DECLARACIÓN DE PRÁCTICAS DE CONSERVACIÓN DE FIRMAS YSELLOS ELECTRÓNICOS

TrustCloud

TIPO DE DOCUMENTO				
				Documentación Secreta
			x	Documentación Pública
				Documentación Interna
				Documentación Confidencial
TÍTULO			DECLARACIÓN DE PRÁCTICAS DE CONSERVACIONDE FIRMAS Y SELLOS ELECTRÓNICOS	
ENTIDAD			TRUSTCLOUD TECH S.L.	
FORMATO			Electrónico - PDF	
PÁGINAS			35	
VERSIÓN	**FECHA DE EMISIÓN**	**OID**	**AUTOR**	
04	24/10/2024	1.3.6.1.4.1.62143.1.1.1	TRUSTCLOUD	
Revisado por: Alberto Angón (CISO-RSI) Firmado electrónicamente por ALBERTO ANGON ROBLES el 2024-11-15 14:03:07 CET			Fecha:	
Aprobado por: Comité de Dirección TRUSTCLOUD Firmado electrónicamente por ALBERTO ANGON ROBLES el 2024-11-15 14:03:08 CET			Fecha:	

HISTORIAL DE MODIFICACIONES

Versión	Fecha	Descripción de la acción	Páginas
01	09/01/2024	Primera version del documento.	
02	22/05/2024	Corrección hallazgos STAGE 1 auditoría. Modificación apartados 4 y 9.2.	
03	17/10/2024	Alinear la documentación de acuerdo con lo previsto en el artículo 24.2.a del Reglamento (UE) nº 910/2014	
04	24/10/2024	Prestadores cualificados de servicios de confianza informarán al organismo de supervisión con una antelación de al menos tres meses en caso de que tengan intención de cesar tales actividades	

Índice

1 INTRODUCCIÓN

El presente documento es una Declaración de Prácticas del Servicio de Conservación de firmas y sellos electrónicos, mediante el cual TRUSTCLOUD TECH S.L., como prestador de servicios de confianza, expone y describe la forma en que presta el servicio de conservación de firmas electrónicas cualificadas y sellos electrónicos cualificados y asegura el cumplimiento de las obligaciones legalmente exigibles, informandoal público sobre el modo correcto de utilización de estos servicios.

Esta Declaración de Prácticas está dirigida a todas las personas físicas y jurídicas solicitantes, subscriptores y en general usuarios de los servicios de custodia, de conformidad con lo establecido enla Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y el Reglamento 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva1999/93/CE.

A tal efecto, TRUSTCLOUD ha implementado un sistema de gestión de seguridad de la información aplicado a la información e infraestructuras que soportan los servicios de diseño, desarrollo y mantenimiento de aplicaciones, sistemas informáticos, servicios de cloud profesional y proveedor integral de servicios de confianza, consiguiendo su certificación en ISO/IEC 27001, con el objetivo de desarrollar e implantar eficazmente sus servicios

Además, para el servicio de custodia de firmas electrónicas y sellos electrónicos, TRUSTCLOUD siguelas indicaciones de los estándares del Instituto Europeo de Estándares de Telecomunicaciones -ETSI- guiándose para ello por las especificaciones técnicas de las normas ETSI TS 119 511, EN 319 401 (requerimientos generales para proveedores de servicios de confianza), EN 319-102-1 (procedimientode creación y validación de AdES firma digital), TS 101 533-1 (estándar europeo para el sistema de conservación) e ISO 14641-1 (especificaciones para el diseño y funcionamiento de un sistema de información para la preservación de la información digital). NOM-151 (Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos)

A tal efecto, TRUSTCLOUD ha llevado a cabo el diseño y desarrollo de una infraestructura tecnológicaque, de forma integrada, pone a disposición de sus Usuarios una herramienta a través de la que poderconservar longevamente las firmas y sellos electrónicos cualificados, y resellarlos periódicamente, de modo que se garantice la eficacia jurídica probatoria suficiente durante toda la vigencia de la custodia.

2 IDENTIFICACIÓN DEL DOCUMENTO

Con el objeto de identificar de forma individual cada tipo de servicio realizado por TRUSTCLOUD, de acuerdo con la presente Declaración de Prácticas de Conservación de firmas y sellos electrónicos cualificados, se asignan a cada tipo un identificador de objeto (OID).

La presente Declaración de Prácticas de Certificación describe los servicios relacionados con la conservación de firmas y sellos electrónicos cualificados prestados a través de la plataforma titularidadde TRUSTCLOUD, incluyendo entre otros aspectos de la descripción y funcionalidad de los servicios prestados los siguientes:

- Las características de cada servicio.
- Los flujos de tratamiento y operación.
- La identificación de todos los intervinientes, desde los aportantes de documentación para custodiar demanera cualificada, hasta los prestadores de servicios de certificación encargados de la generación de sellos de tiempo

y firmas electrónicas.
- Las obligaciones asumidas en la prestación de los servicios.
- Las medidas de seguridad técnicas y organizativas implantadas.
- Las condiciones generales de uso y contratación de los servicios.

3 ACRONIMOS Y DEFINICIONES

Acrónimos

ACRÓNIMO	DEFINICIÓN
LSC	Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
eIDAS	Reglamento 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
RGPD	Reglamento 2016/679, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE
LSSI	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
PCSC	Prestadores de Servicios de Certificación
TSA	Time Stamp Authority – Autoridad de Sellado de Tiempo
CPD	Centro de Procesamiento de Datos
NTP	Network Time Protocol – Protocolo de Internet para sincronizar los relojes delos sistemas informáticos.
PKI	Public Key Infraestructure – Infraestructura de Clave Pública
WF	Work Flow – Flujos de trabajo de cada proceso
CRL	Certificate Revocation List
OID	Object Identifier - Valor, de naturaleza jerárquica y comprensivo de una secuencia de componentes variables, aunque siempre constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto de OID

Definiciones

CONCEPTO	DEFINICIÓN
DPC	**Declaración de Prácticas de Certificación**: Declaración de Trustcloud puesta a disposición del público por vía electrónica y de forma gratuitarealizada en calidad de Prestador de Servicios de Confianza en cumplimientode lo dispuesto por la Ley.
PRESTADOR DE SERVICIOS DE CONFIANZA	Persona física o jurídica que presta uno o más servicios de confianza, de conformidad con lo establecido en el eIDAS
PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA	Prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación.
AUTORIDAD DE SELLADO DE TIEMPO	persona física o jurídica que, de conformidad con la normativa sobre Selladode Tiempo expide Sellos de tiempo electrónicos.
SELLO DE TIEMPO ELECTRÓNICO	Datos en formato electrónico que vinculan otros datos en formato electrónicocon un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.
SELLO DE TIEMPO ELECTRÓNICO CUALIFICADO	Sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42 del eIDAS.
USUARIO	Persona física o jurídica que utiliza los servicios de custodia cualificada de firmas o sellos electrónicos cualificados, previa aceptación de las condiciones asociadas al servicio y las DPC.
DOCUMENTACIÓN	Conjunto de evidencias digitales recibidas por Trustcloud por parte del Usuario, que cumplen con los requisitos establecidos en las presentes DPC.
CERTIFICADO	Fichero firmado electrónicamente por un prestador de servicios decertificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
CLAVE PÚBLICA	Valor matemático conocido públicamente y usado para la verificación de unafirma digital o el cifrado de datos. También llamada datos de verificación de firma.
CLAVE PRIVADA	Valor matemático conocido únicamente por el suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada datosde creación de firma.

FUNCIÓN HASH	Operación que se realiza sobre un conjunto de datos de cualquier tamaño, deforma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado.
HASH O HUELLA DIGITAL	Resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.
PAQUETE DE EXPORTACIÓN-IMPORTACIÓN	Información extraída del servicio de preservación que incluye el objeto de datos de presentación (SubDO), las pruebas de preservación y los metadatosrelacionados con la preservación, lo que permite que otro servicio de preservación lo importe para seguir alcanzando el objetivo de preservación basado en esta información

4 NORMAS Y ESTANDARES DE APLICACIÓN

1] Reglamento 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
[2] Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
[3] Reglamento 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se derogala Directiva 95/46/CE
[4] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
[5] ETSI TS 119 511 V1.1.1 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.
[6] ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers
[7] ETSI EN 319 102-1 v1.1.1 Procedures for Creation and Validation of AdES Digital Signatures: Creation and Validation
[8] ETSI TS 102 778-6 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles

[9] ETSI TS 101 533-1 Information Preservation Systems Security; Part 1: Requirements for Implementation and Management
[10] ETSI EN 319 421 v1.0.0 Electronic Signatures and Infrastructures (ESI); Policy and SecurityRequirements for Trust Service Providers issuing Time-Stamps
[11] ISO/IEC 14641-1 Electronic archiving
[12] ISO/IEC 27001:2022 Information security, cybersecurity, and privacy protection — Information security management systems
[13] ISO/IEC 27002;2022 Information security, cybersecurity, and privacy protection — Information security controls
[14] ETSI SR 019 510. Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures.

5 REQUERIMIENTOS DE CONFORMIDAD

TRUSTCLOUD garantiza, en línea con su declaración de aplicabilidad y con los requisitos legales, que cumple con:

1) La Política de seguridad de la información, que está alineada con la regulación jurídica aplicable.
2) La Política de servicio de conservación de firmas y sellos electrónicos cualificados definida en estaDeclaración de Prácticas de Certificación.
3) Los requerimientos organizativos definidos en el punto 8.1.1.
4) Las Obligación de facilitar la información requerida, cuando sea necesaria, a sus socios comerciales, auditores y autoridades reguladoras, tal y como se especifica en los puntos 8.1.2 y 8.1.3. del presente documento, incluyendo los requisitos organizativos.
5) Que Trustcloud ha implementado los controles que cumplen con los requerimientos especificados en el anexo A de la norma ETSI TS 119 511 [5], garantizado por la implantación de un SGSI basado en la norma ISO/IEC 27001:2022, como proveedor de servicios de confianza.
6) Que Trustcloud tiene en cuenta los requisitos legales necesarios para el uso de firmas y sellos electrónicos cualificados que empleen dispositivos seguros de creación de firma.

6 DATOS DE IDENTIFICACIÓN Y CONTACTO

- Razón Social: TRUSTCLOUD TECH S.L.
- Denominación Comercial: TRUSTCLOUD
- CIF: B67693655
- Domicilio Social: CALLE BUENOS AIRES, 12. 48001 BILBAO
- Servicio de Atención al Cliente (SAC): +34 913 518 558
- Correo electrónico: contact@trustcloud.tech
- Web: https://trustcloud.tech/es/
- Otros datos de contacto: +34 913 518 558

7 DESCRIPCIÓN DEL SERVICIO

TRUSTCLOUD, como prestador de servicios de confianza, ofrece un servicio cualificado de conservación de firmasy sellos electrónicos cualificados, por el que realiza la conservación de las citadas firmas y sellos electrónicos cualificados mediante la utilización de procedimientos y tecnologías capaces de ampliar la fiabilidad de los datos de la firma electrónica cualificada, más allá del período de validez del certificado electrónico

7.1 PARTES INTERVINIENTES EN LOS SERVICIOS DE TRUSTCLOUD

Las partes intervinientes en los servicios de TRUSTCLOUD son:

Usuarios del servicio:

Los usuarios de los servicios son las personas físicas y jurídicas a las que van destinados los servicios de conservación de firmas y sellos electrónicos, que quieran preservar las firmas y sellos electrónicos cualificados alargo plazo, garantizando la integridad, autenticidad y su legalidad a lo largo del tiempo.

Almacén de Custodia:

Almacén y Base de datos SQL donde se almacenan las Declaraciones firmadas y selladas, perfectamente clasificadas.

Prestador de Servicios de Certificación Cualificado:

Entidad legalmente constituida, y debidamente cualificada por alguna de las autoridades competentes de un país miembro de la UE, cuya actividad principal es la emisión de certificados de firmas y sellos cualificados con el fin de generar firmas y sellos cualificados.

Existen dos clases de políticas relacionadas con la adopción del uso de firma electrónica avanzada, según la norma ETSI TS 101 533 [9]:

1) Requerimientos de Política Normalizado (N), basado en firmas electrónicas avanzadas
2) Requerimientos de Política Extendidos (N+), cuyo uso supone una mayor seguridad al ampliar los requerimientos normalizados con requerimientos para firmas electrónicas cualificadas, exigiendo el uso de formatos AdES emitidos con dispositivos seguros de creación de firma y basado en certificados cualificados.

TRUSTCLOUD exige de los Prestadores de Servicios de Confianza Cualificado, en todo caso, que emplee la política N+ (firmas electrónicas cualificadas) en este servicio.

Autoridad de Sellado de Tiempo Cualificada:

Autoridad que genera certificados de sello de tiempo cualificados con el Hash resumen del fichero, la fecha y la hora obtenidas de una fuente fiable de tiempo, procede a su firma electrónica y se lo proporciona a TRUSTCLOUD,garantizando su existencia y su integridad en el tiempo desde el momento de la realización del sellado.

Del mismo modo, la Autoridad de Sellado de Tiempo Cualificada realizará los procesos de resellado de tiempo delas firmas y sellos electrónicos conservados, realizándose antes de su caducidad, un nuevo sellado electrónico detiempo, con el único fin de garantizar la longevidad de esta, y por tanto la fiabilidad de la firma electrónica a lo largo del tiempo.

Otros prestadores de servicios:

TRUSTCLOUD cuenta con los servicios de prestadores de servicio de almacenamiento Cloud para la conservación.

La descripción de la intervención en los diferentes procesos, en los que intervienen los prestadores de servicios anteriormente citados, está reflejada en la presente DPC.

7.2 CARACTERÍSTICAS PRINCIPALES DE LOS SERVICIOS DE TRUSTCLOUD

Mediante el servicio prestado por TRUSTCLOUD, se garantizan los siguientes aspectos

1) Que los ficheros que se reciben por parte del Usuario se encuentran, en todo caso, en formato PAdES.

2) Que las firmas y sellos electrónicos conservados son cualificados, de tal forma que cumple con los siguientes requisitos:

✓ Han sido realizados mediante un certificado electrónico cualificado de firma o sello, emitido bajo una Política de Certificación de certificados electrónicos cualificados.

✓ Que han sido generados, en todo caso, en un dispositivo seguro de creación de firmas.

3) Que las firmas y sellos cualificados conservados cumplen con los requisitos de longevidad, ampliándosela fiabilidad de los datos de la firma o sello electrónico cualificado, utilizados más allá del período de validez del certificado electrónico con el que se realiza la firma.

7.3 SERVICIO DE CONSERVACIÓN DE FIRMAS Y SELLOS ELECTRÓNICOS CUALIFICADOS

El servicio de conservación de firmas y sellos electrónicos consiste en una solución orientada a garantizar la integridad y validez jurídica de los archivos incorporados a la misma. Todo el proceso se realiza de acuerdo con las directrices del servicio cualificado de conservación de firmas y sellos electrónicos cualificados.

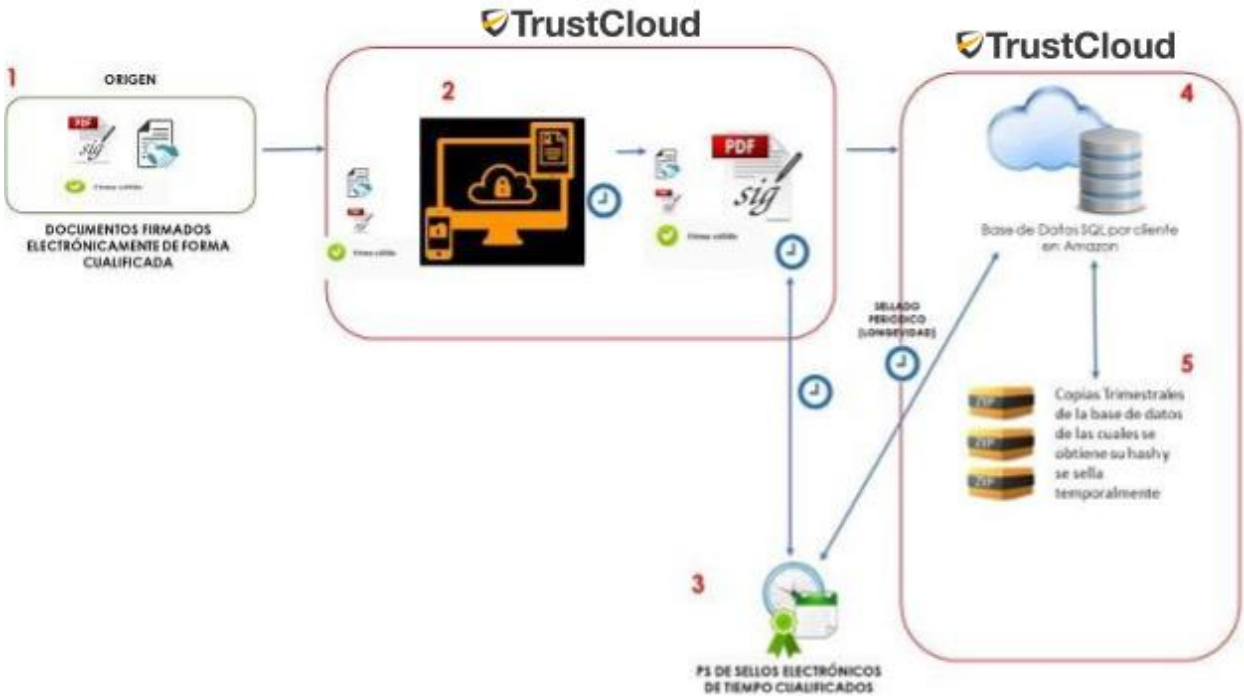
Mediante este servicio se conservan únicamente las firmas y sellos electrónicos de los ficheros (recepción, revisiones y grabación de las firmas y los sellos electrónicos de cada fichero, registro de operaciones para garantizar su integridad, autenticidad y confidencialidad a lo largo del tiempo), mientras que el almacenamientoy la preservación de los ficheros electrónicos asociados a estas firmas y sellos, queda bajo la responsabilidad dela, entidad generadora de las firmas y sellos cualificados.

El procedimiento del servicio de conservación de firmas y sellos cualificados electrónicos de TRUSTCLOUD es el siguiente:

1. El Usuario remite a la plataforma “TRUSTCLOUD” de TRUSTCLOUD los ficheros electrónicos en formato PAdES, cuya integridad y autenticidad desea preservar.
2. El sistema procede a verificar que los mismos se encuentran en formato PAdES.
3. El sistema verifica que los ficheros se encuentran firmados o sellados electrónicamente y si la firma o sello de estos es cualificada.
4. En caso de confirmarse, el sistema procede a añadirle un sello de tiempo cualificado emitido por un prestador de servicios cualificado para este servicio y la correspondiente firma electrónica.
5. El fichero resultante, debidamente firmado y sellado temporalmente de forma cualificada se guarda enel almacén y en la Base de Datos SQL del proveedor.
6. A partir de entonces, TRUSTCLOUD realiza la incorporación de los resellados electrónicos de tiempo sobre los ficheros en formato PAdES-LTV conservados, antes de que caduque el certificado de los sellosde tiempo de la firma inicialmente realizada, garantizándose así la integridad de la firma electrónica archivada.
7. Adicionalmente, TRUSTCLOUD realiza copias trimestrales incrementales de la Base de Datos, de las que se

obtiene su hash y se sella con un sello de tiempo cualificado.

El esquema completo del proceso se puede observar en el siguiente diagrama:



A continuación, se procede a detallar los procesos que realizan estas actividades.

7.3.1 ENTRADA DE LA DOCUMENTACIÓN EN EL SISTEMA DE CUSTODIA DE FIRMAS DE TRUSTCLOUD

Una vez formalizada la relación entre TRUSTCLOUD y el emisor de los ficheros firmados/sellados que deben conservarse para la prestación del servicio de conservación de firmas electrónicas, y tras la aceptación de la presente Declaración de Prácticas de Certificación, TRUSTCLOUD facilitará al Usuario unas claves para poder incorporar la documentación y/o objetos digitales asociados en la plataforma de conservación de TRUSTCLOUD ("TRUSTCLOUD"), siendo comprobado por TRUSTCLOUD que las firmas y los sellos recibidos son cualificados.

El servicio de conservación se integra con los sistemas de gestión de sus Usuarios a través de una aplicación web(API. La plataforma "TRUSTCLOUD" debe comprobar que la firma o sello es cualificado al recibir la transferenciadel fichero en el sistema de información;

7.3.2 SELLADO ELECTRÓNICO DE TIEMPO CUALIFICADO

TRUSTCLOUD solicita a la Autoridad de Sellado de Tiempo (TSA) que le emita un sello de tiempo cualificado, de acuerdo con la recomendación ETSI EN 319 421 [10], mediante un resumen de la información a sellar. Esta TSA genera un sello de tiempo que se compone del resumen o hash, la fecha y la hora que se han obtenido de una fuente fiable de tiempo, y su firma electrónica.

TRUSTCLOUD incorpora este sello al fichero, para garantizar que existe en ese momento y su integridad en el tiempo.

7.3.3 BASE DE DATOS SQL POR CLIENTE EN ALOJADA EN PRESTADOR DE SERVICIOS

Una vez ha finalizado el proceso, las firmas y sellos cualificados son almacenados por TRUSTCLOUD en una base de datos SQL de un prestador de servicios cuyos servidores se encuentran alojados en la Unión Europea.

TRUSTCLOUD se ha asegurado de que dicho proveedor establezca las medidas de seguridad oportunas para garantizar la disponibilidad, integridad y confidencialidad de la base de datos y que tenga las certificaciones de calidad que se requieran para almacenar de forma segura firmas y sellos electrónicos cualificados. El proveedor deberá tener implementadas las especificaciones técnicas, de acuerdo con la legislación europea, de acuerdo con estas dos normas:

- ETSI TS 119 511 [5]
- ISO 14641-1 [11]

Esta documentación se mantiene almacenada durante tiempo indefinido en dichos servidores.

Sin perjuicio de ello, se ha previsto un plan de continuidad del servicio en caso de paralización del servicio por parte de TRUSTCLOUD (punto 10 de la presente DPC).

TRUSTCLOUD proporciona un único servicio de conservación con almacenamiento. Los datos que deben ser

almacenados son preservados por TRUSTCLOUD, mientras que las evidencias y los datos preservados son entregados por TRUSTCLOUD al cliente, previa solicitud

TRUSTCLOUD proporciona un único servicio de conservación con almacenamiento. Los datos que deben ser almacenados son preservados por TRUSTCLOUD, mientras que las evidencias y los datos preservadosson entregados por TRUSTCLOUD al cliente, previa solicitud

7.3.4 COPIAS TRIMESTRALES Y SELLADO DE TIEMPO DE LA BASE DE DATOS

Con el objetivo de aumentar la seguridad de la conservación de las declaraciones, trimestralmente se realiza una copia de seguridad incremental de los datos de la base de datos a través de un fichero CSV, sobre el cual se genera un hash mediante la aplicación del algoritmo SHA 256, e incorpora un sello de tiempo por TRUSTCLOUD

8 OBLIGACIONES Y RESPONSABILIDADES

8.1 OBLIGACIONES DE TRUSTCLOUD

TRUSTCLOUD como PCSC se compromete a cumplir una serie de obligaciones detalladas en esta DPC, en elmarco del eIDAS [1], sus disposiciones de desarrollo y otras legislaciones que sean de aplicación.

8.1.1 REQUISITOS ORGANIZATIVOS DE TRUSTCLOUD

- Operar sus infraestructuras de servicios asociados a la firma digital según lo expuesto en esta DECLARACIÓN PRÁCTICAS DE CERTIFICACIÓN.
- Prestar el servicio de conservación de firmas y sellos electrónicos de forma imparcial y objetiva.
- Garantizar la adecuación de sus procesos y servicios a los estándares a los que estos se adhieren.
- Informar al solicitante del servicio de las características de la prestación del servicio, las obligaciones que asume y los límites de responsabilidad
- Proteger de manera fiable todos los datos de sus Usuarios, así como los registros de actividad y auditoriacon los medios que para ello considere más adecuados y durante el periodo de tiempo contemplado según la naturaleza de los datos registrados.
- Procurar la prestación del servicio de conservación de firmas electrónicas de forma diligente e ininterrumpida
- Comunicar a sus Usuarios con la suficiente antelación la no disponibilidad del sistema en caso de realizarprocesos de modificación, mejora o mantenimiento que impliquen una paralización del servicio.
- Notificar con la mayor prontitud a las partes implicadas siempre que se detecte incidencia alguna en elsistema con afectación para las mismas.
- Garantizar que los sistemas de firma digital operen en sincronía con fuentes fiables de tiempo, utilizando para ello una

Autoridad de Sellado de Tiempo cualificada.

- Publicar las versiones más recientes de este documento y otras definiciones de prácticas de otros servicios de manera previa a la aplicación de las condiciones que en ellos se contemple.
- Disponer de un canal de comunicación con Usuarios y terceros para solicitudes, consultas, quejas y reclamaciones.
- Atender las solicitudes, consultas, quejas y reclamaciones de Usuarios y terceros en un plazo razonable
- En caso de recibir una solicitud de un paquete de exportación-importación se gestionaría a nivel contractual donde se elaborará un plan detallado de cómo realizar el proceso asociado
- Dependiendo del método de producción del paquete o paquetes, se le aplicarán las medidas de seguridad necesarias. Por ejemplo: encriptación, password, doble factor etc.
- Los datos obtenidos una vez finalizado el período de transición pactado con el cliente, inicia el período de bloqueo correspondiente y son eliminados a la finalización de este según lo indicado en la legislación en vigor

8.1.2 INFORMACIÓN PARA SOCIOS COMERCIALES

Los socios comerciales que confían en los objetos digitales archivados por TRUSTCLOUD y hacen uso de sus servicios deberán realizar las siguientes acciones

- Verificar la validez, suspensión o revocación de los certificados empleados utilizando la información sobre el estado de revocación (OCSP o CRL's del Prestador de Servicios de Certificación que emitió el certificado), incorporada dentro del propio fichero PAdES-LTA.
- Respetar las medidas de seguridad que indique TRUSTCLOUD para acceder al servicio de conservación de firmas electrónicas y sellos cualificados

8.1.3 INFORMACIÓN PARA AUDITORES Y AUTORIDADES REGULADORAS

TRUSTCLOUD se compromete a comunicar a la Autoridad Pública competente aquella información confidencial o que contenga datos de carácter personal cuando haya sido requerida por la misma y en los supuestos previstos legalmente:

- Notificar a la autoridad de supervisión y control acreditado (SETSI del MINETAD) cualquier modificaciónen la presente Declaración de Prácticas de conservación de firmas electrónicas.

- Notificar a la autoridad competente y a las partes implicadas el cambio en la infraestructura que pueda afectar a la prestación del servicio.

En concreto, TRUSTCLOUD está obligada a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tengan atribuidas, y en el resto de los supuestos previstos en el RGPD / Legislación de protección de datos vigente [3].

TRUSTCLOUD informará a auditores, autoridades reguladoras y fiscales que confían en el servicio de conservación de firmas y sellos electrónicos, que deberán:

- Verificar la validez, suspensión o revocación de los certificados empleados utilizando la información sobre el estado de revocación (OCSP o CRL's del Prestador de Servicios de Certificación que emitió el certificado), incorporada dentro del propio fichero PAdES-LTA.

Respetar las medidas de seguridad que indique TRUSTCLOUD para acceder al servicio de conservación de firmas y sellos electrónicos cualificados

8.2 RESPONSABILIDAD

TRUSTCLOUD como Prestador de Servicios de Confianza se encuentra sujeto al régimen de responsabilidad recogido en el artículo 13 del eIDAS [1], por lo que asumirá las responsabilidades por los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en los términos previstos en la legislación vigente.

TRUSTCLOUD no responderá de los daños y perjuicios ocasionados por el uso indebido del servicio de conservación de firmas y sellos electrónicos cualificados.

TRUSTCLOUD queda eximido de responsabilidad por los daños y perjuicios ocasionados en caso de fuerza mayor, caso fortuito o imprevisibles o que, siendo previsibles no se hayan podido evitar según el estado de la técnica.

Quedan excluidas de las responsabilidades todos los supuestos contemplados por la ley como Limitaciones a la responsabilidad del PCSC.

TRUSTCLOUD no será responsable de los actos u omisiones realizados por el Usuarios, siendo éste quien asumirátodos los daños y perjuicios, directos e indirectos, que se pudieren ocasionar a cualquier persona, propiedad, empresa, servicio público o privado, concretamente por las pérdidas de beneficios, pérdida de información y datos, o los correspondientes daños, como consecuencia de los actos, omisiones o negligencias del Usuarios asícomo de terceros a él ligados, por uso inadecuado, siendo de exclusivo riesgo del Usuarios.

A estos efectos, TRUSTCLOUD ha suscrito un seguro de responsabilidad civil de 3.000.000 € (tres millones de euros) para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar con motivo del incumplimiento por su parte de las obligaciones que impone el Reglamento eIDAS [1]

8.3 OBLIGACIONES DEL SUSCRIPTOR

Por su parte, el suscriptor del Servicio de Preservación de Firmas y Sellos cualificados deberán cumplir con las siguientes obligaciones:

- Los objetos enviados deberán cumplir con los requisitos establecidos en la norma ETSI 119 511
- Deberá asegurar el cumplimiento legal y la exactitud de los objetos a preservar.
- Deberá enviar los objetos de forma precisa y completa, tal y como se establece en elapartado 7.3 de esta DPC.
- Deberá asumir cualquier otra precaución prescrita en el contrato o acuerdo alcanzado.

9 CONTROLES DE SEGURIDAD

TRUSTCLOUD ha desarrollado e implantado un sistema de gestión de seguridad de la información formado por Políticas, Normas, Estándares, Guías y Procedimientos internos mediante los cuales se define el marco de actuación de la seguridad en los sistemas, servicios y procesos de la compañía, con la finalidad de garantizar queen todos los ámbitos de la entidad se alcanzase el máximo nivel de seguridad.

9.1 SEGURIDAD FÍSICA

TRUSTCLOUD garantiza que cumple la normativa aplicable y los principales estándares y buenas prácticas en materia de seguridad física, según se describe en el presente apartado.

En las instalaciones de TRUSTCLOUD se han establecido diferentes perímetros de seguridad con barreras de seguridad y controles de entrada adecuados a las actividades que se desarrollan en cada uno de ellos. Todo ellocon el fin de reducir el riesgo de accesos no autorizados o de daños a los recursos informáticos.

Los sistemas de información de TRUSTCLOUD se encuentran ubicados en zonas con acceso restringido que han sido adecuadamente protegidas mediante los mecanismos de control de acceso físico apropiados. Asimismo, estos sistemas han sido protegidos frente a otro tipo de amenazas del entorno como incendios, inundaciones ocortes en el suministro eléctrico.

Dicha protección se extiende a aquellos sistemas cuya securización física está delegada en algún proveedor. Paraello, han sido firmadas las cláusulas oportunas en los contratos y se establecen los mecanismos de seguimiento necesarios por parte de TRUSTCLOUD. El tratamiento de información fuera de los sistemas de TRUSTCLOUD es debidamente autorizado, una vez que se garantiza el cumplimiento del nivel de seguridad requerido.

TRUSTCLOUD ha implementado igualmente una política de gestión de activos basada en el inventariado y clasificación, almacenamiento y registros de entrada y salida. En la vertiente técnica, se adoptan procedimientosque garanticen que la información contenida en ella está adecuadamente securizada, así como que permitan lareutilización de estos sin que presente riesgos para la información.

Algunas de las medidas adoptadas por TRUSTCLOUD son las siguientes:

• Autenticación y Control de Accesos. Control de acceso al edificio
• Control de acceso a centros de proceso de datos (DataCenter) basado en identificación biométrica de la huella dactilar y autorización centralizada con registro de accesos, tanto de entrada como de salida.
• Las condiciones de temperatura quedan garantizadas por equipos de refrigeración autónomos ubicados dentro del DataCenter que mantienen la temperatura de este dentro de los márgenes establecidos
• Alimentación redundante, dotando de dos líneas de alimentación eléctrica a los racks destinados a albergar los equipos.
• El cableado utilizado en el Data Center es categoría 6,7 y fibra óptica.
• Sistemas de alimentación ininterrumpida. • Detección de incendios, basado en detectores de humo y aspiración
• Climatización continua y adecuada de las zonas CPD con redundancia n+1 en cada zona. • Detectores de humedad en las zonas de CPD y sala eléctrica.
• Se cuenta con un acuerdo con un proveedor de servicios especializado para la custodia de soportes magnéticos,

contando para ello con una sala acorazada anti-sismos.
• Acceso de personas ajenas (visitas) al CPD
• Exposición al agua
• Recuperación de la información

9.2 SEGURIDAD LÓGICA

TRUSTCLOUD utiliza medidas de seguridad lógica comunes a todos los sistemas. Los sistemas específicos utilizados para la prestación del servicio objeto de la presente DPC han sido dotados de un segundo nivel de medidas de seguridad.

Formalmente se han establecido responsabilidades y procedimientos documentados para asegurar la correcta configuración, administración, operación y monitorización de los sistemas de información y comunicaciones de TRUSTCLOUD.

Se ha establecido y definido un procedimiento de gestión de incidencias con el fin de minimizar el impacto ocasionado debido a incidentes de seguridad o fallos en el funcionamiento de los sistemas, que permite una rápida reacción ante las posibles incidencias producidas, así como el establecimiento de medidas correctivas queeviten su repetición.

Se ha establecido igualmente una adecuada segregación de funciones en la asignación de responsabilidades conel objetivo de prevenir un uso no adecuado de los sistemas de información, estableciendo, en los casos en que dicha segregación no sea factible, otros mecanismos de control adecuados que permitan su seguimiento y control.

Se han establecido los procedimientos y controles que prevengan adecuadamente frente a la introducción de software malicioso, garantizando la integridad del software y de la información de TRUSTCLOUD.

Se han establecido medidas de salvaguarda, incluyendo las copias de seguridad necesarias, comprobando periódicamente su validez mediante su restauración, junto a la monitorización permanente de los sistemas, lo que permite garantizar la continuidad de los sistemas, servicios e informaciones de TRUSTCLOUD y los servicios prestados.

La información transmitida por redes de comunicaciones, públicas o privadas, se encuentran adecuadamente protegidas mediante los mecanismos oportunos que garanticen su confidencialidad e integridad. Se han establecido los controles necesarios que impidan la suplantación del emisor, modificación o pérdida de la información transmitida, tanto en las comunicaciones con sistemas situados en las redes internas, como con otros sistemas externos, como aquellas entidades con las que TRUSTCLOUD cuenta en la prestación de sus servicios como parte interviniente en los mismos.

Se han establecido procedimientos que regulan la estrategia de cifrado de la información de TRUSTCLOUD, describiendo las medidas organizativas y técnicas que garanticen la confidencialidad e integridad de la información.

Se establecen igualmente procedimientos que regulan de forma detallada el almacenamiento, manipulación transporte y destrucción de la información sensible tanto en ordenadores portátiles, dispositivos móviles, etc.), como residualmente, en soporte papel, todo ello con la finalidad de mitigar el riesgo de acceso no autorizado, perdida o hurto.

9.2.1 ACCESO A SISTEMAS

El acceso por parte del personal tanto interno como externo a los sistemas de información de TRUSTCLOUD, así como a la información que tratan y almacenan, se regula sobre la base de las necesidades de información y operación de cada usuario, otorgando acceso exclusivamente a aquellas funciones e información que se requieran para el correcto desempeño de su actividad laboral, acorde con su función y/o perfil operacional.

Los responsables del tratamiento de los activos de información serán los responsables de definir los niveles de acceso

a los recursos y autorizar cualquier acceso extraordinario, todo ello de acuerdo con las directrices de lospropietarios de la información, o, en su caso, de los propietarios del proceso o negocio.

Sin prejuicio de precisar un mayor detalle en su aplicación, ni de la delegación formal de funciones, se entiendencomo propietarios del proceso o negocio los responsables de las siguientes posiciones:

- Responsable de Seguridad de la Información (RSI-CISO)
- Responsable Sistemas (RS)

Todos los accesos realizados a los sistemas de información de TRUSTCLOUD por los usuarios llevarán asociado unproceso de identificación, autenticación y autorización, estableciéndose los controles adecuados para que talesprocesos se realicen de forma segura.

A tal efecto, se han diseñado e implantado mecanismos de registro, monitorización de acceso y uso de los sistemas, que permitan conocer la efectividad de las medidas instaladas y detectar posibles incidentes de seguridad.

9.2.2 REFERENCIA A EVENTOS DEL SISTEMA

En relación con los posibles eventos del sistema, teniendo en cuenta la categoría de los servicios prestados, TRUSTCLOUD ha diseñado un sistema de registros y controles que permiten la inspección reactiva entre otros delos siguientes eventos sobre sus sistemas:

- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Intentos exitosos o fracasados de creación, modificación o cancelación de peticiones dentro de los diferentes componentes del sistema.
- Intentos exitosos o fracasados de firma de ficheros.
- Intentos exitosos o fracasados de ficheros de certificación.
- Intentos exitosos o fracasados de intento de envío de comunicaciones.
- Cambios en la configuración del sistema.

9.2.3 GESTIÓN DE REGISTROS

Se mantendrá en todo momento la integridad y disponibilidad de los registros de auditoría, guardando la sincronización de las fuentes de tiempos con todos los sistemas que generen dichos registros, centralizando, siempre que tecnológicamente sea posible, el control y la monitorización de los registros mediante alguna herramienta de gestión.

Los registros de auditoría generados por los sistemas que traten información confidencial se deberán de almacenar según marque la ley, para el resto de los sistemas este tiempo será regulado por los procedimientos oportunos.

Los sistemas de información deberán tener suficiente capacidad para que el almacenamiento de los registros de auditoría no degrade el nivel de servicio.

Cualquier cambio que fuera estrictamente necesario llevar a cabo en relación con la generación de los registros de auditoría deberá estar debidamente autorizado por el responsable de seguridad.

La eliminación de los registros se deberá de realizar por mecanismos que no degrade la confidencialidad de estos.

9.2.3.1 PROTECCIÓN SOBRE LOS REGISTROS

El acceso a los sistemas de archivo y custodia de documentación de TRUSTCLOUD se encuentra restringido exclusivamente al personal autorizado. Así, se ha configurado un sistema de control de accesos, identificación y autenticación de tal manera que se encuentra protegido contra accesos, modificación, borrado u otras manipulaciones no autorizadas.

Los sistemas, soportes y medios que contienen la documentación e información susceptible de archivo y custodia, así como las aplicaciones necesarias para procesar y tratar los datos custodiados son mantenidos y puedan ser accedidos por el período de tiempo establecido en la presente DPC.

9.2.3.2 PERIODO DE RETENCIÓN DE REGISTROS

Los registros anteriormente comentados, incluyendo las evidencias de servicio serán almacenados y retenidos como registros de auditoría generados por el sistema por un periodo mínimo desde la fecha de su creación de un (1) años para los pertenecientes a auditorías diarias, dos (2) años para las mensuales y cuatro (4) años para los de auditorías anuales.

9.2.3.3 REQUERIMIENTOS PARA LAS FUENTES DE TIEMPO

Los certificados, CRLs, y otras entradas de bases de datos de revocación deberán contener información de fechay hora.

Los sistemas de TRUSTCLOUD realizan el registro del instante de tiempo exacto en el que se realizan los registros, utilizando a tal efecto un sello de tiempo emitido por una TSA cualificada para el caso de formar parte de los procesos integrantes de los servicios de conservación de firmas electrónicas cualificados prestados por TRUSTCLOUD.

Todos los sistemas de TRUSTCLOUD sincronizan su instante de tiempo con fuentes fiables de tiempo basadas enel protocolo NTP (Network Time Protocol), auto calibrándose por distintos medios.

9.2.3.4 COPIA DE SEGURIDAD DE REGISTROS

Se realizan copias de seguridad de los ficheros que contienen los registros objeto de retención, que son almacenadas en la nube.

Estas copias de seguridad se realizan sobre todos los componentes del servicio.

9.3 ANÁLISIS DE VULNERABILIDADES

Dado el creciente riesgo de inserción de código malicioso en programas, será obligatorio adoptar unos criterios para colaborar en la protección de los Sistemas de Información contra este tipo de ataques.

El departamento de informática establecerá todas las medidas de índole técnica y organizativa a su alcance paraevitar la entrada y propagación de código malicioso en sus sistemas informáticos.

Entre estas medidas se encuentran, con carácter enunciativo, pero no limitativo, las siguientes:

Los Sistemas de Información de TRUSTCLOUD deberán tener instalado antivirus, cortafuegos, antispyware y filtrado de correo, DLP todos ellos de actualización automatizada, siempre que tecnológicamente los sistemas soporten controles de estos tipos. Disponemos de Defender corporativo, firewall interno SonicWall y firewall gestionado por Movistar para conexión de red de oficina y las medidas de SI de AWS.

- Los sistemas antivirus y de filtrado de correo de TRUSTCLOUD deberán chequear todos los mensajes entrantes y salientes de correo electrónico, así como todos los mensajes internos de sus redes de comunicaciones
- Cuando un correo no cumpliese con los criterios de seguridad definidos en las aplicaciones antivirus y de filtrado de contenidos, el correo no será entregado a su destinatario y será borrado automáticamente. Esta acción se realizará de acuerdo con las debidas garantías legales y de respeto a la intimidad.
- El estado de cualquier dispositivo portátil, independientemente de la forma en que este ha sido obtenido, deberá ser comprobado mediante las herramientas de detección de código malicioso.

TRUSTCLOUD, o un auditor externo con la certificación y conocimiento suficiente efectuará al menos, un análisisanual de vulnerabilidades.

Es responsabilidad de los coordinadores de los equipos de análisis el informar a los responsables del servicio de TRUSTCLOUD, a través del Responsable de Seguridad, de los resultados de los análisis realizados, de cualquier problema que impida la realización de las auditorias, o la entrega de la documentación resultante.

Los análisis de seguridad implican el inicio de las tareas precisas para corregir las vulnerabilidades detectadas y la emisión de un contra-informe.

Las vulnerabilidades encontradas serán detalladas en un documento resultante etiquetado como: "Análisis de vulnerabilidades sobre plataforma TRUSTCLOUD ". Si fuera encontrada alguna vulnerabilidad, el equipo deTRUSTCLOUD las analizará y las categorizará y ponderará según el grado de afectación procediendo a crear una propuesta con contramedidas.

Las contramedidas serán aplicadas en el menor plazo de tiempo posible, notificando a las partes implicadas si existieran entidades perjudicadas por las vulnerabilidades encontradas.

9.4 SEGURIDAD DE PERSONAL

TRUSTCLOUD determinará cuál es el equipo humano y técnico necesario para la prestación de los servicios asegurando las condiciones de calidad y operación requeridas y garantizando el nivel de servicio acordado.

TRUSTCLOUD utilizará todos los medios técnicos y humanos necesarios para la ejecución de los servicios, con la capacidad, cualificación y experiencia adecuada para la prestación de estos.

TRUSTCLOUD se reserva la capacidad de realizar los cambios técnicos y humanos que estime adecuados para mantener la calidad del servicio prestado, sin perjuicio de lo cual, se intentará que los cambios en la prestación del Servicio sean los menores posibles.

TRUSTCLOUD garantiza poner a disposición de su personal los cursos de formación que resultaren necesarios para que la prestación de servicios realice de manera diligente y con el nivel de cualificación adecuado para el desarrollo óptimo del servicio.

Igualmente, serán a cuenta de TRUSTCLOUD la formación que resultare necesaria para que el personal del Usuarioque utilice el servicio contratado. La duración y el número de asistentes serán acordados con el USUARIO.

10 CONTINUIDAD Y PLAN DE CONTINGENCIAS

TRUSTCLOUD ha establecido procesos de gestión de continuidad y disponibilidad de negocio para minimizar el impacto en las funciones y procesos críticos en caso de desastre, de forma que se reduzca el tiempo de indisponibilidad a niveles establecidos previamente. Dichos procesos cuentan con la adecuada combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

Estos procesos se apoyan en un Plan de Continuidad y disponibilidad de Negocio que es probado de forma periódica, manteniéndose actualizado en todo momento. Para ello se evalúa el riesgo ante amenazas y el impacto asociadoocasionado por la ausencia de continuidad de los activos de información que den soporte o estén implicados enlos procesos de negocio de TRUSTCLOUD.

10.1 PLAN DE CONTINUIDAD y DISPONIBILIDAD DE NEGOCIO

La Continuidad de Negocio es la capacidad táctica y estratégica que tiene TRUSTCLOUD para planificar y responderа incidentes e interrupciones del negocio con el fin de continuar con las operaciones críticas del negocio dentrode un nivel de servicio aceptable y asumible por TRUSTCLOUD.

El alcance para el Plan de Continuidad Y Disponibilidad de negocio es el mismo que se ha definido para la implantación del Sistema de Gestión de Seguridad de la Información (SI). Comprende los servicios y procesos de TRUSTCLOUD, de la sede que se sitúa en Madrid, así como los sistemas de información y activos en los que se apoyan: información y datos, software, equipamiento, comunicaciones, elementos auxiliares, soportes de información, personal y local.

En situación de desastre, la protección sobre las personas ostenta la mayor prioridad. Este aspecto no está contemplado en este plan, ya que está únicamente orientado desde el punto de vista tecnológico. Ninguna actividad será considerada hasta que la seguridad y el bienestar de las personas no estén asegurados.

El personal que forma el equipo de recuperación estará familiarizado con las responsabilidades y el contenido contemplado en este Plan.

En caso de una situación de desastre TRUSTCLOUD se pondrá en contacto con el proveedor correspondiente de suministro de material. Si el tiempo de reposición no puede ser asegurado, podrían ser necesarias compras de equipamiento y su almacenamiento en una ubicación alternativa a las instalaciones principales.

Una vez que el Procedimiento de Recuperación ha sido establecido, su mantenimiento es obligatorio. El procesode recuperación es viable únicamente si este documento está actualizado y completo.

TRUSTCLOUD ha previsto un plan financiero que le permita disponer de la suficiente estabilidad financiera y recursos para operar de conformidad con las presentes DPC y dar respuesta a situaciones de contingencia.

10.2 PLAN DE CONTINGENCIAS

TRUSTCLOUD ha establecido un plan de respuesta ante contingencias, en el que se determina la estrategia y tratamiento a dar a las mismas.

Se determinan los servicios y procesos del departamento de informática que resultan más críticos para el negocio. En caso de contingencias graves el servicio será suspendido mientras estas duren, notificando a la mayorbrevedad posible a los usuarios del sistema.

Las contingencias contempladas que pudieran suponer algún tipo de riesgo para la calidad del servicio son:

- Tiempos de respuesta tan elevados que supusieran una clara violación de la política de calidad de servicio.
- Pérdida de sincronismo con las fuentes de tiempo primaria y secundaria.

Las contingencias que pueden suponer un riesgo para la prestación del servicio son:

- Errores en los sistemas de explotación asociados a la prestación del servicio.
- Errores en los sistemas de comunicación asociados a la prestación del servicio.
- Errores que afecten a la prestación del servicio detectado en el software de alguno de los servicios.

Además, se definen los procedimientos para que los equipos reconstituyan las operaciones de TRUSTCLOUD usando datos de respaldo y las copias de respaldo de las llaves.

11 AUDITORIAS DE CONFORMIDAD

11.1 PERFIL AUDITOR

El auditor externo o equipo de auditores externos será seleccionado en el momento de la planificación de cadaauditoria.

Cualquier empresa o persona contratada para realizar una auditoría de seguridad sobre TRUSTCLOUD o algunode sus servicios en concreto deberá cumplir con los siguientes requisitos:

- Adecuada y acreditada capacitación y experiencia en seguridad y procesos de auditoría de sistemasde información.
- Independencia a nivel organizativo de la autoridad de TRUSTCLOUD, para el caso de auditoríasexternas.

El auditor externo o equipo de auditores externos además no deberán tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses con TRUSTCLOUD. Para poder cumplir con la normativa vigente en materia de tratamiento de datos, y si el proceso de auditoria implicara el acceso a los datos de carácter personal, el auditor tendrá la consideración de Encargadode Tratamiento, en virtud de lo previsto en el artículo 28 del RGPD [3].

11.2 CRITERIOS DE AUDITORÍA

Sin perjuicio de verse ampliados por documentos de los servicios particulares ofrecidos por TRUSTCLOUD, en este apartado definiremos el conjunto de las comprobaciones mínimas de la adecuación de los servicios ofertados respecto a lo definido en esta DPC. Los aspectos cubiertos por una auditoria incluirán, pero no estará limitada a:

- Política de seguridad.
- Seguridad física de las instalaciones del servicio auditado.
- Seguridad lógica de los sistemas y servicios de TRUSTCLOUD
- Evaluación tecnológica de los componentes del servicio.
- Administración de los servicios, así como seguridad en la misma.
- La presente DPC y políticas de servicios vigentes.
- Cumplimiento de las exigencias legales aplicables

11.3 FRECUENCIA

Las Auditorías de conformidad y cumplimiento son llevadas a cabo al menos con carácter bianual, salvo que se produjesen cambios relevantes o esenciales en los sistemas y servicios de TRUSTCLOUD, en donde se ejecutarán auditorías de carácter extraordinario.

11.4 PLAN DE ACCIÓN

La identificación de deficiencias en la auditoria dará lugar como medida inmediata a la adopción de medidas correctivas. Las autoridades competentes en la materia según lo definido por la legislación vigente en colaboración con el auditor será la responsable de la determinación de estas

11.5 COMUNICACIÓN DE RESULTADOS

El auditor externo o auditores externos comunicarán los resultados de la auditoria al Responsable de Seguridad de TRUSTCLOUD, así como a los responsables de las distintas áreas en las que se detecten no conformidades, así como en su caso a la autoridad competente según lo determinado en la legislación vigente.

12 POLÍTICA DE CONFIDENCIALIDAD

Existe el deber genérico de confidencialidad respecto a la información que los empleados de TRUSTCLOUD conozcan por razón de su puesto de trabajo. La información considerada como confidencial facilitada a TRUSTCLOUD no será en ningún caso divulgada a terceros salvo que se encuentre amparada en los supuestos derequerimiento de colaboración con las instituciones competentes

Las Partes no estarán sujetas a la obligación de confidencialidad regulada en la presente Cláusula cuando la información confidencial deba ser revelada por imperativo legal o para dar cumplimiento a una orden de naturaleza judicial o administrativa, siempre que notifiquen dicha circunstancia a la Parte a quien pertenece la información confidencial en cuestión.

En este sentido, se considerará información del tipo “confidencial” (sin perjuicio de que otro tipo de información pueda serlo también):

- Planes de continuidad de negocio y de emergencia.
- Información relativa a la operativa de operaciones y mantenimiento del servicio.
- Toda información relativa a las operaciones que lleve a cabo TRUSTCLOUD.
- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a TRUSTCLOUD durante el proceso de registro de los suscriptores de certificados, con la salvedad de lo especificado por la Política de Certificación aplicable y el contrato de certificación.
- La información de negocio suministrada por sus proveedores y otras personas con las que TRUSTCLOUD tiene el deber de guardar secreto establecida legal o convencionalmente.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Toda la información clasificada como "CONFIDENCIAL" o "ESTRICTAMENTE CONFIDENCIAL"

Sin embargo, serán considerados como documentos públicos no confidenciales entre otros los siguientes materiales:

- Declaración de Prácticas de Conservación de Firmas y Sellos Electrónicos Cualificados de TRUSTCLOUD
- Toda aquella información que sea considerada como "Pública"

13 PROTECCIÓN DE DATOS PERSONALES

TRUSTCLOUD tratará aquellos datos de carácter personal necesarios para el desarrollo de su actividad obteniendo la garantía por parte del DPO de la correcta obtención del consentimiento expreso de los firmantes. Este tratamiento se realizará atendiendo a lo establecido el RGPD [3].

Los datos de carácter personal aportados por los Usuarios serán tratados por TRUSTCLOUD en calidad de Encargado de Tratamiento de los datos responsabilidad de terceros en los términos y condiciones previstos en el artículo 28 del RGPD [3]. En este sentido, TRUSTCLOUD se compromete a cumplir las siguientes condiciones:

- El tratamiento de datos que TRUSTCLOUD realizará se limitará a las actuaciones que resulten necesarias para prestar al RESPONSABLE DEL Tratamiento los Servicios contratados.
- En concreto, TRUSTCLOUD se compromete a realizar el tratamiento de los Datos Personales ajustándose a las instrucciones que, en cada momento, le indique el RESPONSABLE DEL FICHERO, así como a lo dispuesto en la normativa que le resulte aplicable en materia de protección de datos personales.
- Asimismo, TRUSTCLOUD se compromete a no realizar ningún otro tratamiento sobre los Datos Personales, ni a aplicar o utilizar los datos con una finalidad distinta a la prestación del Servicio.
- TRUSTCLOUD declara que cumple con las medidas de seguridad definidas en las presentes DPD, siendo estas las que resultan necesarias para garantizar la seguridad de los datos de carácter personal tratadosen el servicio prestado, a los efectos de garantizar la confidencialidad e integridad en función de la naturaleza de los datos, de conformidad con lo establecido en el RGPD [3].

A los efectos de lo previsto en el presente apartado, TRUSTCLOUD, deberá informar a sus empleados de la obligación de secreto y confidencialidad, así como las consecuencias de su incumplimiento, respecto deltratamiento de datos de carácter personal.

TRUSTCLOUD se compromete a guardar bajo su control y custodia los datos personales suministrados por el RESPONSABLE DEL FICHERO a los que acceda con motivo de la prestación del Servicio y a no divulgarlos, transferirlos, o de cualquier otra forma comunicarlos, ni siquiera para su conservación a otras personas.

Una vez cumplida la prestación del servicio objeto del Contrato, TRUSTCLOUD se compromete a destruir o devolver aquella información que contenga datos de carácter personal que haya sido transmitida por elRESPONSABLE DEL FICHERO a TRUSTCLOUD con motivo de la prestación del Servicio

En el caso de que los afectados, cuyos datos se encuentren en ficheros titularidad del RESPONSABLE DEL FICHERO, ejercitasen sus derechos ante TRUSTCLOUD, éste deberá dar traslado de la solicitud de forma inmediataal RESPONSABLE DEL FICHERO y, a no más tardar, dentro del plazo de 3 días laborables a contar desde su recepción, para que el RESPONSABLE DEL FICHERO resuelva debidamente dicha solicitud.

La presente DPC tiene la consideración de documento de referencia para la implantación de las medidas de seguridad técnicas y organizativas, atendiendo a la responsabilidad proactiva de Trustcloud para garantizar elcumplimiento del RGPD [3].

TRUSTCLOUD garantiza el cumplimiento de las obligaciones que le correspondan en virtud de la normativa que leresulte de aplicación en materia de protección de datos personales.

En caso de violación de la seguridad o pérdida de la integridad que suponga un impacto significativo en el servicioprestado o en los datos de carácter personal tratados, TRUSTCLOUD lo notificará en el plazo máximo de 24 horasdesde que se tuviera conocimiento de tal incidente al organismo de supervisión y en caso necesario a la Agencia Española de Protección de datos en cumplimiento del artículo 19.2 del eIDAS [1].

14 TÉRMINOS Y CONDICIONES DEL SERVICIO

14.1 MODELO DE PRESTACIÓN DEL SERVICIO (SOPORTE, DISPONIBILIDAD)

TRUSTCLOUD ha implantado un modelo de prestación de los servicios de conformidad con lo descrito en la presente DPC. Este modelo irá acompañado de un acuerdo de nivel de servicio para medir su realización, así como de un servicio de soporte, que incorporará en términos generales:
En caso de recibir una solicitud de un paquete de exportación- importación se gestionaría a nivel contractual. Lospaquetes de exportación-importación se elaborarán según lo indicado en la ETSI 119 512

TRUSTCLOUD proporciona un servicio de conservación con almacenamiento. Los datos que deben ser almacenadosson preservados por TRUSTCLOUD, mientras que las evidencias y los datos preservados son entregados por TRUSTCLOUD al cliente, previa solicitud

Cuando TRUSTCLOUD no pueda recoger y verificar todos los datos de validación, se enviaría una notificación del fallo y

se archivaría como expediente no cualificado.

El objetivo de preservación asumido por TRUSTCLOUD es la Preservación de firmas digitales (PDS)

TRUSTCLOUD utiliza como registro de pruebas Excel, dentro del cual se especifican los ciclos de pruebas según él caso de uso asociados al servicio de conservación proporcionado por TRUSTCLOUD
Las pruebas se realizan dentro de TrustCloud, almacenadas en base de datos y en la herramienta de logs, las evidencias se conservan en la herramienta de almacenamiento.

Las pruebas se validan utilizando el Digital Signature Service (DSS). El aumento de las pruebas de preservación se consigue con el resellado.

TRUSTCLOUD cuenta con un proveedor de sellado de tiempo y un proveedor de certificados.

TRUSTCLOUD en caso de que el remitente de la preservación desempeñe un papel en el proceso de preservación,se negociará caso a caso a nivel contractual

LOS CRITERIOS QUE SE VAN A UTILIZAR PARA LA ATENCIÓN DE LAS PETICIONES

- El nivel de soporte funcional que se va a proporcionar y disponibilidad del mismo
- El nivel de soporte técnico que se va a proporcionar y disponibilidad del mismo
- El proceso de escalado que se va a seguir a la hora de notificar la ocurrencia de una incidencia
- El sistema de gestión de peticiones para la resolución de incidencias que se va a utilizar
- Los mecanismos de comunicación que se van a emplear para proporcionar el soporte
- Los idiomas disponibles en los que se va a proporcionar el soporte
- El Acuerdo de Nivel de Servicio (ANS) asociado al servicio contendrá:
  - ANS relativos a tiempos de atención y resolución a la hora de resolver las incidencias
  - ANS relativos a la calidad general con la cual se prestan los servicios
  - ANS relativos a la disponibilidad de los servicios
  - ANS relativos al tiempo de aprovisionamiento de servicios nuevo y/o escalables
  - ANS relativos al rendimiento de volúmenes de información
- Cuadro de Mando para la gestión, control y gobierno del servicio.
- Informes estadísticos, operativos y de cumplimiento de ANS.

TRUSTCLOUD, en la medida de lo posible, tratará de garantizar que sus servicios son accesibles a todos aquellos que quisieran subscribirse a los mismos, siempre que acordaran cumplir con sus obligaciones tal y como se establece en estos términos y condiciones.

TRUSTCLOUD en la prestación de los servicios descritos en estas DPC, garantiza que no operará de modo que se produzca algún tipo de discriminación.

14.2 OBLIGACIONES DE SUSCRIPTORES

Las tarifas y condiciones económicas de los diferentes servicios se encuentran disponibles en el documento de "Condiciones Generales de Contratación de TRUSTCLOUD ".

No obstante, TRUSTCLOUD puede establecer marcos contractuales con Usuarios puntuales que particularicenestas condiciones para el escenario de colaboración establecido entre ambas partes.

Las tarifas establecidas por TRUSTCLOUD para el pago por la prestación del servicio se mantendrán en base a

lossiguientes conceptos:

- Cuota mensual por la utilización del Servicio
- Coste por operación de certificación gestionada por la Plataforma: el importe de cada solicitud de operación a la Plataforma.
- Coste por operación de comunicación gestionada por la Plataforma.

En el momento de la contratación, así como previamente o en cualquier otro momento que se precise, si sesolicitan a TRUSTCLOUD estos datos, puede accederse a esta información económica actualizada.

14.3 LIMITACIONES EN EL USO DEL SERVICIO

Los Servicios prestados por TRUSTCLOUD no tienen límite territorial.

14.4 PREVISIONES EN CASO DE TERMINACIÓN DEL SERVICIO

TRUSTCLOUD se compromete a adoptar todas las medidas necesarias para minimizar el impacto que podría sufrirun Usuario o terceras partes intervinientes en el servicio de las presentes DPC, como consecuencia de la paralización o finalización del servicio. En particular, se realizará un mantenimiento periódico y continuo de la información requerida para verificar la efectiva prestación de los servicios prestados por TRUSTCLOUD.

En concreto TRUSTCLOUD cuenta con un procedimiento de plan de terminación del servicio actualizado, en el quese recoge el proceso que llevará a cabo TRUSTCLOUD antes de la terminación del servicio, en concreto en cuantoa portabilidad y cese de actividad

TRUSTCLOUD tiene acuerdos que permitirán cubrir los costes asociados a estos requisitos mínimos en caso de que no tuviera fondos suficientes o se dieran otras razones que impidieran cubrir dichos costes por sí mismo, teniendo en cuenta la normativa vigente en materia concursal.

14.4.1 PORTABILIDAD

TRUSTCLOUD efectuará la transmisión de la documentación que evidencie todo el registro y otro material en su poder que pudiera ser necesario a quien se considere, para poder demostrar la correcta operación del servicio durante un periodo de tiempo razonable según lo dispuesto en la legislación de aplicación vigente.

Los procesos de destrucción de material o traspasos concretos de cada servicio, si estos existieran quedarían definidos en sus definiciones de políticas concretas.

14.4.2 CESE ACTIVIDAD

En caso de cese de su actividad como Prestador de Servicios de Certificación, TRUSTCLOUD realizará, con una antelación mínima de tres meses, las siguientes acciones:

- Informar a todos los suscriptores de sus servicios del cese de la actividad.
- Informar a todas las terceras partes con las que tenga que haya firmado un contrato referente a este servicio.
- Comunicar al Ministerio competente en materia de Sociedad de la Información el cese de su actividad yel destino que va a dar a las firmas y sellos electrónicos conservados, así como cualquier otra circunstancia relevante relacionada con el cese de actividad.

14.5 RESOLUCIÓN

Sin perjuicio de las causas descritas en la normativa española, TRUSTCLOUD considerará como causa de resolución anticipada de la prestación de los servicios, las siguientes:

- El incumplimiento por las partes de cualquier obligación de las previstas en las presentes Condiciones Generales de Uso, requerida la Parte incumplidora, ésta no procede a la subsanación del incumplimientoen un plazo de 30 días.
- Por decisión judicial o administrativa, que implique la imposibilidad para cualquiera de las partes de ejecutar las condiciones pactadas del servicio.
- El simple incumplimiento y/o retraso en el pago de cualquiera de las obligaciones de abono que se relacionan en las condiciones de contratación, se entenderá como motivo suficiente para que TRUSTCLOUD de por resuelto de manera unilateral el contrato de prestación de servicio, sin perjuicio dereclamar las obligaciones pendientes de abono o pagos si las hubiere.

TRUSTCLOUD se reserva la facultad de resolución del contrato en caso de que existieran circunstancias sobrevenidas, derivadas en un cambio de las condiciones de mercado, por vicios o deficiencias en los datos o informaciones recibidas para la elaboración de la Propuesta Económica, o cualquier otra circunstancia ajena a suvoluntad, incluida la producción de un desajuste entre los precios pactados y el coste de ejecución del Servicio, derivado de circunstancias del mercado resultare un déficit económico por la ejecución del Servicio y en generalpor cualquier causa ajena a la voluntad de TRUSTCLOUD , que produzca la ruptura del equilibrio económico del mismo.

14.6 SUBCONTRATACIÓN

TRUSTCLOUD podrá subcontratar los servicios que estime necesarios para el aprovisionamiento y explotación delServicio de acuerdo con las necesidades que surgieran, y formalizará esta relación mediante un acuerdo escrito que determinará las condiciones del servicio prestado mediante esta subcontratación.

14.7 NULIDAD

Si cualquiera de las Condiciones Generales de Uso fuese declarada total o parcialmente nula o ineficaz, tal nulidado

ineficacia afectará únicamente a dicha disposición o parte de la misma que resulte ineficaz o nula, y el resto delas cláusulas continuarán vigentes, teniéndose tal condición o la parte de la misma que resulte afectada por no puesta.

14.8 NOTIFICACIONES

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las practicas descritas en esta Declaración de Prácticas de Certificación se realizará mediante documento o mensaje electrónico firmado digitalmente o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto relativo a Datos de contacto. Las comunicaciones electrónicas se harán efectivas una vez que las reciba eldestinatario al que van dirigidas A los efectos las partes designarán expresamente los domicilios para la práctica de comunicaciones. En caso de modificación del domicilio, las partes se obligarán a notificar a la otra la modificación en la forma establecida enel párrafo primero.

14.9 APROBACIÓN Y REVISIÓN DE PRÁCTICAS DEL SERVICIO DE CONFIANZA

14.9.1 APROBACIÓN E IMPLANTACIÓN

Las presentes DPC serán aprobadas por el Director de TRUSTCLOUD, máximo nivel y autoridad de responsabilidaddentro de TRUSTCLOUD, que además estará dotado de la responsabilidad y capacidad para elaborar y gestionar las mismas.
Se ha establecido un equipo de gestión responsable de la implantación de las prácticas de seguridad y organizativas requeridas para garantizar la confidencialidad, integridad y todo lo establecido en estas DPC. TRUSTCLOUD ha definido un equipo integrado por los responsables de las diferentes áreas implicadas en cada uno de los pasos del servicio de conservación de firmas y sellos electrónicos.

14.9.2 MODIFICACIONES

TRUSTCLOUD se reserva el derecho de modificar unilateralmente este documento siempre y cuando:

- La modificación esté justificada desde el punto de vista técnico y legal.
- Se notifiquen a los usuarios de todas las afectaciones derivadas de estas modificaciones y estos acepten las mismas previo uso del servicio.
- Se ofrezca un mecanismo de control de cambios y de ediciones.

En este sentido, se ha establecido un procedimiento al efecto en el que se regulan los mecanismos a seguir en caso de necesidad de modificación de las DPC. Una vez decidida la conveniencia de realizar una revisión, el responsable de la elaboración del documento efectuará las modificaciones oportunas, quedando identificadas en la nueva edición mediante sombreado del texto modificado. Este método puede coexistir o ser sustituido por un listado de control de cambios en el que se relacionen los cambios introducidos en cada una de las ediciones o versiones del documento.

Si las modificaciones efectuadas sobre el documento producen una alteración que afecte al servicio prestado a los usuarios estas serán consideradas un “major release”. De otro modo serán consideradas un “minor release”.

Los usuarios serán informados en caso de producirse un “major release” quedando modificada la relación contractual entre TRUSTCLOUD y éstos. De este modo los Usuarios deberán adherirse a las nuevas condiciones

de uso previa prestación de nuevos servicios o abrirse un proceso de baja en el servicio

14.9.3 VERSIONES

Estas DPC pueden sufrir cambios en el transcurso del tiempo. Cuando se produzca un cambio “major release” supondrá aumentar en uno las versiones del documento. Sin embargo, cuando se produzca un cambio “minor release” modificará el número de su versión.

14.9.4 PUBLICACIÓN

Es obligación de TRUSTCLOUD publicar la información relativa a sus prácticas, sus certificados y el estado en que se encuentran dichos certificados. Todo el histórico de esta documentación deberá ser conservado y accesible bajo demanda a través de email de contacto de la web (punto 6) al menos por un periodo de 15 años.

Toda publicación se llevará a cabo en el sitio web de TRUSTCLOUD o en sitios web bajo el control de TRUSTCLOUD ycon una vinculación directa o indirecta a la razón social y/o marca de TRUSTCLOUD. También se publicará mediante el envío de correo electrónico certificado y en la página de la Autoridad competente. La publicación serealizará en el momento de su creación

14.9.5 LEGISLACIÓN Y JURISDICCIÓN APLICABLE

Las presentes condiciones generales de contratación se regirán por la normativa española.

Las partes, con expresa renuncia a cualquier fuero propio que pudiera corresponderles, se someten a la Jurisdicción y Competencia de los Juzgados y Tribunales de Madrid para cualquier cuestión relativa a la interpretación, cumplimiento o ejecución de la presente declaración

15 PERFIL DE CONSERVACION

TRUSTCLOUD únicamente presta el servicio de preservación con almacenamiento. Una vez finalizado el período de transición pactado con el cliente, se inicia el período de bloqueo de los datos obtenidos, los cuales son eliminados a la finalización de este según lo indicado en la legislación en vigor

El perfil de preservación se identifica a través del siguiente OID: 1.3.6.1.4.1.5 2582.1.1.1.

Las operaciones soportadas por el protocolo de preservación son las siguientes:

Llamada 1) Enviar. Mandar la información. Descrito en el punto 7.2 CARACTERÍSTICAS PRINCIPALES DE LOSSERVICIOS DE TRUSTCLOUD

Llamada 2) recuperar el fichero. Método de recuperación de ficheros a través de la APILlamada 3) Borrar P0. Método de borrado a través de la API.

El período de validez del perfil de preservación se iniciará una vez finalizado el proceso descrito en el punto 7.3SERVICIO DE CONSERVACIÓN DE FIRMAS Y SELLOS ELECTRÓNICOS CUALIFICADOS

El modelo de almacenamiento con preservación que presta TRUSTCLOUD es un modelo de preservación con almacenamiento.

En relación con los períodos de conservación de datos bloqueados, TRUSTCLOUD se remite a los plazos legales:

- En cumplimiento del artículo 9.3.a) Ley 6/2020 de 11 de noviembre, relativa a las obligaciones aplicables a los prestadores cualificados, "el período de tiempo durante el que deberán conservar la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014, será de 15 años desde la extinción del certificado o la finalización del servicio prestado". Por lo tanto, TrustCloud conservará la información relativa al servicio de conservación de firmas y sellos durante 15 años desde la finalización del servicio prestado.

Los objetivos de preservación son una combinación de Preservación de firmas digitales y aumento de las pruebasde preservación a través del resellado.

16 POLÍTICA DE EVIDENCIA DE PRESERVACIÓN

Las pruebas se realizan dentro de Trustcloud almacenadas en base de datos y en la herramienta de logs, las evidencias se conservan en la herramienta de almacenamiento

Se utilizan Algoritmos SHA-256 para hashes de documentos y SHA-512 para sellos de tiempo.

Las evidencias de conservación se validan a través del servicio Digital Signature Service (DSS). Las evidencias PDFson PAdES. Esta misma validación la podría hacer un tercero. El aumento de las pruebas de preservación se consigue con el resellado.

Usamos PAdES, al descargar la evidencia no tienen información de nuestro servicio, sólo el sello de tiempo.

TRUSTCLOUD cuenta con un proveedor cualificado de sellado de tiempo y un proveedor cualificado de certificados.

TRUSTCLOUD cuando no pueda recoger y verificar todos los datos de validación, enviará una notificación del fallo y archivará como expediente no cualificado.

17 ACUERDO DE SUSCRIPTOR

Para los derechos de acceso se aplica la siguiente política:

- Lectura: usuarios autorizados.
- Modificación: administradores, y solo bajo petición por causa justificada
- Borrado: administradores. y solo bajo petición por causa justificada

Todas las evidencias generadas durante el proceso de custodia quedan registradas en un certificado de evidencias generadas por TRUSTCLOUD. Estas evidencias se entregarán a la finalización del servicio o se entrega al suscriptor previa solicitud.