DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

SERVICIO DE CONTRATACIÓN ELECTRÓNICA:

SignyDocs

CONTROL DE VERSIONES

La presente Declaración de Prácticas de Certificación (DPC) estará disponible de manera permanente a través de la web de ORIGINPATH, en https://www.originpath.com/. Cualquier modificación sustancial en las condiciones de prestación del servicio aquí indicados será reflejado en la web de ORIGINPATH, indicando la versión y fecha del documento, así como una descripción somera de los cambios indicados.

El control de versiones se mantendrá durante 5 años, pudiendo los usuarios solicitar el contenido de todas aquellas versiones que se hayan realizado durante dicho período.

Control de versiones		
Versión	**Fecha del cambio**	**Modificaciones**
1.0	15/10/20	Documento original

ÍNDICE DE CONTENIDOS

1 DEFINICIONES Y ACRÓNIMOS

Para una mayor comprensión del contenido del presente documento se facilita, por orden alfabético, una breve definición de los siguientes términos y acrónimos:

AEPD: Es el acrónimo de Agencia Española de Protección de Protección de Datos. Se trata del organismo de control español encargado de velar por el cumplimiento de la normativa de protección de datos.

Autenticación: Es el proceso de verificación de la identidad de una persona por medio del uso de una solución tecnológica, es decir, la solución tecnológica utilizada para asegurar que alguien es quien dice ser.

Autoridad de Certificación: La Autoridad de Certificación, o CA (Certification Authority) es una entidad destinada a emitir y/o revocar certificados digitales reconocidos por medio de firma electrónica.

Certificado de finalización: Documento emitido bajo la firma electrónica de ORIGINPATH en el que se recogen las evidencias obtenidas en un proceso electrónico de obtención de consentimientos.

Cifrado: Operación o conjunto de operaciones que permiten convertir un mensaje en claro en un mensaje ilegible, excepto para aquél que disponga de la clave de descifrado.

Criptografía: Es la ciencia que estudia la alteración del texto original con el objetivo de que el significado del mensaje solo pueda ser comprendido por su destinatario.

CPD: Acrónimo de "Centro de Proceso de Datos", ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

Dato de carácter personal: El RGPD define dato de carácter personal como *"toda información sobre una persona física identificada o identificable (…)"*[1].

[1] Vid. Art. 4.1 del RGPD.

De este modo:

a Se considera dato personal, por ejemplo, información como: El nombre y apellidos, dirección de e-mail, dirección IP o la cuenta corriente y movimientos bancarios de una persona física.

b No se considera dato personal: Los datos de las personas jurídicas como su NIF, denominación social, datos bancarios… Sin embargo, los datos que permitan identificar a sus socios (personas físicas) y trabajadores sí serán datos de carácter personal.

Empresa-cliente: Hace referencia a cada una de las empresas que contrata con ORIGINPATH el servicio SignyDocs.

eIDAS: Son las siglas inglesas del Reglamento núm. 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicos que viene a establecer, entre otras novedades, un marco jurídico único europeo para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

Evidencias: Hace referencia a todos los elementos acreditativos generados durante un proceso electrónico de obtención de consentimientos que pueden ser utilizadas para acreditar su realidad.

Estas evidencias son obtenidas y custodiados por ORIGINPATH y se reproducen en el certificado de finalización.

Firma electrónica: La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Firma electrónica avanzada: Es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control.

Firma electrónica cualificada: Es aquella firma electrónica avanzada basada en un certificado cualificado y generada mediante un dispositivo cualificado de creación de firma. Posee efectos equivalentes a los atribuidos a la firma manuscrita.

Fuerza mayor: Se entiende por ésta, de conformidad con el artículo 1.105 del Código Civil, cualquier circunstancia sobre la que los intervinientes no puedan tener un control razonable y entre otros: los desastres naturales, la guerra, el estado de sitio, las alteraciones de orden público, la huelga de transportes, el corte de suministro eléctrico y/o telefónico, los virus o ataques informáticos de diversa índole causados por un avance imprevisible de la técnica, las deficiencias en los servicios de telecomunicaciones, o cualquier perjuicio de naturaleza similar.

Función hash: La función hash, o función resumen, es un algoritmo que aplicado a un documento permite obtener un código alfanumérico con las siguientes características:

- Es único, por lo que un mismo documento dará siempre como resultado el mismo código, mientras que, si alguna de las características o contenido del documento ha sido alterado, el código será distinto.

- Es unidireccional, por lo que del código alfanumérico no resulta matemáticamente posible extraer el documento original, según el estado actual de la ciencia.

Se utiliza principalmente para comprobar si un documento ha sufrido modificaciones ulteriores a su firma.

Huella digital: La huella digital es el código alfanumérico obtenido tras haber aplicado la función hash a un documento. En ocasiones también se la denomina “resumen único” o “hash”.

Interesado: Persona física cuyos datos son tratados por el Responsable del Tratamiento para la consecución de una o varias finalidades.

Integridad del contenido: La integridad del contenido se refiere a todo documento o conjunto de datos que no han sido objeto de cambios o alteraciones con posterioridad a su firma.

LSSI: Es el acrónimo con el que se identifica a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico cuyo objeto es la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica.

En su artículo 25 recoge el concepto de Tercero de confianza, el cual será derogado si se aprueba el actual Anteproyecto de Ley Reguladora de determinados aspectos de los servicios electrónicos de confianza.

Prestador de Servicios de Confianza: En atención a la definición contenida en eIDAS será Prestador de Servicios de Confianza *"una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas"*. ORIGINPATH actuará como un Prestador de Servicios de Confianza en el proceso de obtención de consentimientos.

RGPD o Reglamento General de Protección de Datos: Son las siglas del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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.

Servicios de confianza: A los efectos de lo dispuesto en eIDAS, se entenderá por servicio de confianza, "el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

a la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o

b la creación, verificación y validación de certificados para la autenticación de sitios web, o

c la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios";

No obstante, cada uno de los Estados Miembros podrá definir servicios de confianza adicionales. En todo caso nos encontraremos ante servicios que acreditan la realidad de un suceso formalizado a través de medios electrónicos o la identidad de los sujetos intervinientes.

Servicios en la nube (o Cloud Computing): Según determina la Guía para clientes que contraten servicios de Cloud Computing emitida por la AEPD *"En un entorno de cloud computing la gestión de la información está de forma virtual en manos del cliente que contrata los servicios de la nube,*

que la trata a través de Internet accediendo a soluciones de bases de datos, correo electrónico, nóminas o gestión de recursos humanos de acuerdo a sus necesidades". Podemos distinguir tres grandes modalidades de servicios de Cloud Computing:

a Software as a Service (SaaS):

Proporcionan utilidades al usuario para construir aplicaciones, como bases de datos o entornos de programación sobre las que el usuario puede desarrollar sus propias soluciones.

b Infrastructure as a Service (IaaS):

Se caracteriza porque el proveedor proporciona capacidades de almacenamiento y proceso en bruto, sobre las que el usuario ha de construir las aplicaciones que necesita su empresa prácticamente desde cero. Por ejemplo, dentro de Internet, serán IaaS aquellos servicios que proporcionan una capacidad de almacenamiento masivo a través de la red y los servidores de alojamiento web.

c Software as a Service (SaaS):

En este tipo de servicios el usuario encuentra en la nube las herramientas finales con las que puede implementar directamente los procesos de su empresa: una aplicación de contabilidad, de correo electrónico, un *workflow*, un programa para la gestión documental de su empresa, etc.

Repudio: Desde el punto de vista del emisor, el repudio del mensaje supone la negación de haberlo enviado. Por su parte, desde el punto de vista del destinatario se relaciona con la negación de haberlo recibido.

SignyDocs: Servicio de firma electrónica avanzada desarrollada por ORIGINPATH. Esta solución está orientada a facilitar procesos de firma de documentos electrónicos de forma rápida y segura a través de almacenamiento en la nube y uso de certificado.

Usuario-interesado: Hace referencia a cada una de las personas físicas que, a través de SignyDocs, prestan -o deniegan- su consentimiento a una empresa-cliente para el desarrollo de distintas finalidades.

2 SOBRE ORIGINPATH

ORIGINPATH, S.L., (en lo sucesivo, “ORIGINPATH”) nace en el año 2016, como un proyecto de 5 socios con amplia experiencia en proyectos de software de alto rendimiento a servicio de grandes de corporaciones y sociedades en I+D+I.

Desde el inicio de su andadura comercial, ORIGINPATH ha llevado a cabo labores de desarrollo y consultoría de software, así como la realización de formaciones a empresas.

En el desarrollo de esta actividad, ORIGINPATH ha llevado a cabo proyectos de software de amplio recorrido, como es Work4Data, un laboratorio de investigación I+D destinado al desarrollo de soluciones tecnológicas de alto rendimiento y la investigación de nuevos procesos de negocio a través de la tecnología.

Fruto del proceso de mejora continuo en nuestra oferta de servicios y productos, ORIGINPATH quiere implantar en el mercado SignyDocs, una solución de firma electrónica avanzada para la automatización de procesos de firma de contratos y documentos, y que será objeto de descripción detallada en la presente declaración de prácticas de certificación.

3 OBJETO Y MODIFICACIONES

3.1 OBJETO DE LA DPC

En cumplimiento de lo dispuesto en el art. 30.2[2] de la LFE y ajustando el contenido del art. 19[3] de la LFE a los concretos servicios que ofrece ORIGINPATH, se emite la presente Declaración de Prácticas de Certificación (en lo sucesivo "DPC"), la cual será habilitada de manera pública y gratuita en la web de ORIGINPATH a disposición de todos los usuarios. La declaración de esta DPC incluirá información concreta sobre los siguientes aspectos:

- Naturaleza jurídica, características y uso de los servicios ofrecidos por ORIGINPATH: Contratación electrónica certificada, notificación electrónica certificada y custodia digital.
- Derechos y obligaciones asumidos por ORIGINPATH, los usuarios del servicio y el resto de intervinientes.
- Requisitos técnicos exigidos.
- Régimen de responsabilidad asumido y límites.
- Medidas de seguridad técnicas y organizativas aplicadas por ORIGINPATH.
- Política de protección de datos.
- Plan de contingencia y de finalización del servicio.
- Propiedad Intelectual e Industrial de los servicios, los elementos que los integran y aquellos que intervienen de forma conexa.
- Normativa aplicable.

[2] Art. 30.2 de la LFE: *"Los prestadores de servicios de certificación deberán comunicar al Ministerio de Ciencia y Tecnología el inicio de su actividad, sus datos de identificación, incluyendo la identificación fiscal y registral, en su caso, los datos que permitan establecer comunicación con el prestador, incluidos el nombre de dominio de internet, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen. Esta información deberá ser convenientemente actualizada por los prestadores y será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento".*

[3] Art. 19 de la LFE: *"Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta ley y de sus disposiciones de desarrollo, las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros".*

3.2 ACCESO A LA VERSIÓN EN VIGOR

En la página web de ORIGINPATH se publicarán de forma permanente y fácilmente accesible para el usuario medio la DPC que en cada momento se halle en vigor, haciéndose referencia a su versión y su fecha de última actualización. Toda persona que navegue por la web podrá descargar la DPC en vigor de un modo sencillo y gratuito.

3.3 CAMBIOS SUSTANCIALES

A la hora de identificar la DPC se utilizarán las siglas "DPC", seguidas de un número secuencial que haga referencia a la versión y a la subversión y, por último, la fecha en que se emite. Así, siendo ésta la presente la primera DPC, su referencia será "DPC-1.1-1.06.2020". El cambio de versión obedecerá a modificaciones sustanciales de la presente DPC, tales como la inclusión de nuevos servicios de confianza dentro de la oferta de ORIGINTPAH o una actualización que afecte de forma esencial la naturaleza de los servicios ya prestados; por su parte, la subversión hará referencia a modificaciones de carácter menor, como mejoras en la funcionalidad de los servicios.

3.4 ACCESO A LAS VERSIONES ANTERIORES DE LA DPC

Las versiones anteriores de esta DPC estarán alojadas en un repositorio habilitado al efecto, que contendrá un listado con todas las versiones de la DPC previas a la versión en vigor que se hayan publicado durante los últimos 5 años. En caso de precisarse una versión anterior a las contenidas durante este período, y siempre que exista una causa justificada para ello, el usuario podrá solicitarlo expresamente a ORIGINPATH, formulando su petición por escrito a través de la siguiente dirección: administración@originpath.com

4 SERVICIO OBJETO DE LA DPC Y SUS CARACTERÍSTICAS

4.1 INTRODUCCIÓN

El servicio de notificación electrónica se ofrece como una solución destinada a proporcionar a los usuarios un sistema de notificación fehaciente a través de e-mail o SMS que permita monitorizar y registrar todos los eventos que se produzcan hasta la fecha y hora en que la comunicación fue puesta a disposición del destinatario. Adicionalmente, se pueden incluir funcionalidades accesorias que permitan registrar el momento en que el destinatario accedió al contenido de la comunicación.

4.2 INTERVINIENTES

- **El Prestador de Servicios de Confianza**

ORIGINPATH llevará a cabo la prestación del presente servicio, a través de su propia solución, configurada en formato SaaS. Por su parte, la generación de las evidencias y la emisión del certificado será provisto por un Proveedor de Servicios de Confianza cualificado.

- **El usuario/emisor**

El emisor de la comunicación será la persona que, a través del entorno seguro habilitado por ORIGINPATH, identifica el destinatario y ordena el envío de la comunicación.

- **El firmante/destinatario**

El destinatario es el receptor de la comunicación. SignyDocs permite la participación de varios firmantes en un mismo documento.

- **La Autoridad de Certificación**

Es la empresa responsable de emitir y revocar el certificado reconocido que vincula los datos de verificación de firma de ORIGINPATH y confirma su identidad, permitiendo rubricar con su firma electrónica cualificada el certificado de finalización.

4.3 DESCRIPCIÓN FUNCIONAL DEL PROCESO DE FIRMA A TRAVÉS DE SIGNYDOCS

FASE 1: Generación y maquetación del documento

En primer lugar, el emisor debe seleccionar un documento en formato .pdf, que deberá cargar dentro de la plataforma. Una vez alojado el documento, el usuario tendrá la posibilidad de configurar plantillas e insertar "cajas" (espacio alojado para la firma de los intervinientes).

Una vez el documento está listo para su envío, el emisor deberá cargar los datos del/los destinatario/s de la comunicación. Para ello, deberá indicar el nombre, mail y teléfono de contacto donde se recibirá la solicitud de firma. Adicionalmente, se podrá incorporar información adicional durante el proceso de firma, como la localización donde se produce la misma a través de la geolocalización del dispositivo (en caso de que el remitente así lo indique en la configuración del proceso de firma).

FASE 2: Remisión y recepción del documento

Una vez indicados los datos del firmante, el documento será remitido al destinatario vía mail. El destinario tendrá a su disposición un enlace a la plataforma de SignyDocs, para poder acceder a su contenido.

Dado que SignyDocs ofrece la posibilidad de realizar multifirma en un documento, el archivo podrá ser remitido a varios destinatarios, por lo que habrá varias casillas de firma a cumplimentar y varias direcciones de mail a las que remitir el documento para que se perfeccione el acto jurídico que se pretenda realizar.

FASE 3: Firma del documento

El acceso a la plataforma puede realizarse de dos formas:

- Acceso directo a la plataforma a través del enlace. El usuario puede acceder al contenido del documento directamente desde el enlace.
- Acceso mediante OTP. Si el remitente así lo ha seleccionado durante el proceso de generación y envío del documento, deberá introducir una clave de acceso que habrá recibido en su móvil vía SMS.

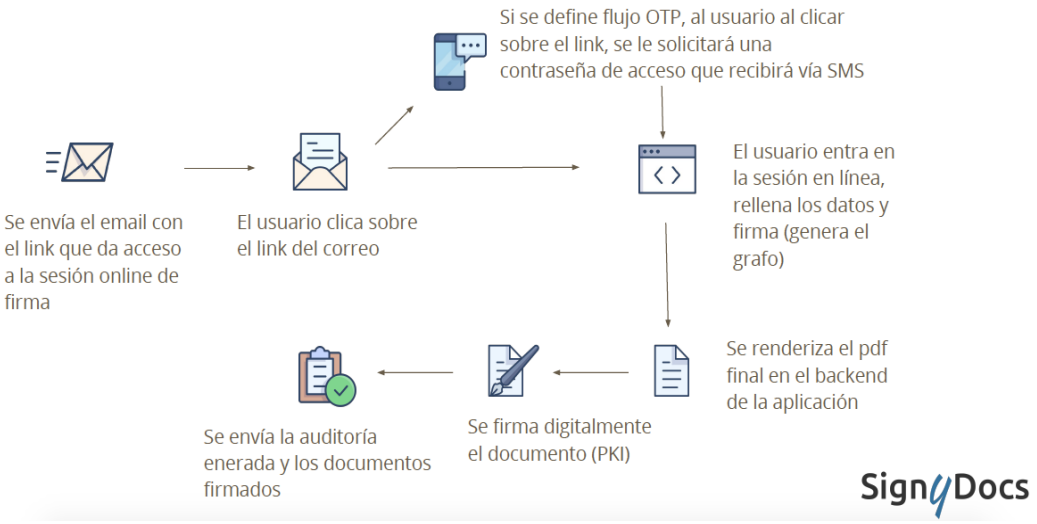

Figure 1 Flujo funcional de SignyDocs

Con independencia del modo de acceso, el destinatario accede a un interfaz en la que cumplimentará los datos necesarios para la firma del documento, incluyendo la traza de la firma (grafo).

Una vez cumplimentado el documento, cada una de las partes recibirá una copia del documento.

FASE 5: Generación de evidencias

En paralelo a todo el proceso de firma del documento, ORIGINPATH recaba todas las evidencias necesarias para acreditar la traza en cada uno de los hitos del proceso de firma. De esta forma, los datos cumplimentados por el/los firmante/s son remitidos, vía https, al backend de

ORIGINPATH, de manera que son únicamente accesibles para el personal de ORIGINPATH. La información recabada incluye los datos de envío y entrega de los correos electrónicos a través de la información generada por el proveedor de mensajería del interviniente (metadatos), lo que incluye la fecha y otra del envío, el resultado de la comunicación, los datos del navegador o la IP asociada a cada usuario.

Toda esta información se recopila en un certificado (denominado internamente "auditoría del documento") en el que dicha información queda asociada a una denominación del archivo, un código de envío, así como los datos del destinatario indicados con anterioridad.

La auditoría del documento se certifica a través de la aplicación de un sistema de infraestructura de clave pública (PKI) a través de un certificado cualificado de un prestador de servicios de confianza, incluyendo un sellado de tiempo (o *timestamp*) en el que refleja la fecha y hora de emisión del certificado asociado a dicho contenido.

FASE 6: Custodia

El certificado y los documentos asociados al mismo son custodiados por ORIGINPATH durante un período de 5 años, sin perjuicio de la aplicación de otros plazos superiores si así lo interesara el cliente.

Esta fase de custodia se ejecuta a través del sistema de almacenamiento de acceso lento de AMAZON WEB SERVICES (AWS).

5 OBLIGACIONES Y RESPONSABILIDAD DE LOS INTERVINIENTES

5.1 POR PARTE DE ORIGINPATH

5.1.1 OBLIGACIONES DE ORIGINPATH

ORIGINPATH como Prestador de Servicios de Confianza se compromete a cumplir las siguientes obligaciones:

Obligaciones con respecto al servicio de confianza:

ORIGINPATH se compromete, con carácter general, a cumplir con todas las obligaciones establecidas en la normativa eIDAS y, en particular:

- Garantizar el correcto funcionamiento del servicio y los estándares marcados por eIDAS.
- Garantizar los niveles de prestación del servicio acordados particularmente con los clientes de ORIGINPATH. La aplicación de esta última obligación se incardina dentro de las disposiciones de la normativa civil y, particularmente, la buena fe contractual; por motivo de lo anterior, las obligaciones asumidas por ORIGINPATH no serán de aplicación en supuestos de fuerza mayor, sin perjuicio de las condiciones particulares y que sus servicios se presten conforme a lo aquí establecido, amén de dar cumplimiento a todas las prestaciones que particularmente puedan acordarse con sus clientes o así se refleje en las condiciones generales de uso de SignyDocs.
- ORIGINPATH dispondrá de los medios materiales, técnicos y humanos que sean necesarios para prestar el servicio en las condiciones ofertadas. Esta obligación incluye la previsión de contar con una entidad que disponga de un certificado cualificado de firma electrónica y con todos los medios técnicos y humanos necesarios para la debida prestación de los servicios indicados.
- ORIGINPATH informará de cualquier incidencia en el servicio, incluyendo interrupciones no programadas o la producción de un incidente de seguridad.
- Informar y publicar cualquier modificación sustancial en las condiciones de prestación del servicio.

Obligaciones con respecto al tratamiento de datos personales:

Con carácter general, ORIGINPATH asume el compromiso de cumplir con lo dispuesto en la normativa de protección de datos vigente, con especial atención a lo dispuesto en el RGPD y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales. Expresamente, ORIGINPATH se compromete a cumplir con las siguientes obligaciones:

- Cumplir con los deberes de información y transparencia, de acuerdo con lo establecido en los arts. 12 y siguientes del RGPD.
- Contar con un Registro de Actividades del tratamiento que incluya las finalidades identificadas en la ejecución del servicio objeto de esta DPC.
- Con carácter adicional a lo anterior, ORIGINPATH llevará a cabo una evaluación de los riesgos inherentes a los tratamientos de datos objeto del servicio y, en su caso, realizará las oportunas evaluaciones de impacto en la privacidad para aquellos tratamientos que puedan suponer un riesgo para los derechos de los usuarios que así lo requiera.
- ORIGINPATH implantará las medidas de seguridad técnicas y organizativas que resulten exigibles conforme a los riesgos identificados en el tratamiento de datos objeto del servicio.
- No permitir el acceso a los datos gestionados por cuenta de terceros si estos no se comprometen a cumplir el nivel de seguridad exigido y las obligaciones de confidencialidad adoptadas por ORIGINPATH.
- Informar a los usuarios afectados y, en caso de ser necesario, al organismo administrativo competente ante la producción de brechas de seguridad.

Otras obligaciones:

- Mantener actualizada la DPC y publicar las modificaciones conforme al procedimiento establecido en el inicio de la presente DPC.
- Colaborar y cooperar ante cualquier actuación o requerimiento por parte de un organismo administrativo o judicial competente.

- Informar al usuario de forma clara y comprensible de las condiciones relativas a la utilización de cada uno de los servicios.
- Garantizar el ejercicio de los derechos propios de los consumidores y usuarios si fueran de aplicación al concreto cliente.
- Recoger los precios finales de sus servicios, incluyendo de forma detallada cualquier impuesto aplicable y los gastos o descuentos adicionales.

5.1.2 RESPONSABILIDAD DE ORIGINPATH

De conformidad con lo dispuesto en el art. 22 de la LFE, ORIGINPATH será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica por razón del incumplimiento de las obligaciones asumidas.

No obstante lo anterior, no será responsable frente al cliente por daños indirectos, lucro cesante, pérdidas ingresos o beneficios o conceptos similares, a no ser que tales responsabilidades no pudieran ser limitadas por aplicación de una norma de carácter imperativo. En ningún caso, ORIGINPATH será responsable en supuestos de fuerza mayor.

Si bien la presente obligación, conforme a lo dispuesto en el art. 24 eIDAS, solo deberán suscribir una póliza de seguro los prestadores de servicios de confianza cualificados. No obstante, ORIGINPATH tiene contratada una póliza de seguro por responsabilidad civil para sus servicios de confianza, cuya cobertura asciende a un total de seis cientos mil (600.000) euros.

5.2 POR PARTE DE LOS USUARIOS

5.2.1 OBLIGACIONES DE LOS USUARIOS

Los usuarios de los servicios ofrecidos por ORIGINPATH se comprometen a cumplir las siguientes obligaciones:

Obligaciones de uso:

- Usar los servicios proporcionados por ORIGINPATH de forma responsable y con los fines para los que se le han facilitado conforme a sus especificaciones técnicas y condiciones de uso.
- No utilizar los servicios de ORIGINPATH para la comisión de actividades ilícitas o en perjuicio de ORIGINPATH o terceros.

  ORIGINPATH no supervisa el contenido de los documentos que se intercambian o archivan a través de su sistema por lo que es responsabilidad exclusiva del usuario garantizar su licitud.
- Actuar con la debida diligencia en la guarda y custodia de las claves que le sean proporcionadas para el uso de los servicios de ORIGINPATH e informar ante cualquier sospecha sobre la pérdida o usurpación de las mismas.
- Mantener sus equipos informáticos suficientemente protegidos frente a las amenazas externas e internas.
- Emplear personal que cuente con una formación suficiente para el manejo del servicio ofrecido por ORIGINPATH.

Obligaciones económicas:

- Abonar el precio pactado por la recepción de los servicios en el plazo y forma que se estipulen.

Obligaciones de información:

- Suministrar a ORIGINPATH toda información que éste considere necesaria para la correcta prestación de los servicios contratados y el cumplimiento de las obligaciones asumidas.
- Proporcionar información veraz y mantenerla permanentemente actualizada.
- Informar a ORIGINPATH sobre cualquier incidencia relacionada con la prestación del servicio.

5.2.2 RESPONSABILIDAD DE LOS USUARIOS

El usuario será responsable por los daños y perjuicios que su comportamiento negligente o doloso pudiera ocasionar a ORIGINPATH.

La obligación de pago resulta esencial para la continuidad del servicio por lo que ORIGINPATH podrá suspender su prestación habiendo transcurrido un mes sin que se hubiera procedido al abono acordado.

5.3 LA AUTORIDAD DE CERTIFICACIÓN

La Autoridad de Certificación no establece relación alguna ni con el emisor, ni con el destinatario. Su actividad y régimen de responsabilidad en relación con la emisión y gestión del certificado del que hace uso ORIGINPATH se regirá por la Declaración de Prácticas de Certificación emitidas por la propia Autoridad y el contrato de prestación de servicios de certificación digital o condiciones generales de uso que se formalizaran.

6 POLÍTICA DE PROTECCIÓN DE DATOS

Considerando el impacto que la presente actividad implica en relación con el tratamiento de datos personales que va a llevar a cabo en el desarrollo de sus servicios, ORIGINPATH ha elaborado la presente política de privacidad, que será de aplicación a todo tratamiento que se desarrolle en el contexto de los servicios de confianza de la compañía, y que estará a disposición de sus usuarios de manera clara y accesible.

POLÍTICA DE PRIVACIDAD EN LA PRESTACIÓN DE SERVICIOS DE CONFIANZA ELECTRÓNICA

La presente política de privacidad se elabora de conformidad con lo dispuesto en la vigente normativa de protección de datos personales y, en particular, las obligaciones establecidas en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO 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 (RGPD, en adelante), con relación a los servicios de confianza ofrecidos por ORIGINPATH.

Esta política de privacidad podrá ser objeto de modificaciones y actualizaciones, en cuyo caso se referirá de modo expreso la fecha a partir de la cual se encuentra vigente la última versión publicada.

¿QUIÉN ES EL RESPONSABLE DE SUS DATOS?

El responsable del tratamiento de sus datos personales es la sociedad Originpath, S.L., con N.I.F. B-87624888 y domicilio social en C/ los Nardos 12, 3ºA, Alcorcón, 28925, Madrid.

Con el fin de garantizar el adecuado cumplimiento de la normativa de protección de datos personales, ORIGINPATH ha nombrado un delegado de protección de datos (DPO) al que podrá dirigirse para plantear cualquier cuestión relativa al tratamiento de sus datos personales. Para ello, podrá remitir sus consulta o petición con el asunto “Protección de datos” a la siguiente dirección electrónica: rgpd@originpath.com

¿CON QUÉ FINALIDAD TRATAMOS SUS DATOS Y SOBRE QUÉ BASE LEGITIMADORA LO HACEMOS?

ORIGINPATH tratará sus datos para la realización de las siguientes finalidades:

- En base a la ejecución de relaciones contractuales o precontractuales: Por motivo de la ejecución de los servicios ofertados por ORIGINPATH que usted haya contratado o interese contratar en un futuro, podremos tratar sus datos para:

    1 Desarrollar los servicios de confianza electrónica contratados por el interesado.
    2 Gestionar las consultas y solicitudes que podamos recibir a través de los medios habilitados a tal fin, lo que implica la gestión de relaciones precontractuales por parte de ORIGINPATH.

- En base al consentimiento otorgado: En caso de que otorgue el oportuno consentimiento al efecto a través de alguno de los medios habilitados para ello, podremos usar sus datos para:

    1 Realizar un perfil de su persona con el fin de realizar estudios estadísticos y comportamentales destinados a conocer sus hábitos y preferencias como usuario de nuestros productos y servicios.
    2 Enviarle información comercial de ORIGINPATH basada en su perfil, con el fin de darle a conocer otros productos y servicios de ORIGINPATH que puedan ser de su interés.

¿QUÉ TIPO DE DATOS TRATAMOS?

La ejecución de los servicios de confianza de ORIGINPATH implica el tratamiento de las siguientes categorías de datos:

- Datos identificativos, como el nombre o apellidos del interesado.

- Datos de contacto, como son el mail o el número de teléfono de los usuarios de nuestros servicios.
- Datos biométricos, como es la captación del trazo utilizado para representar la firma de los participantes.
- Otros, como son los datos derivados de las acciones de navegación que lleva a cabo durante la navegación por nuestra web.
- Datos de geolocalización, en caso de otorgar los consentimientos oportunos (en el dispositivo empleado) y en caso de que el gestor del proceso de firma electrónica configure el parámetro de activación de la geolocalización de los firmantes.

Todos estos datos son obtenidos directamente del interesado, bien de forma directa a través de la propia acción del usuario, o de forma indirecta, como es a través de las cookies y la información habilitada por el usuario durante su navegación.

¿DURANTE CUÁNTO TIEMPO TRATAREMOS SUS DATOS?

Sus datos serán tratados en tanto se mantenga la vigencia de los servicios prestados por ORIGINPATH. Una vez cumplida dicha finalidad, los datos se mantendrán bloqueados durante los plazos legalmente exigidos, momento a partir del cual se procederá a su definitiva supresión. Con carácter general, y considerando la naturaleza de la relación que se puede formalizar entre usted y ORIGINPATH, sus datos podrán ser conservados durante un período de 5 años, conforme a los plazos de prescripción de reclamaciones establecido en la normativa civil.

¿A QUIÉN COMUNICAREMOS SUS DATOS?

La ejecución de los servicios de confianza electrónicos de ORIGINPATH no implicará la comunicación de datos a terceros, salvo en aquellos supuestos en los que, por cumplimiento de las obligaciones legales que nos son de obligación, deban comunicarse por aplicación de algún precepto legal o por requerimiento de una Autoridad competente.

No obstante, debemos indicar que, en el contexto de nuestros servicios, ORIGINPATH puede tener la necesidad de externalizar parte de los mismo a terceras entidades para poder garantizar

el adecuado desarrollo de las condiciones acordadas con sus usuarios. Esta acción se formalizará conforme a las exigencias de la normativa de protección de datos y, si bien esta acción se considera una comunicación de datos a terceros, a continuación le indicamos los datos de las sociedades que participan de nuestra actividad:

- **AMAZON WEB SERVICES SPAIN, S.L.:** CIF B-86339595. Vía De La Dos Castillas, 33. CP 28224 de Pozuelo de Alarcón (MADRID). Esta entidad gestiona los servicios de almacenamiento y custodia de las evidencias que generamos durante nuestros servicios.
- **MASVOZ TELECOMUNICACIONES INTERACTIVAS, S.**L.U. (TWILIO para España): con N.I.F B 62959077 y domicilio social en Travessera de Gràcia 17-21, 1ª planta, 08021, Barcelona (España). Esta entidad gestiona el envío de SMS.

En cualquier caso, ninguna de las comunicaciones de datos o servicios externalizados por ORIGINPATH implicara la comunicación de sus datos fuera del Espacio Económico Europeo. Los servidores del proveedor AWS se encuentran ubicados en Francia.

¿QUÉ DERECHOS LE ASISTEN?

Conforme a lo dispuesto en la normativa de protección de datos personales, le informamos sobre los derechos que le asisten con relación al tratamiento de sus datos personales:

- Tiene derecho a ACCEDER a sus datos, conociendo qué información tratamos sobre usted y para qué fines.
- Tiene derecho a OPONERSE al tratamiento de sus datos, en aquellos supuestos que así se lo habiliten.
- Tiene derecho a la RECTIFICACIÓN de sus datos, pudiendo solicitar la corrección o modificación de cualquier información que sea imprecisa.
- Tiene derecho a solicitar a SUPRESIÓN de sus datos. En su caso, procederemos a su bloqueo conforme a los plazos legalmente establecidos antes de proceder a su definitiva destrucción.

- Tiene derechos a solicitar la PORTABILIDAD de sus datos a través de un formato estructurado y de uso común que permita su comunicación a otro responsable del tratamiento.
- Bajo ciertas condiciones, tiene derecho a solicitar la LIMITACIÓN del tratamiento de sus datos tales como, por ejemplo, cuando dichos datos sean objeto de una rectificación, en tanto dicha acción se concrete.
- Tiene derechos a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD), en caso de que considere que sus datos personales no han sido tratados conforme a lo dispuesto en la normativa aplicable.

7 ENCARGO DEL TRATAMIENTO

Los servicios prestados por ORIGINPATH, que se desarrollan por petición expresa de una de las partes intervinientes, tienen encaje en el desarrollo de una relación de encargo del tratamiento. Ello obedece a la circunstancia de que la participación de ORIGINPATH implica que su intervención como Prestador de Servicios de Confianza quede supeditada a la ejecución de una tarea cuyos fines y propósitos son determinados por el cliente de ORIGINPATH, que ostenta la consideración de responsable del tratamiento.

Esta situación no afecta a las garantías de imparcialidad ni la presunción de veracidad de las acciones acometidas por ORIGINPATH ya que, conforme a lo dispuesto en el art. 25 LSSI, es una actuación expresamente reconocida en la normativa aplicable en la que únicamente se podrán generar las oportunas evidencias de los efectivamente acordado por las partes.

Debido a lo anterior, ORIGINPATH formaliza la ejecución de sus servicios conforme al modelo que se facilita a continuación, sin perjuicio de las acciones específicas que se puedan acordar particularmente con cada cliente.

CONTRATO DE ENCARGO DE TRATAMIENTO

Como complemento al contrato firmado entre las partes (en adelante, el Contrato) el [-] entre ORIGINPATH (en adelante, ENCARGADO) y _____ (en adelante, el RESPONSABLE o el CLIENTE), se pacta entre ambas partes el siguiente contrato de encargo de tratamiento.

1 **Objeto.**

El presente acuerdo tiene por objeto definir las condiciones conforme a las cuales el ENCARGADO llevará a cabo el tratamiento de datos personales que resulten necesarios para la prestación de los servicios objeto del Contrato, y del que el presente Contrato de Encargo de Tratamiento trae causa.

2 **Obligaciones del ENCARGADO.**

El ENCARGADO DE TRATAMIENTO, llevará a cabo el tratamiento de datos personales derivado de la prestación del servicio contratado, de conformidad con las siguientes obligaciones:

- Limitarse a realizar, exclusivamente, las actuaciones que resulten necesarias para prestar al RESPONSABLE el Servicio contratado, sometiéndose a las instrucciones que le indique, inclusive con respecto a las transferencias de datos personales a un tercer país o a una organización internacional salvo el caso de cumplimiento de una obligación legal, en tal caso, informará al RESPONSABLE de esa exigencia legal previa al tratamiento.

  Si el ENCARGADO considera que alguna instrucción infringe la legislación vigente, informará inmediatamente al RESPONSABLE.

- Mantener un registro, por escrito, de todas las actividades de tratamiento efectuadas por cuenta del RESPONSABLE, que contenga al menos: identificación de autorizados; categorías de tratamientos y una descripción general de las medidas técnicas y organizativas de seguridad adoptadas.

- Comprometerse a guardar bajo su control y custodia los datos personales accedidos y a no comunicarlos en modo alguno a terceros.

- Dar apoyo al RESPONSABLE en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda, así como en la realización de las consultas previas a la autoridad de control, cuando proceda.

- Poner a disposición del RESPONSABLE toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el RESPONSABLE u otro auditor autorizado por él.

- Asistir al RESPONSABLE en la respuesta al ejercicio de los derechos de los interesados debiendo dar traslado de la solicitud de forma inmediata y, a no más tardar, dentro del plazo de tres días naturales a contar desde su recepción.

3 **Seguridad de los datos personales.**

El ENCARGADO implantará las medidas de seguridad y mecanismos establecidos en el artículo 32 del RGPD para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en su caso.

Asimismo, el ENCARGADO DE TRATAMIENTO deberá adoptar todas aquellas medidas técnicas y organizativas que, a tenor del análisis de riesgo efectuado por el RESPONSABLE, éste considere que resultan necesarias para garantizar un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

4 Notificación de violaciones de la seguridad de los datos.

El ENCARGADO deberá notificar al RESPONSABLE, sin dilación indebida, y en cualquier caso antes del plazo máximo de 72 horas, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, incluyendo toda la información relevante para la documentación y comunicación de la incidencia.

El ENCARGADO facilitará, como mínimo, la descripción de la naturaleza de la violación de la seguridad de los datos personales, el punto de contacto en el que pueda obtenerse más información, análisis de las posibles consecuencias de la violación de la seguridad de los datos personales y descripción de las medidas adoptadas o propuestas para mitigar los posibles efectos negativos.

Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5 **Deber de confidencialidad.**

El ENCARGADO queda obligado a guardar secreto durante la vigencia del contrato y, en función de la tipología de información de que se trate, durante los plazos máximos previstos en la legislación vigente. Asimismo, garantizará que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de lo que informará al RESPONSABLE poniendo, además, a su disposición la documentación acreditativa del cumplimiento de esta obligación.

6 **Deber de información.**

Corresponde al RESPONSABLE facilitar el derecho de información en el momento de la recogida de los datos.

7 **Obligación de devolución de los datos.**

Una vez cumplida la prestación del servicio objeto del Contrato, el ENCARGADO se compromete a destruir aquella información que contenga datos de carácter personal que haya sido transmitida por el RESPONSABLE al ENCARGADO con motivo de la prestación del Servicio. Una vez destruidos, emitirá un certificado de destrucción al RESPONSABLE donde se relacionará la información, soportes físicos y documentación destruidos. Sin perjuicio de lo anterior, el ENCARGADO podrá conservar, una vez finalizada la relación mantenida con el RESPONSABLE, los datos personales afectados por la prestación de los servicios, debidamente bloqueados, en cumplimiento de obligaciones legales y ante la posibilidad de ser necesarios para el ejercicio, formulación o defensa de acciones y reclamaciones, durante el plazo legal que sea fijado en cada caso o durante el tiempo que resulte preciso para dichas finalidades.

8 **Subcontratación.**

El ENCARGADO no recurrirá a otro encargado sin la autorización previa por escrito del RESPONSABLE. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al RESPONSABLE, indicando los tratamientos que se

pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto.

Corresponde al ENCARGADO inicial regular la nueva relación de conformidad con el artículo 28 del RGPD, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas.

En el caso de incumplimiento por parte del subencargado, el ENCARGADO inicial seguirá siendo plenamente responsable ante el RESPONSABLE en lo referente al cumplimiento de las obligaciones.

El RESPONSABLE autoriza expresamente al ENCARGADO a sub-contratar con los siguientes proveedores:

- **AMAZON WEB SERVICES SPAIN, S.L.:** CIF B-86339595. Vía De La Dos Castillas, 33. CP 28224 de Pozuelo de Alarcón (MADRID). Esta entidad gestiona los servicios de almacenamiento y custodia de las evidencias que generamos durante nuestros servicios.
- **MASVOZ TELECOMUNICACIONES INTERACTIVAS, S.**L.U. (TWILIO para España): con N.I.F B 62959077 y domicilio social en Travessera de Gràcia 17-21, 1ª planta, 08021, Barcelona (España). Esta entidad gestiona el envío de SMS.

9 Responsabilidades.

Si el ENCARGADO infringe lo establecido en el RGPD al determinar los fines y medios del tratamiento será considerado responsable del tratamiento con respecto a dicho tratamiento, debiendo mantener indemne al RESPONSABLE de cualquier daño ocasionado como consecuencia del incumplimiento del presente acuerdo.

Y en prueba de conformidad con cuanto antecede y con voluntad de obligarse desde su fecha, las partes firman el presente documento en duplicado ejemplar en el lugar y fecha indicados.

D/Dña _____

El RESPONSABLE

D/Dña _____

El ENCARGADO

8 MEDIDAS DE SEGURIDAD APLICADAS

El presente apartado refleja el conjunto de medidas técnicas y organizativas que ORIGINPATH aplicará en la ejecución del servicio identificado en la presente DPC, cuyo catálogo está basado en el Esquema Nacional de Seguridad (ENS) y en base a la evaluación de impacto en la privacidad (PIA) adjunto.

BASES DE DATOS

- Los administradores de Bases de Datos, o aquel personal que realice labores de mantenimiento de Bases de Datos mantendrán, en todo momento, la integridad y la estabilidad de las Bases de Datos.

CIFRADO

- Se aplicarán técnicas de cifrado en aquellos repositorios de información que así lo requieran, especialmente con relación al tratamiento de datos personales o aquella información relacionada con la ejecución del servicio informado en la presente DPC.
- En todos los sistemas donde exista información cifrada, existen procedimientos que aseguren el acceso a las claves de cifrado por parte de ORIGINPATH cuando sea necesario.

CONTROL DE ACCESO

- Se establece un protocolo de Gestión de Identidades.
- El acceso a la información, bases de datos, sistemas, plataformas y aplicaciones, se fundamenta en Roles/Perfiles y en Permisos de Acceso, Exigiendo la identificación inequívoca y personalizada de los usuarios.
- Los privilegios de acceso son los mínimos indispensables y estrictamente necesarios para el desarrollo de las funciones asociadas a cada Rol/Perfil.
- Existen Listas de Control de Accesos sobre recursos o funciones de los sistemas. Estas listas incluyen los distintos perfiles de acceso que se hayan definido.

- Los usuarios con acceso a la información, sistemas, plataformas, aplicaciones y/o bases de datos que tengan permisos de administración, deberán firmar el Acuerdo de Confidencialidad.

CONFIGURACIÓN Y CAMBIO DE LOS SISTEMAS DE LA INFORMACIÓN

- Las modificaciones de los sistemas y/o aplicaciones que afecten a ORIGINPATH, deberán ser autorizadas por el departamento de seguridad lógica de ORIGINPATH y se deberán llevar a cabo de forma coordinada con las todas áreas implicadas, informando con suficiente antelación.
- Las modificaciones deberán estar adecuadamente argumentadas, planificadas, se realizarán copias de seguridad de toda la información, se realizarán pruebas a nivel de sistema y de aplicación según corresponda, y se detallará un mecanismo de *rollback*.
- Existen procedimientos operativos para la realización de cambios de emergencia.

ACTUALIZACIONES DE SEGURIDAD

- Las modificaciones y/o actualizaciones de seguridad (*patches*) para resolver errores (*bugs*), procederán de fuentes confiables y serán probadas antes de su despliegue en los sistemas en producción.

GESTIÓN DE COPIAS DE RESPALDO

- Las copias de respaldo de los sistemas de información se realizan asegurando la recuperación total del sistema ante cualquier eventualidad, salvaguardando en cada una de las fases del ciclo de vida del dato, la confidencialidad e integridad de la información tratada.
- Cuando se efectúan copias de respaldo, se realizan pruebas de funcionamiento.
- La periodicidad en la realización de las copias de seguridad y su período de conservación, son los determinados por la legislación vigente.
- Las medidas de Seguridad de las Copias de Respaldo serán como mínimo las mismas que las de la información de la que son copia.

CONTINUIDAD DEL SERVICIO PRESTADO

- Se dispone de un procedimiento de coordinación ante incidentes y desastres que puedan afectar a los sistemas de ORIGINPATH.

GESTIÓN DE INCIDENTES

- Se dispone de un plan de gestión de incidentes de seguridad en el que se detallan los criterios para la priorización de los incidentes, medidas de contención, etc.
- Será necesario notificar de forma inmediata y por escrito, la existencia (o sospecha, duda o conocimiento) de cualquier "Brecha de Seguridad" en el sentido de toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita, la pérdida y la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, conservados o tratados de otra forma o la comunicación o acceso no autorizados a dichos datos y colaborará en la recopilación de la información necesaria que permita analizar si tiene la obligación de reportar dicha Brecha de Seguridad al órgano de control correspondiente.

SEGURIDAD EN LAS INTEGRACIONES

- La conexión desde cualquier red externa se realizará mediante VPN, con mecanismos robustos de autenticación y cifrado.

SEGURIDAD DE CONTRASEÑAS

- Las contraseñas almacenadas o transmitidas por cualquier sistema de información serán cifradas.
- La política de contraseñas establece, al menos:
    - Una longitud mínima de 8 caracteres.
    - La combinación diferentes tipos de caracteres tipográficos: mayúsculas, minúsculas, números y caracteres especiales.
    - No se permite la generación de contraseñas formadas por secuencias de caracteres fácilmente predecibles.
    - Las contraseñas tendrán caducidad, pudiendo establecer ORIGINPATH el plazo máximo de vigencia.
- La entrega de contraseña, después de la creación de una cuenta de usuario, se realizará

mediante un medio seguro y privado al peticionario de la solicitud.

- Será necesario que se fuerce el cambio de contraseña en el primer acceso al sistema.
- No se permitirá la visualización de las contraseñas cuando estén siendo introducidas.
- Las sesiones quedarán bloqueadas mediante contraseña a partir de treinta minutos de inactividad.

SEGURIDAD EN DOCUMENTOS

- Almacenamiento: Los documentos deberán almacenarse en soportes o dispositivos que aseguren su tratamiento dentro del entorno tecnológico que use ORIGINPATH, evitando así que cualquier obsolescencia tecnológica del soporte pueda crear una indisponibilidad de la información almacenada.
- Destrucción: Se deberá entregar a ORIGINPATH un Certificado de Garantía de Destrucción de los documentos acreditando la completa eliminación de la información contenida en los mismos.

SEGURIDAD EN LAS INFRAESTRUCTURAS

- Será necesario garantizar, y documentar, la Seguridad Física y de la Información en las infraestructuras del Centro de Datos:
    - Nivel de Certificación TIER 3.
    - Certificaciones de Seguridad.
    - Bastionado de los servidores y parcheado actualizado.

PRUEBAS DE LOS SISTEMAS

- Se pondrá a disposición entornos de Desarrollo/Pruebas, y entornos de Preproducción, teniendo estos últimos una configuración y seguridad iguales a las del entorno de Producción, en la medida de lo posible.
- Las pruebas relativas a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

9 PLAN DE CONTINGENCIA

ORIGINPATH utiliza en sus datacenters sistemas de diagnóstico para detectar y dar solución a los eventos que repercuten negativamente en el negocio. La detección de incidencias, su gestión y resolución son servicios que están activos 24 horas al día, los 7 días de la semana y los 365 días del año.

Con el plan de contingencia se persigue asegurar la continuidad en los procesos de negocio necesarios para el funcionamiento de los servicios que ofrece ORIGINPATH a sus clientes.

El plan de contingencia consta de las siguientes fases:

- Fase de Detección y evaluación.
- Fase de Restablecimiento.
- Fase de Restauración del servicio.

En caso de producirse cualquier circunstancia que redujese los niveles de seguridad de la información se aplicará el plan de contingencia.

Se hará un análisis del impacto que ha tenido la incidencia de seguridad en el negocio, en base al cual se trazará una estrategia de recuperación. En el análisis se establecerán las causas y descripción de la incidencia, su nivel de impacto, criticidad y las soluciones que se proponen.

10 PLAN DE CESE DE ACTIVIDAD

En el caso de ORIGINPATH cesara en las actividades detalladas en la presente DPC, notificará a todos los clientes de sus servicios el susodicho cese con una antelación mínima de 3 meses, salvo causa sobrevenida que impida cumplir con dicho plazo.

En el escrito de notificación de cese de actividad, ORIGINPATH podrá proponer la transferencia de la gestión de los servicios a otro prestador, identificándolo debidamente e informando sobre sus características. Si el cliente otorga su consentimiento expreso se procederá a transmitir todos los archivos custodiados, los logs de los procesos seguidos y cualquier otro material que se hallase en su poder.

Completado este proceso, o si el cliente no contestase a la notificación de fin de actividad en el plazo de 3 meses desde su recepción, ORIGINPATH procederá a la destrucción completa del material archivado en su sistema.

Asimismo, comunicará al Autoridad competente dicho cese y el destino que va a dar a los archivos y resto de documentación gestionada con una antelación mínima de 2 meses.

En todo caso, en el proceso de fin de actividad se seguirá lo dispuesto en el art. 21 de la LFE o en la normativa que, en su caso, la sustituyese.

11 NORMATIVA Y JURISDICCIÓN APLICABLE

Los servicios que se detallan en la presente DPC y toda reclamación judicial o extrajudicial que de los mismos pudiera derivarse se regirán por la legislación española, salvo que una norma de carácter imperativo dispusiera lo contrario.

Salvo que una norma de derecho imperativo dispusiera lo contrario, los usuarios acuerdan que todo litigio, discrepancia o reclamación que pudiera derivarse directa o indirectamente de cualquiera de los servicios relacionados en la presente DPC se someterá a los Juzgados y Tribunales de la villa de Madrid. A estos efectos, los usuarios renuncian de manera expresa a los fueros propios que les pudiera corresponder.