DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS SERVICIO DE VERIFICACIÓN DE IDENTIDAD (DPyP)

TrustCloud

TIPO DE DOCUMENTO				**Documentación Secreta**
			x	**Documentación Pública**
				Documentación Interna
				Documentación confidencial
TÍTULO			DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS SERVICIO DE VERIFICACIÓN DE IDENTIDAD	
ENTIDAD			TRUSTCLOUD INC.	
FORMATO			Electrónico - PDF	
PÁGINAS				
VERSIÓN	**FECHA DE EMISIÓN**	**OID**	**AUTOR**	
1.1	07/11/2023	1.3.6.1.4.1.52582.1.1.1	TRUSTCLOUD	
Revisado por: Alberto Angón (CISO-RSI)			Fecha:	
Aprobado Por Comité de Dirección TRUSTCLOUD			Fecha:	

HISTORIAL DE MODIFICACIONES

Versión	Fecha	Descripción de la acción	Páginas
1.0	10/04/2023	Edición inicial	
1.1	08/11/2023	Actualización referencias marco normativo (apartados 3 y 4).	

INDICE

1. INTRODUCCIÓN

El presente documento es una Declaración de Prácticas y Políticas del Servicio de Verificación de Identidad, mediante el cual TRUSTCLOUD, como prestador de servicios de confianza no cualificado, expone y describe la forma en que presta el Servicio de Verificación de Identidad y asegura el cumplimiento de las obligaciones legalmente exigibles, informando al 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 Verificación de Identidad, de conformidad con lo establecido en el Reglamento de ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica 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 Directiva 1999/93/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 Verificación de Identidad, TRUSTCLOUD sigue las indicaciones de los estándares del Instituto Europeo de Estándares de Telecomunicaciones -ETSI- guiándose para ello por las especificaciones técnicas de las normas, EN 319 401 (requerimientos generales para proveedores de servicios de confianza), EN 119 461 (Requisitos de política y seguridad para los componentes de los servicios de confianza acreditación de la identidad de los sujetos de los servicios de confianza) ISO 30107 Biometría. A tal efecto, TRUSTCLOUD ha llevado a cabo el diseño y desarrollo de una infraestructura tecnológica que, de forma integrada, pone a disposición de sus Usuarios una herramienta a través de la que poder comprobar la correspondencia entre sus datos identificativos y sus parámetros biométricos con los recogidos en su documento fehaciente, así como corroborarla autenticidad, vigencia e integridad de este último

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 y Políticas del Servicio de Verificación de Identidad, se asignan a cada tipo un identificador de objeto (OID).

La presente Declaración de Prácticas describe los servicios relacionados con la verificación de identidad prestados a través de la plataforma titularidad de 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
- 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. ACRÓNIMOS 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 de 2014 relativo a la identificación electrónica y los servicios de confianza paralas 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
PKI	Public Key Infraestructure – Infraestructura de Clave Pública
PBC&FT	Prevención del Blanqueo de Capitales (PBC) y la Financiación del Terrorismo (FT)
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
DPyP	**Declaración de Prácticas de y políticas servicio de verificación de identidad**: Declaración de TRUSTCLOUD puesta a disposición del público por vía electrónica y de forma gratuita realizada en calidad de Prestador de Servicios de Confianza en cumplimiento de 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.
USUARIO	Persona física o jurídica que utiliza los servicios de verificación de identidad
DOCUMENTACIÓN	Conjunto de evidencias digitales recibidas por TRUSTCLOUD por parte del Usuario, que cumplen con los requisitos establecidos en las presentes DPyP

4. NORMAS Y ESTÁNDARES 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 deroga la 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) Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo de 20 de mayo de 2015 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) no 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión ("DPBAC")
6) ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers
7) [ETSI EN 119 461 Policy and security requirements for trust service components providing identity proofing of trust service subjects.
8) ISO/IEC 30107-1 Biometric
9) ISO/IEC 27001:2022 Information security, cybersecurity, and privacy protection — Information security management systems
10) ISO/IEC 27002;2022 Information security, cybersecurity, and privacy protection — Information security controls

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 Verificación de Identidad en esta Declaración de Prácticas y Políticas.
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 la norma ETSI TS 119 461, garantizado por la implantación de un SGSI basado en la norma ISO/IEC 27001
6) Que TRUSTCLOUD tiene en cuenta los requisitos legales necesarios

6. DATOS DE IDENTIFICACIÓN Y CONTACTO

- Razón Social: TRUSTCLOUD S.L.
- Denominación Comercial: TRUSTCLOUD
- CIF: B87142618
- Domicilio Social: Paseo Club Deportivo 1, 28223 Pozuelo de Alarcón, Madrid
- Servicio de Atención al Cliente (SAC): +34 913 518 558
- Correo electrónico: soporte@trustcloud.tech
- Web: https://www.trustcloud.tech/
- Otros datos de contacto: +34 913 518 558

7. DESCRIPCIÓN DEL SERVICIO

A través de la solución “VideoID”, TRUSTCLOUD, pone a disposición de sus clientes sujetos obligados un sistema de identificación por video-identificación que permite autenticar al usuario procediendo a comprobar la correspondencia entre sus datos identificativos y sus parámetros biométricos – rasgos faciales - con los recogidos en su documento fehaciente (Depende del país, pero en general ID en formato tarjeta, con fotografía, y MRZ. permisos de residencia que cumplan el formato también, y pasaportes), así como corroborar la autenticidad, vigencia e integridad de este último.

A lo largo del proceso se generan y registran toda una serie de evidencias electrónicas susceptibles de ser utilizadas como prueba en un posterior proceso judicial para acreditar el contenido de la video-identificación realizada.

Todas estas pruebas se recogen en un documento, denominado “certificado de finalización”, que se emite bajo la firma electrónica cualificada de TRUSTCLOUD en el momento en que se produce cualquiera de los eventos de terminación del proceso de video-identificación. A saber:

I. La correcta identificación del usuario.

II. La falta de correspondencia entre los datos facilitados por el usuario y los recogidos en el documento fehaciente o la existencia de indicios de falsedad o manipulación en el citado documento.

III. La imposibilidad de completar el proceso de identificación debido a causas técnicas que impidan o dificulten verificar la correspondencia entre el titular del documento y el cliente objeto de identificación.

Asimismo, una vez finalizada la video-identificación, se procede a aplicar sobre el documento electrónico que contiene la grabación de la misma la firma electrónica cualificada de TRUSTCLOUD así como un algoritmo SHA-256que garantizan que la grabación ha sido emitida por TRUSTCLOUD y que la misma ha permanecido intacta e inalterable.

Una de las características principales del servicio es su versatilidad y la posibilidad de integrarlo con las plataformas de contratación del cliente sujeto obligado y adaptarlo a su modelo de negocio y criterios de riesgo. No obstante, en líneas generales, el proceso de video-identificación se estructura en los siguientes pasos:

A. Acceso del usuario a la plataforma de video-identificación

Debido a las mencionadas características, el usuario final puede acceder a la plataforma de video-identificación:

1. De forma integrada con la plataforma digital del cliente sujeto obligado: incrustando en este proceso –generalmente, una vez que el usuario final ha facilitado sus datos identificativos básicos- un botón con la opción "Acceder a la video- identificación" o de análogo significado en la aplicación web o mobile.
2. De forma independiente a la plataforma digital del cliente sujeto obligado: remitiendo al usuario un correo electrónico o SMS en el que se le informe de la existencia de un proceso de video-identificación pendiente de ser completado y se le facilite un enlace al mismo.

En ambos casos, el efectivo acceso a la plataforma puede vincularse a la previa validación del usuario a través de alguno de los métodos de identificación de que dispone TRUSTCLOUD aportando un mayor nivel de seguridad. No obstante, no consideramos que este punto resulte esencial para la validez legal del proceso, pues la identificaciónexigida a efectos de la normativa PBC&FT es la que tiene lugar durante el desarrollo de la video-identificación y no la que acaece con carácter previo a la misma.

En este sentido, llamamos la atención respecto a que, conforme a la Resolución del SEPBLAC de 11 de mayo de 2017, se entiende que no será admisible el uso de archivos pregrabados por el cliente u otras personas ajenas al sujeto obligado. La Solución tal y como está planteada no se corresponde con ninguna de estas situaciones por lo que también cumpliría este requerimiento.

En cualquier caso, es preciso señalar que de forma simultánea al acceso a la plataforma de video- identificación se establece una conexión entre el dispositivo del usuario y el servidor de destino mediante el protocolo TLS 1.2 que permite una comunicación cifrada y segura conforme a los más elevados estándares existentes actualmente en el mercado

B. Desarrollo del proceso de video-identificación, autenticación del usuario y comprobación de la validez del documento

B.1 Proceso de identificación asistida

El proceso de identificación asistida se caracteriza porque, una vez el usuario ha accedido a la plataforma de video-identificación, un videoagente se encargará de guiarle a lo largo de todo el proceso. Las líneas básicas del flujograma son las siguientes:

1. El usuario debe decir su nombre, apellidos y número del documento de identificación a fin de comprobar que coinciden con los introducidos en la plataforma del cliente sujeto obligado -o los facilitados por el mismo para el caso en que no se encuentren integradas ambas plataformas- y con los que se muestran en el documento de identificación que posteriormente se exhibirá a la cámara.

2. El videoagente toma el control en remoto de la cámara del dispositivo utilizado –previo consentimiento

del usuario- y solicita al usuario que exhiba el anverso y el reverso del documento de identificación, moviéndolo ligeramente para que puedan grabarse los distintos elementos de seguridad físicos a él incorporados (CLI, kinegrama, tinta OVI, entre otros).

3. El videoagente toma fotografías del anverso y el reverso del documento de identificación y del rostro del usuario y devuelve el control de la cámara al usuario
4. El videoagente comprueba que las instantáneas cuentan con las condiciones de calidad y nitidez necesarias y, en su caso, las remite al sistema de validación y cotejo
5. El videoagente comunica al usuario la conclusión del proceso de video- identificación y le remite a la plataforma del cliente sujeto obligado.
6. El cliente sujeto obligado, a través de su plataforma digital o por el medio que estime más oportuno, informa al usuario del resultado de la video-identificación y:

I. En caso de haber sido correcta, de los siguientes pasos a dar para completar la contratación solicitada.

II. En caso de haber resultado fallida, de los métodos alternativos de identificación formal que el cliente sujeto obligado pone a su disposición, como por ejemplo la reiteración del proceso de video-identificación para el caso de que éste haya finalizado por causas técnicas.

El proceso únicamente se puede llevar a cabo desde un dispositivo y la comunicación se desarrolla, en todo caso en directo, en formato digital, de forma continua y sin interrupción, procediendo a su grabación inmediata, salvo que existan incidencias técnicas o físicas que impidan que éste cuente con el nivel de calidad necesario. Ante estas circunstancias, se tratará de subsanar estas deficiencias y, en caso de que no resulte posible o viable en un tiempo razonable, se informará al usuario de la imposibilidad de completar el proceso de video-identificación, solicitándole, si se trata de una incidencia temporal, que lo intente de nuevo más tarde o, en caso contrario, que opte por alguno de los métodos de identificación formal alternativos.

B.2 Proceso de identificación no asistida

El proceso de identificación no asistida se caracteriza porque el cliente únicamente interactúa con la plataforma de videoidentificación. No existe, por tanto, ningún videoagente (persona física) encargado de guiar al cliente durante el proceso de videoidentificación, sino que esta labor es desarrollada de forma automática por la propia plataforma. Las líneas básicas del flujograma son las siguientes:

1. La plataforma solicita al usuario que exhiba el anverso y el reverso del documento de identificación y que lo sitúe en un recuadro determinado para tomar sendas fotografías de ambas caras.
2. Realizadas las fotografías del documento identificativo, la plataforma solicita al usuario que sitúe su rostro en un espacio determinado, realice ciertos movimientos como “prueba de vida” y, posteriormente, toma una fotografía de su rostro.
3. Después de las fotografías, el proceso -desde la perspectiva del cliente- finaliza.
4. La plataforma, de forma automática, comprueba que:
    a. La información recogida en el documento de identificación coincide con la facilitada por el cliente en la plataforma del cliente sujeto obligado.
    b. No existen indicios de falsificación en el documento identificativo.
    c. Existe una correspondencia entre los rasgos faciales del cliente objeto de identificación y la fotografía contenida en el documento identificativo que ha sido exhibido y fotografiado.
5. En los supuestos de identificación positiva, un agente revisa la grabación y verifica que se han cumplido

todos los requisitos.

Para ambos procesos (asistido y no asistido), la Solución tiene implementadas las siguientes medidas:

- ✓ La grabación es inmediata y puede ser configurada para iniciarse automáticamente en todas las sesiones o ser manualmente iniciada por el agente.
- ✓ La comunicación se desarrolla en formato digital y sin alteración.
- ✓ Se asegura la protección de los datos de usuario y la seguridad en general de su plataforma en la nube.
- ✓ Todas las comunicaciones, incluyendo la señalización y los medios audiovisuales son asegurados a través de túnel encriptado.
- ✓ El software que se instala el cliente está firmado digitalmente para evitar su modificación o ataques por inyección de código.

C. Autenticación del usuario y comprobación de la validez del documento

C.1 Proceso de identificación asistida

Completado el proceso de video-identificación, el videoagente, con la ayuda del sistema automático de validación y cotejo, comprueba que no se dan ninguna de las circunstancias impeditivas. A saber:

I. **Indicios de falsedad o manipulación del documento de identificación;**

II. **Indicios de falta de correspondencia entre el titular del documento y el cliente objeto de identificación;**

III. **Unas deficientes condiciones de comunicación que impidan o dificulten las tareas de verificación a realizar.**

El resultado del proceso es positivo siempre y cuando no se den ninguna de las anteriores circunstancias y quede, en consecuencia, acreditada la correspondencia entre el usuario y el documento de identificación válido que éste exhibe.

C.2 Proceso de identificación no asistida

Por su parte, como se detalló en el punto B.2, en el proceso de identificación no asistida es la propia plataforma quien, de forma automática, comprueba la autenticidad del documento y la correspondencia entre su titular y el cliente objeto de videoidentificación. Adicionalmente, un agente revisa la grabación y verifica que se han cumplido todos los requisitos.

D. Comunicación del resultado del proceso y emisión del expediente de finalización

Una vez analizado el proceso de video-identificación, TRUSTCLOUD comunica su resultado al cliente sujeto obligadodetallando, en su caso, las causas de la denegación.

Asimismo, si así es solicitado, pone a disposición del cliente sujeto obligado el “certificado de finalización” que –como detallamos en el apartado 7- es emitido de forma automática una vez se ha producido alguno de los hitos

que conllevan la finalización del proceso.

E. Requisitos a cumplir durante el desarrollo del proceso de video-identificación.

1. Ser gestionado por personal con formación específica

Con el objetivo de cumplir con esta especificación, todo el personal de TRUSTCLOUD relacionado directa o indirectamente con la prestación del servicio de video- identificación deberá haber recibido la oportuna formación sobre PBC&FT e identificación electrónica. Asimismo, los videoagentes serán formados en el uso y empleo de la herramienta, así como en los flujogramas y la respuesta ante las posibles incidencias que puedan acaecer.

2. Grabar el proceso de video-identificación y dejar constancia de su fecha y hora

La solución desarrollada procede a la grabación de todos y cada uno de los procesos de video-identificación dejando constancia de la fecha y hora en que tiene lugar y de su inicio y terminación. Asimismo, una vez el proceso ha finalizado se procede a calcular el resumen único de la grabación y a recoger en el "expediente de finalización" este dato junto con las mencionadas fechas y horas con el objetivo de poder acreditar posteriormente su realización.

Es preciso reseñar que:

I. Cada uno de los procesos de video-identificación cuenta con su grabación única e independiente y con su hash (número de identificación) asociado pues, en caso contrario, (es decir, si en un mismo fichero se recogen varios procesos de video-identificación) la posible alteración o el deterioro de uno de los procesos afectaría a todos aquellos otros con los que comparte archivo.

II. El proceso de video-identificación se graba íntegramente lo que permite su reproducción secuencial sin saltos temporales y permite acreditar su contenido, así como la fecha y hora en la que el mismo ha sido grabado.

3. Asegurar la privacidad de la conversación y del cliente, la seguridad en la transmisión y la autenticidad e integridad de la grabación

TRUSTCLOUD tiene implantadas medidas técnicas y físicas para asegurar la privacidad de la conversación mantenidacon el usuario, así como del cliente y del propio proceso de video-identificación a tenor del estado de la técnica a fecha de emisión del presente informe. Adicionalmente, estas medidas permiten garantizar la seguridad en la transmisión.

Con respecto a las medidas técnicas, la comunicación con los usuarios se articula mediante el protocolo TLS 1.2 que establece una conexión cifrada con el servidor de destino. Este protocolo responde a los estándares del mercado más elevados, reemplazando al antiguo protocolo SSL. De esta forma, se procura una comunicación segura que impide la interceptación subrepticia de su contenido, pues éste viaja cifrado y solo es posible su deducción haciendo uso de las claves que los intervinientes previamente han intercambiado. Este mecanismo de intercambio de clave se ejecuta a través del sistema ECDHE_RSA que, a día de hoy, garantiza un "secreto perfecto hacia adelante", siendo un prestador de servicios de confianza -distinto de TRUSTCLOUD- quien emite un certificadoen el que se acredita la autenticidad de la plataforma sobre la que se desarrolla la grabación y la identidad de sutitular. Por último, se ha de destacar que, estas soluciones hacen uso de cifrados a través de algoritmos como

AES_256_GCM y el código de autenticación empleado es el HMAC-SHA2.

Con respecto a las medidas físicas para los supuestos de procedimientos de identificación asistidos, los puestos de los videoagentes están separados por biombos y durante la video- identificación se utilizan auriculares todo ello con el objetivo de asegurar la necesaria privacidad y evitar que la video-identificación sea vista y escuchada por un trabajador distinto de su responsable. Asimismo, los videoagentes deben cumplir con el protocolo de "No Parar. No Mirar. No Hablar (NOPMH)" cuando se levantan de su puesto de trabajo y pasan por detrás de la conversación que otro videoagente está llevando a cabo durante ese momento.

En lo relativo a la autenticidad de la grabación, el hecho de que en el mismo momento de finalización de la misma se proceda a su firma mediante una firma electrónica cualificada de TRUSTCLOUD permite contar con evidencias sólidas que garanticen que dicha grabación ha sido realizada y emitida por TRUSTCLOUD y no por ningún otro tercero.

Por último, respecto a la integridad de la grabación, la Solución ofrecida por TRUSTCLOUD cuenta con un mecanismo que procede a aplicar el algoritmo SHA-256 sobre el documento electrónico que contiene la grabación, lo que permite obtener de cada documento electrónico un único valor de longitud fija (denominado resumen único o hash). El hash es objeto de custodia y se plasma en cada uno de los certificados de finalización emitidos.

La solvencia del sistema empleado se basa en las siguientes premisas:

1. Irreplicabilidad del resultado: Aplicado el mismo algoritmo a dos documentos idénticos se obtendrá siempre el mismo hash. Sin embargo, si estos documentos difieren –aunque sea en una simple coma-, el resumen será distinto.
2. Unidireccionalidad de la función: Ésta permite obtener de un documento electrónico su resumen único, pero el resultado inverso no es técnicamente posible, es decir, aplicando el algoritmo al hash no se extrae el documento original. De este modo, su utilización permite garantizar la integridad del documento electrónico sin crear una serie de copias que pudieran comprometer su confidencialidad.
3. Reconocimiento internacional: El algoritmo empleado SHA-2 es un estándar FIPS diseñado por la NSA27.

De este modo, el mecanismo implantado por TRUSTCLOUD ofrece garantías de que el documento electrónico donde se encuentra la grabación y, por ende, la propia grabación, ha permanecido intacto e inalterable pues, si una de las partes denunciara que el documento ha sufrido alteraciones, se procedería a obtener su hash y a compararlo con el que fue emitido y depositado en los sistemas de TRUSTCLOUD.

4. Exhibir el anverso y el reverso del documento de identificación y obtener y conservar una fotografía o instantánea

El videoagente solicita al usuario que exhiba su documento de identificación y toma el control de la cámara con el objetivo de ser él quien toma las fotografías y evitar que el usuario pudiera enviar unas almacenadas con anterioridad en su dispositivo. Asimismo, con carácter previo a considerar finalizada la video-identificación, el videoagente comprueba que éstas cuentan con las garantías de calidad y nitidez necesarias pudiendo proceder a hacerlas de nuevo en caso de que, por ejemplo, estén movidas o las condiciones de luminosidad no sean adecuadas.

5. Acreditar la autenticidad, vigencia e integridad de los documentos y su correspondencia con el usuario

Aparte de la formación recibida en la que se detallan las medidas de seguridad vinculadas a los documentos

identificados analizados actualmente, el servicio puede incluir un sistema de cotejo y validación automático que procederá a la lectura OCR y a comprobar la coincidencia entre los rasgos faciales del usuario y los recogidos en la fotografía del documento de identificación a través de una serie de puntos críticos. Asimismo, es importante destacar la posibilidad de añadir capas de seguridad complementarias como, en su caso, la validación electrónica del DNIe 3.0. en caso de que el usuario cuente con un dispositivo con tecnología NFC accesible.

La suma de estos elementos nos permite declarar que, formalmente y de acuerdo con la información facilitada, el sistema propuesto, en una situación de funcionamiento óptima, acredita la autenticidad, vigencia e integridad de los documentos y su correspondencia con el usuario dentro del margen de riesgo propio de toda actividad a distancia

6. Asegurar que el proceso se realiza desde un único dispositivo, que la comunicación se realiza en formato digital, sin alteración y en directo y que se procede a su grabación inmediata

En atención a la descripción funcional del servicio facilitada, la implantación de las medidas que garanticen las obligaciones relativas a la realización del proceso, el establecimiento de la comunicación y la grabación de la misma supondría que el servicio “VideoID” cumple formalmente con las citada exigencias.

F. Requisitos posteriores al desarrollo del proceso de video-identificación

1. Arrojar un resultado negativo ante determinados supuestos

Del modo expuesto en la descripción funcional del servicio, el resultado de la video- identificación será siempre negativo cuando se cumplan las circunstancias impeditivas desglosadas en la Especificación:

1. Indicios de falsedad o manipulación en el documento de identificación.
2. Indicios de falta de correspondencia entre el titular del documento y el cliente objeto de identificación.
3. Deficientes condiciones de la comunicación impidan o dificulten verificar la autenticidad e integridad del documento y la correspondencia entre el titular y el cliente objeto de identificación.

2. Conservar la grabación del proceso y de los documentos empleados en el mismo durante un período de 10 años

TRUSTCLOUD archiva en soporte electrónico, como mínimo, la siguiente documentación:

1. El “certificado de finalización”.
2. La grabación del proceso de video-identificación.
3. Las instantáneas tomadas del anverso y el reverso del documento de identificación y del rostro del usuario identificado.

Esta documentación electrónica, entre la que se encuentra la grabación de la video-identificación, es conservada y debidamente custodiada por TRUSTCLOUD durante un periodo mínimo de 10 años, contando para ello con un mecanismo que ofrece garantías sobre su autenticidad e integridad conforme a lo expuesto anteriormente. Asimismo, será entregada al cliente sujeto obligado en cualquier momento de la relación contractual o a la

finalización de la misma, para que el mismo pueda cumplir con sus obligaciones en materia de PBC&FT.

Adicionalmente, se debe destacar que TRUSTCLOUD cuenta con la consideración de Prestador de Servicios deConfianza Cualificado para el servicio de conservación de firmas y sellos electrónicos cualificados.

3. **Someter el procedimiento de video-identificación a un examen anual emitido por un experto externo**

En relación con este requerimiento, debe destacarse por un criterio de imparcialidad, que consideramos debe ser el sujeto obligado quién nombre al experto encargado de analizar anualmente el proceso de video-identificación como uno más de los procedimientos establecidos por el sujeto obligado en materia de PBC&FT.

4. **Someter el procedimiento de video-identificación a una revisión específica e individual previa a la ejecución de cualesquiera operaciones**

Por último, y en relación únicamente con los procedimientos de video-identificación no asistidos, será necesaria una revisión específica e individual de la grabación del proceso con carácter previo a la ejecución de cualesquiera obligaciones.

8. OBLIGACIONES Y RESPONSABILIDADES

8.1 OBLIGACIONES DE TRUSTCLOUD

TRUSTCLOUD como Prestador de servicio de confianza, no cualificado se compromete a cumplir una serie deobligaciones detalladas en esta DPyP, en el marco 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 de Verificación de Identidad según lo expuesto en esta Declaración de Prácticas Y Políticas.
- Prestar el Servicio de Verificación de Identidad 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 auditoria con 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 Verificación de Identidad de forma diligente e ininterrumpida
- Comunicar a sus Usuarios con la suficiente antelación la no disponibilidad del sistema en caso de realizar procesos 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 el sistema con afectación para las mismas.
- 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 secontemple.
- 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

8.1.2 INFORMACIÓN PARA SOCIOS COMERCIALES

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

- Verificar la validez, suspensión o revocación de la verificación de identidad
- Respetar las medidas de seguridad que indique TRUSTCLOUD para acceder al Servicio de Verificación deIdentidad

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 modificación en la presente Declaración de Prácticas y políticas.

- Notificar a la autoridad competente y a las partes implicadas el cambio en la infraestructura que pueda

afectar a la prestación del servicio.

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 Verificación de Identidad.

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 asumirá todos 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 así como 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 Verificación de Identidad deberá cumplir con las siguientes obligaciones:

- Los objetos enviados deberán cumplir con los requisitos establecidos en la norma ETSI 119 461
- Deberá asegurar el cumplimiento legal y la exactitud de los objetos a preservar
- 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 que en 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 ello con 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 o cortes en el suministro eléctrico.

Dicha protección se extiende a aquellos sistemas cuya securización física está delegada en algún proveedor. Para ello, 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 procedimientos que garanticen que la información contenida en ella está adecuadamente securizada, así como que permitan la reutilización 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 DPyP 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 que eviten su repetición.

Se ha establecido igualmente una adecuada segregación de funciones en la asignación de responsabilidades con el 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, ordenadoresportátiles, dispositivos móviles y teléfonos, etc.), como residualmente, en soporte papel, todo ello con la finalidad de mitigar el riesgo de acceso no autorizado, perdidao 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 los propietarios 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 entienden como 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 un proceso de identificación, autenticación y autorización, estableciéndose los controles adecuados para que tales procesos 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 los mismos.

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 DPyP. (Conservar la grabación del proceso y de los documentos empleados en el mismo durante un período de 10 años

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.

9.3.2.3 REQUERIMIENTOS PARA LAS FUENTES DE TIEMPO

Los certificados, CRLs, y otras entradas de bases de datos de revocación deberán contener información de fecha y 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 en el protocolo NTP (Network Time Protocol), auto calibrándose por distintos medios.

9.3.2.4 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 para evitar 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, filtrado de correo y DLP, todos ellos de actualización automatizada, siempre que tecnológicamente los sistemas soporten controles de estos tipos. Disponemos de Defender for business, firewall interno Sonicwall y firewall gestionado por Movistar para conexión de red de oficina y las medidas de SI de AWS. Previa autorización, se permite a su vez la utilización de Avast (Android) y Firewall (iOS).
  También de un SIEM (Wazhu) y de una herramienta de gestión proactiva de vulnerabilidades (Tenable)
- 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 análisis anual 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 de TRUSTCLOUD 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 los mismos.

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 Usuario que 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 nivelesestablecidos 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 de Negocio y disponibilidad 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 responder a incidentes e interrupciones del negocio con el fin de continuar con las operaciones críticas del negocio dentro de 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 Sistemade 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 proceso de 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 DPyP 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 mayor brevedad 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 cada auditoria.

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

- Adecuada y acreditada capacitación y experiencia en seguridad y procesos de auditoria de sistemas de 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 Encargado de Tratamiento, en virtud de lo previsto en el artículo 28 del RGPD [4].

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 DPyP. 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 DPyP 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 las mismas.

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 de requerimiento 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 y Políticas (DPyP) 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 cuando este fuese necesario. 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 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 tratamiento, 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 o al cumplimiento de obligaciones legales o contractuales.
- 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 tratados en 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 del tratamiento de datos de carácter personal.

TRUSTCLOUD se compromete a guardar bajo su control y custodia los datos personales suministrados por el RESPONSABLE 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 salvo en cumplimiento de obligaciones legales.

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 el RESPONSABLE 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, ejercitasen sus derechos ante TRUSTCLOUD, éste deberá dar traslado de la solicitud de forma inmediata al RESPONSABLE y, a no más tardar, dentro del plazo de 3 días laborables a contar desde su recepción, para que el RESPONSABLE resuelva debidamente dicha solicitud.

La presente DPyP 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 el cumplimiento del RGPD [3].

TRUSTCLOUD garantiza el cumplimiento de las obligaciones que le correspondan en virtud de la normativa que le resulte 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 servicio prestado o en los datos de carácter personal tratados, TRUSTCLOUD lo notificará en el plazo máximo de 24 horas desde 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 DPyP. 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:

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 DPyP, 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 periódica 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 se solicitan 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. El Cliente será responsable de asegurarse que el uso de los Servicios es conforme a la normativa del país en el que el Cliente desee operar.

14.4 PREVISIONES EN CASO DE TERMINACIÓN DEL SERVICIO

TRUSTCLOUD se compromete a adoptar todas las medidas necesarias para minimizar el impacto que podría sufrir un Usuario o terceras partes intervinientes en el servicio de las presentes DPyP, 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 que se recoge el proceso que llevará a cabo TRUSTCLOUD antes de la terminación del servicio, en concreto en cuanto a 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 unaantelación mínima de dos 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 y el 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 incumplimiento

en 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 de reclamar 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 su voluntad, 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 general por 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 del Servicio 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 nulidad o ineficacia afectará únicamente a dicha disposición o parte de la misma que resulte ineficaz o nula, y el resto de las 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 y Políticas 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 el destinatario 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 en el párrafo primero.

14.9 APROBACIÓN Y REVISIÓN DE PRÁCTICAS DEL SERVICIO DE CONFIANZA

14.9.1 APROBACIÓN E IMPLANTACIÓN

La presentes DPyP será aprobadas por el Director de TRUSTCLOUD, máximo nivel y autoridad de responsabilidad dentro 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 DPyP. TRUSTCLOUD ha definido un equipo integrado por los responsables de las diferentes áreas implicadas en cada uno de los pasos del Servicio de Verificación de Identidad.

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 DPyP 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 DPyP 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 y con 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 se realizará 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. 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 Verificación de Identidad quedan registradas en un certificado de evidencias generadas por TRUSTCLOUD. Estas evidencias se entregarán a la finalización del servicio ose entrega al suscriptor previa solicitud.