

- Intentos exitosos o fallidos de inicio y fin de sesión por parte de los usuarios.
- Intentos exitosos o fallidos de crear, modificar o eliminar cuentas del sistema.
- Intentos exitosos o fallidos de crear, modificar o eliminar credenciales de cuentas del sistema.
- Intentos exitosos o fallidos de crear, modificar o eliminar roles del sistema.
- Operaciones relacionadas con el tratamiento de documentos a almacenar o conservar (recepción, procesado, creación de evidencias).
- Accesos para la consulta de registros/logs.
- Cambios en la configuración y mantenimiento del sistema.
- Encendido y apagado de sistemas y aplicaciones.

6.5.2. Tratamiento de registros de auditoría

Además de lo anterior, se realiza una revisión de los registros cuando existe 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.

Se mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de registros.
- Que los ficheros de registros no se reescriben y que mantienen su integridad

- Que se permita identificar de forma unívoca en los registros la recepción y procesado en el sistema de un determinado objeto a almacenar o conservar (ej. almacenando el hash/resumen de dicho objeto de datos).
- 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 registro se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

6.5.3. Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP.

6.5.4. Período de conservación de registros de auditoría

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

No obstante lo anterior, los registros de auditoría que tengan relación con los Servicios de Almacenamiento y Conservación y en concreto con el procesado de los documentos electrónicos de los Suscriptores, se conservarán por el periodo máximo de 15 años.

6.5.5. Protección de los registros de auditoría

Únicamente el personal autorizado tiene permiso para acceder a los sistemas de almacenamiento y gestión de registros de ITSS. Se ha establecido un sistema de seguridad que controla el acceso, verifica la identidad y autenticidad de los usuarios, con el fin de prevenir cualquier intento no autorizado de acceder, alterar, eliminar o manipular la información almacenada.

6.5.6. Procedimientos de copia de respaldo

Se dispone de un procedimiento adecuado de copia de seguridad de los registros de manera que, en caso de pérdida o destrucción de archivos relevantes, dichas copias se encuentren disponibles durante el periodo de tiempo correspondiente.

Se realizan copias de respaldo diarias de todos los registros relativos a los servicios de Almacenamiento y Conservación para casos de recuperación de datos. Dichas copias se almacenan en un centro de datos propiedad del proveedor Amazon Web Services, dónde se preparan para ser almacenadas durante el periodo de tiempo pertinente.

6.5.7. Análisis de vulnerabilidades

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

Los análisis de vulnerabilidad deben ser ejecutados 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. Gestión de incidencias y recuperación de desastre

6.6.1. Procedimientos de gestión de incidencias y compromisos

ITSS 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.

6.6.2. 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, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de recuperación de desastres de ITSS.

6.6.3. Continuidad del negocio después de un desastre

ITSS dispone de un plan de continuidad de negocio. Deberán restablecerse 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.

6.7. Terminación del servicio

ITSS asegura que las posibles interrupciones a los Suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios como Prestador de Servicios de Almacenamiento de Documentos Electrónicos.

Antes de terminar sus servicios, se ha realizado el desarrollo de 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 terminación.
- Informará a todos Suscriptores y terceros interesados con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará, si las hubiera, toda autorización a entidades subcontratadas para actuar en nombre de ITSS.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores.
- 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 indicados al suscriptor.
- Comunicará al Organismo Supervisor Nacional que tenga las competencias atribuidas, con una antelación mínima de 90 días hábiles, el cese de su actividad y si se transfiere la gestión y a quién o si se extinguirá su vigencia.
- Comunicará, también al Organismo Supervisor Nacional que tenga las competencias atribuidas, la apertura de cualquier proceso concursal que se siga contra ITSS, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

7. Controles de procedimientos y del personal

7.1. Controles de procedimientos

Se 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 ITSS ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

7.1.1. Funciones fiables

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

- **Auditor Interno:** Autorizado para ver archivos y registros de auditoría de los sistemas confiables del PSADE.
- **Administrador de Sistemas**: Autorizado para instalar, configurar y mantener los sistemas confiables del PSADE para la gestión de los servicios. Asimismo se incluyen las tareas destinadas a la recuperación de los sistemas.
- **Operador de Sistemas**: Responsables de operar los sistemas confiables del PSADE en el día a día. Autorizado para realizar copias de seguridad del sistema.
- **Responsable de Seguridad**: Responsable general de administrar la implementación de las prácticas y políticas de seguridad.

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

7.1.2. Designación y autenticación para cada función

Las personas asignadas para cada rol son designadas por el personal al cargo de la dirección del PSADE.

Cada persona ha aceptado el cargo, declarando el sometimiento a las políticas y prácticas de seguridad de ITSS, guardando la confidencialidad en el desempeño de su cargo y asegurando encontrarse libre de conflictos de interés.

7.2. Controles de personal

7.2.1. 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 entran en conflicto con el desarrollo de la función que tenga encomendada.

En general, 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. Además de ello, no asignará a 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.

7.2.2. Procedimientos de investigación de historial

ITSS 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.

ITSS 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.

7.2.3. Requisitos de formación

Debe otorgarse al personal una formación respecto de los puestos fiables y de la gestión de estos, hasta que se obtenga la cualificación necesaria, manteniendo el archivo de la formación impartida.

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

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad. 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.

7.2.4. Requisitos y frecuencia de actualización formativa

Se actualiza la formación del personal atendiendo a sus necesidades y con la frecuencia temporal suficiente para que los mismos puedan cumplir sus funciones y obligaciones de

forma competente y satisfactoria, principalmente cuando se realicen modificaciones sustanciales de las tareas establecidas de certificación.

7.2.5. Sanciones para acciones no autorizadas

ITSS 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.

7.2.6. 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 ITSS. 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 Almacenamiento y Conservación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la Declaración de Prácticas de Almacenamiento y Conservación, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los Servicios de Almacenamiento y Conservación.

No obstante lo anterior, el PSADE 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 Almacenamiento y Conservación por tercero distinto a ITSS.

7.2.7. Suministro de documentación al personal

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

8. Auditoría de conformidad

ITSS ha comunicado el inicio de su actividad como Proveedor de Servicios de Almacenamiento de Documentos Electrónicos al Organismo Supervisor Nacional y se encuentra sometido a las revisiones de control que este organismo considere necesarias.

8.1. Frecuencia de la auditoría de conformidad

ITSS lleva a cabo una auditoría de conformidad anualmente.

8.2. Identificación y calificación del auditor

Las auditorías son realizadas por el personal designado por el Organismo Superior Nacional y/o 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.

8.3. 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 ITSS.

8.4. Listado de elementos objeto de auditoría

La auditoría verifica respecto a ITSS:

a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
b) Que la entidad cumple con los requerimientos de la Declaración de Prácticas de Almacenamiento y Conservación; y otra documentación vinculada con los Servicios de Almacenamiento y Conservación.

c) Que la Declaración de Prácticas de Almacenamiento y Conservación y demás documentación jurídica vinculada, se ajusta a lo acordado por ITSS y con lo establecido en la normativa vigente.
d) Que la entidad gestiona de forma adecuada sus sistemas de información.

En particular, los elementos objeto de auditoría serán los siguientes:

a) Procesos del PSADE para el Almacenamiento y Conservación de documentos electrónico y elementos relacionados.
b) Sistemas de información.
c) Protección del centro de proceso de datos.
d) Documentos.

8.5. 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 solventen dichas deficiencias.

Si ITSS 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, se aplicará lo establecido en el Plan de cese.

9. Términos y condiciones del servicio

ITSS pone a disposición de los Suscriptores del servicio esta Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos, que incluye los términos y condiciones de los Servicios de Almacenamiento y Conservación de ITSS.

Esta DPAC, así como demás documentos importantes para la prestación del servicio, se encuentran permanentemente disponibles en: https://itss.sv/politicas-practicas.

9.1. Contratación del servicio

La contratación de los Servicios de Almacenamiento y Conservación de ITSS requieren la suscripción del contrato de prestación de servicios de almacenamiento y conservación, por el que el Suscriptor acepta, entre otras previsiones, el sometimiento a la presente DPAC y términos y condiciones.

El contrato de prestación de servicios de almacenamiento y conservación indicará el servicio escogido por el suscriptor, así como la modalidad del servicio de preservación de larga duración.

9.2. Disponibilidad del servicio

Los Servicios de Almacenamiento y Conservación de ITSS se encuentran disponibles las 24 horas del día los 7 días de la semana. En este sentido, se entiende por disponibilidad del servicio, como la capacidad que tiene el Suscriptor de acceder a los Servicios de Almacenamiento y Conservación una vez contratados.

No obstante lo anterior, ITSS pone a disposición de los Suscriptores un Acuerdo de Nivel de Servicio (SLA), por el que se compromete a mantener un nivel de disponibilidad de: 99,90%.

9.3. Modelo de prestación del servicio

ITSS ha implementado un modelo de prestación de servicio conforme lo descrito en esta Declaración de Prácticas de Almacenamiento y Conservación.

En este sentido y con el fin de dar cumplimiento a lo establecido en los estándares técnicos de referencia, ITSS declara que:

- Los servicios de almacenamiento y conservación tienen como objetivo el almacenamiento de documentos electrónicos y la Preservación de datos a Largo Plazo.

- En el supuesto que el servicio no sea capaz de recibir, recopilar y/o validar la documentación enviada al servicio por el Suscriptor, se informará oportunamente de que no ha sido posible tramitar el solicitud. La notificación se realizará a través de los medios de comunicación aportados por el Suscriptor, ya sea en la contratación como en el alta del servicio, como norma general por correo electrónico.

- De conformidad con lo establecido en el servicio de conservación, el suscriptor que lo desee podrá solicitar a ITSS la importación y/o exportación de sus documentos conforme lo estipulado DPAC.

- Ante la terminación del servicio de conservación, independientemente de la causa, ITSS procederá a la devolución toda la documentación electrónica custodiada. Para ello, realizará la exportación de la documentación electrónica y sus evidencias y acordará con el Suscriptor su puesta en disposición.

- Toda la información relativa a los servicios está disponible en: https://itss.sv/politicas-practicas.

9.4. Tarifas

Las tarifas y condiciones económicas a satisfacer por los Servicios de Almacenamiento y Conservación de ITSS, se establecerán de acuerdo a las condiciones particulares de las partes. En cualquier caso, se informará al Suscriptor con carácter previo a la contratación de los servicios.

9.5. Capacidad financiera

ITSS 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, en relación con la gestión de la finalización de los servicios y plan de cese.

9.6. Cobertura de seguro

ITSS 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.

9.7. Confidencialidad

9.7.1. Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por ITSS:

- Solicitudes de Servicios de Almacenamiento y Conservación, así como toda otra información personal obtenida para la prestación del servicio.
- Documentos electrónicos y evidencias generadas y/o almacenadas por el PSADE.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por el PSADE y sus auditores.

- 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”.

9.7.2. Divulgación legal de información

ITSS divulga la información confidencial únicamente en los casos legalmente previstos y de conformidad con las medidas, controles y procedimientos identificados en esta Declaración de Prácticas de Almacenamiento y Conservación.

9.8. Protección de datos personales

ITSS garantiza el cumplimiento de la normativa vigente en materia de protección de datos personales especialmente en lo referente al artículo 5 de la L ey de Firma Electrónica de El Salvador.

En cumplimiento de esta, ITSS ha documentado en esta Declaración de Prácticas de Almacenamiento y Conservación 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 la política de privacidad aplicable a todos los Servicios de Almacenamiento y Conservación de ITSS en el que se detalla toda la información necesaria con respecto al tratamiento de datos personales realizado por ITSS:

Responsable del tratamiento

IT Security Services, Sociedad Anónima de Capital Variable
Dirección fiscal: 89 Avenida Norte y Calle El Mirador Colonia Escaló, Edificio WTC, Torre I, Piso 2, Local 201-A, Colonia Escalón, San Salvador. Código postal 1101
NIT: 0623-290424-104-0
NRC: 343908-4

Finalidad del tratamiento

ITSS trata los datos de carácter personal facilitados para llevar a cabo los servicios electrónicos solicitados, concretamente: (i) almacenamiento de documentos electrónicos y Preservación de datos a Largo Plazo, todo ello de acuerdo con lo previsto en la Declaración de Prácticas de Almacenamiento y Conservación de ITSS, la cual se encuentra disponible en el siguiente enlace: https://itss.sv/politicas-practicas.

Las finalidades de tratamiento de datos relativos a los servicios de ITSS son las siguientes:

- Identificación de los suscriptores de los servicios.
- Prestación de los Servicios de Almacenamiento y Conservación.
- Comunicaciones relativas al servicio.
- Gestión administrativa, contable y de facturación derivada de la contratación.

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

Los datos serán obtenidos directamente de los Suscriptores del servicio.

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 de datos personales para la Prestación de Servicios de Almacenamiento y Conservación, se basa en la ejecución de un contrato de los servicios solicitados, donde el usuario es parte del mismo.
- La legitimación del tratamiento para atender las consultas y solicitudes se basa en el consentimiento del interesado, el cual lo presta expresa e inequívocamente, mediante acción positiva y previa al envío, al aceptar las condiciones y la política de privacidad. Dicho consentimiento puede ser retirado en cualquier momento mediante el envío de un correo electrónico a comercial@it-securityservices.com.

Datos tratados y conservación

Las categorías de datos personales tratados por ITSS, a título enunciativo pero no limitativo, comprenden:

- Datos identificativos: nombre, apellidos y número oficial de identidad.
- Datos profesionales: organización, departamento y/o cargo.

- Datos de contacto: dirección postal, correo electrónico y número de teléfono.

Los datos personales se conservarán hasta la finalización de la relación contractual y posteriormente, durante los plazos legalmente exigidos acorde a cada caso. Como norma general, los datos personales relativos a los Servicios de Almacenamiento y Conservación se conservarán durante 15 años desde la finalización del servicio.

Transferencia de datos

Como norma general los datos personales únicamente se cederán a terceros bajo obligación legal.

Derechos de los usuarios

Los usuarios podrán ejercitar sus derechos de confirmación, acceso, rectificación, supresión, cancelación, limitación, oposición y portabilidad.

- Confirmación. Todos los usuarios tienen derecho a obtener confirmación sobre si ITSS está tratando datos personales que les conciernan.
- 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 y 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 ITSS obligada a dejar de tratarlos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

Para ejercer sus derechos, los usuarios pueden enviar una petición a la dirección de correo electrónico comercial@it-securityservices.com o bien dirigir un escrito a la dirección indicada en el apartado de información del Responsable del tratamiento. En dicha petición, deberán adjuntar copia de su documento de identidad e indicar claramente cuál es el derecho que se desea ejercer.

9.9. Derechos de propiedad intelectual

Los derechos de propiedad industrial e intelectual relativos a los Servicios de Almacenamiento y Conservación, de manera enunciativa pero no limitativa, textos, fotografías, imágenes, marcas, código fuente, diseño, estructura, bases de datos y en general toda la información y elementos contenidos en la mismo son titularidad de ITSS, a quienes corresponde el ejercicio exclusivo de los derechos de explotación de los mismos en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación.

La firma del contrato de prestación de servicios no implica, en modo alguno, directa o indirectamente, transmisión, cesión, licencia y en general derecho alguno respecto de los derechos de propiedad industrial e intelectual de los que es titular ITSS.

9.10. Obligaciones de los participantes

9.10.1. Obligaciones de ITSS

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

De manera orientativa, pero no limitativa, ITSS se obliga a:

- Prestar los Servicios de Almacenamiento y Conservación conforme con esta Declaración de Prácticas de Almacenamiento y Conservación.
- Informar al Suscriptor de los términos y condiciones relativos al uso de los Servicios de Almacenamiento y Conservación, de su precio y de sus limitaciones de uso, todo ello mediante un contrato de prestación de servicios con el Suscriptor.
- Monitorizar el estado de la técnica criptográfica.
- Utilizar certificados electrónicos de un Prestador de Servicios de Certificación confiable.
- Utilizar servicios de sellado de tiempo de un Prestador de Servicios de Certificación confiable.

- Garantizar procedimientos para generar y salvaguardar los documentos electrónicos en las tareas mencionadas, garantizando su resguardo contra pérdida, daño o manipulación indebida.
- Garantizar la confidencialidad de los documentos electrónicos gestionados por el servicio.
- Mantener, actualizar y publicar la versión actual y vigente del presente documento.

9.10.2. Obligaciones de los Suscriptores

Los Suscriptores de los Servicios de Almacenamiento y Conservación de ITSS, deberá cumplir con la siguientes obligaciones:

- Utilizar el Servicio de acuerdo con su finalidad y si los hubiese, las instrucciones y/o documentos indicados por ITSS.
- Respetar con lo dispuesto en esta Declaración de Prácticas de Almacenamiento y conservación, términos y condiciones y contrato de prestación de servicios.
- Enviar los documentos electrónicos y objeto de datos conforme los formatos y requisitos exigidos por el servicio.
- Asegurar el cumplimiento legal y exactitud de los documentos electrónicos y/u objetos de datos enviados al servicio de ITSS.
- No copiar, realizar ingeniería inversa, desarmar, descompilar, cambiar, modificar o de otra manera intentar investigar, manipular y/o descubrir el código fuente, marco estructural y/o los principios en que se basa el servicio, así como cualquier acción que pueda comprometer la integridad respecto del servicio o cualquier software, documentación o información relacionada con el mismo.
- Asumir la responsabilidad de los daños y perjuicios ocasionados a terceros que resulten de cualquier inexactitud, error u omisión del funcionamiento incorrecto o negligente del servicio por parte del Suscriptor.
- Salvaguardar y utilizar correctamente las credenciales de acceso al servicio.

9.10.3. Obligaciones del tercero que confía

ITSS informa al tercero que confía, que para validar la documentación electrónica procesada por los servicios de almacenamiento y/o conservación, debe asumir las siguientes obligaciones:

- Verificar el documento electrónico, esto es verificar la validez, suspensión o revocación de los certificados electrónicos y sellado de tiempo utilizados en el documento electrónico.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de ITSS, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de ITSS.

9.11. Responsabilidades y garantías

9.11.1. Rechazo de otras garantías

ITSS rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección anterior.

9.11.2. Limitación de responsabilidades

ITSS limita su responsabilidad a la prestación de Servicios de Almacenamiento y Conservación.

ITSS no asumirá ningún tipo de responsabilidad en caso de:

- Uso fraudulento, negligente, doloso o abusivo de los Servicios de Almacenamiento y Conservación por parte del Suscriptor.
- Falta de veracidad o autenticidad de la información o documentos gestionados a través del servicio.
- Funcionamiento incorrecto de los servicios, por causas no imputables a ITSS, por fuerza mayor o caso fortuito, así como por mantenimientos programados.
- Pérdida, destrucción y/o extravío de la documentación electrónica durante su conservación, una vez entregada al Suscriptor.
- Ataques y/o daños causados por terceros que afecten al servicio, siempre y cuando se hubiera aplicado la diligencia debida conforme lo estipulado en las políticas y prácticas de seguridad aplicables.

9.11.3. Caso fortuito y fuerza mayor

ITSS no será responsable en ningún caso bajo situaciones que incurran en caso fortuito y en caso de fuerza mayor.

Se entiende por caso fortuito como aquella situación o suceso que sea imposible de prever, o que, previsto, sea inevitable respecto de su mitigación. Adicionalmente, se entiende por fuerza mayor aquellas situación o suceso que es inevitable de hacer efectivas sus circunstancias, imprevisible y extraordinario en su origen, emanante de un ámbito ajeno e irresistible.

Por ello, ITSS no será responsable bajo ningún concepto en situación de guerra, desastres naturales, funcionamiento disfuncional de servicios eléctricos, redes o infraestructura informática, por causa no imputable a ITSS.

9.12. Aspectos legales

9.12.1. Normativa aplicable

ITSS establece, en el presente documento y en el contrato de suscriptor, que la ley aplicable a la prestación de los Servicios de Almacenamiento y Conservación es la Ley salvadoreña.

Sin perjuicio de lo anterior, dentro de las principales normas de aplicación directa a los servicios de almacenamiento y conservación, ITSS declara su especial atención al cumplimiento de la normativa aplicable siguiente:

- Ley de Firma Electrónica (Decreto Legislativo No 133).
- Reglamento de la Ley de Firma Electrónica (Decreto Legislativo No 60).
- Reglamento técnico Salvadoreño (RTS) 35.01.02:21. Para la Prestación de Servicios de Almacenamiento de Documentos electrónicos.
- ETSI EN 319 401. Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

- ETSI TS 102 573. Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objects.
- ETSI TS 119 511. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.
- ETSI TS 119 512. Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services.

9.12.2. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

ITSS establece, en el contrato de suscriptor, y en el presente documento, 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, el PSADE vela porque, al menos los requisitos contenidos en: 9.7 Confidencialidad, 9.8 Protección de datos personales, 9.10 Obligaciones de los participantes y 9.11 Responsabilidad y garantías , continúen vigentes tras la terminación del servicio.
- 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, las comunicaciones relativas a los Servicios se realizarán por los medios indicados en el contrato y en su defecto por lo identificado en el apartado 1.6 del presente documento.

9.12.3. Cláusula de jurisdicción competente

ITSS establece, en el contrato de suscriptor y en el presente documento, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces salvadoreños.

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.

9.12.4. Resolución de conflictos

ITSS establece, en el contrato de suscriptor, y en el presente documento, los procedimientos de mediación y resolución de conflictos aplicables.

Las Partes tratarán de resolver mediante mutuo acuerdo cualquier disconformidad acerca de la ejecución o interpretación de las disposiciones contenidas en este documento y/o contrato de prestación de servicio. Para ello, ITSS dispone de un procedimiento de gestión de disputas.

No obstante lo anterior, en caso de no llegar a un acuerdo, los casos se someterán a la jurisdicción de los Juzgados y Tribunales de El Salvador, con renuncia expresa a cualquier otro fuero o jurisdicción que les pudiese corresponder.

Anexo I - Acrónimos

AdES	Firma electrónica avanzada
AIP	Paquete de Conservación (AIP - Archival Information Package)
API	Application programming interface
AUG	Augmentation
AWS	Amazon Web Services
C.V	Capital Variable
CA	Entidad / Autoridad de Certificación
CRL	Listas de Revocación de Certificados
DIP	Paquetes de Consulta (DIP - Dissemination Information Packages)
DPAC	Declaración de Prácticas de Almacenamiento y Conservación de Documentos Electrónicos
DPC	Declaración de Practicas de Certificación
ETSI	Instituto Europeo de Normas de Telecomunicaciones
IETF	Grupo de Trabajo de Ingeniería de Internet
ISO	Organización Internacional de Normalización
NIT	Número de Identificación Tributaria
NRC	Número de Registro
OAIS	Open Archival Information System
OCSP	Protocolo de Verificación de Certificados en Línea
OID	Identificador de Objeto Único
PC	Política de Certificación
PDF	Portable Document Format
PGD	Preservación general de datos
PSADE	Proveedor del Servicio de Almacenamiento de Documentos Electrónicos
RFC	Request for Comments
RIP	Paquetes de Revisión (RIP - Revision Information Package)
S.A	Sociedad Anónima
SHA	Secure Hash Algorithm
SIP	Paquete de Depósito (SIP - Submission Information Package)
SLA	Service Level Agreement
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TSA	Autoridad de Sellado de Tiempo

VPN	Red privada virtual
WST	Servicio de preservación con conservación