DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Servicio de contratación electrónica:
Signyourdocs

Abril 2023

ORiGiNPATH

CONTROL DE VERSIONES

La presente Declaración de Prácticas de Certificación estará disponible de manera permanente a través de la web de:

(i) ORIGINPATH, accesible a través de https://www.originpath.com/

(ii) la web específica de Signyourdocs, accesible a través de www.signyourdocs.com.

Cualquier modificación sustancial en las condiciones de prestación del servicio aquí indicados será reflejada en las anteriores páginas web, 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
2.0	12/11/21	Actualización de referencias normativas
3.0	27/04/2023	Actualización del nombre comercial de la solución de firma electrónica, de la política de privacidad y de las condiciones de encargo de tratamiento, aplicables a contrataciones posteriores a la fecha del cambio

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 generación de firma.
- **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 Reglamento (UE) 2016/679, General de Protección de Datos ("**RGPD**") define dato de carácter personal como *"toda información sobre una persona física identificada o identificable (…)"*[1].

De este modo:

[1] Vid. Art. 4.1 del RGPD.

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 Signyourdocs.

- **eIDAS:** Son las siglas inglesas del Reglamento (UE) núm. 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior 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 generación de firma 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 personales son tratados por el Responsable del Tratamiento, y en su caso, por los encargados y subencargados que en cada momento se determine, 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.

- **Ley 6/2020**: Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios de confianza.

- **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.

- **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 generación de firma electrónica.

- **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:*

  - *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*
  - *la creación, verificación y validación de certificados para la autenticación de sitios web, o*
  - *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):** En este tipo de servicios el usuario encuentra en la nube las herramientas finales con las que puede implementar directamente los procesos de su organización: una aplicación de contabilidad, de correo electrónico, un *workflow*, un programa para la gestión documental de su empresa, etc.

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. **Platform as a Service (PaaS):** 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.

- **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.

-

- **Signyourdocs:** 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.

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 Signyourdocs, 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

a. OBJETO DE LA DPC

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 y la web específica de Signyourdocs, 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: envío de documentación y generación de firmas electrónicas.
- Derechos y obligaciones asumidos por ORIGINPATH, los usuarios del servicio y el resto de los intervinientes.
- Requisitos técnicos exigidos.
- Régimen de responsabilidad asumido y límites.
- Medidas de seguridad técnicas y organizativas aplicadas por ORIGINPATH.
- Política de privacidad.
- 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.

La DPC se emite sobre la base de las disposiciones del Reglamento eIDAS y de la Ley 6/2020.

b. 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.

c. 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. 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.

d. 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: administracion@originpath.com

4. SERVICIO OBJETO DE LA DPC Y SUS CARACTERÍSTICAS

a. INTRODUCCIÓN

El servicio Signyourdocs se ofrece como una solución destinada a proporcionar a sus usuarios un sistema de envío de documentación que permite a cada destinatario firmarla electrónicamente, con el cual también se permite 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 cuenta con funcionalidades accesorias que permiten registrar el momento en que el destinatario accedió al contenido de la comunicación.

Conforme a las distintas fases que se detallan en el apartado 4.3 de la DPC, Signyourdocs permite recabar una serie de información relativa al proceso de firma de la documentación para identificar posteriormente a cada uno de los firmantes.

b. 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, lo cual incluye la generación de las evidencias y generación del documento de auditoría del proceso de firma. Por su parte, un Proveedor de Servicios de Confianza cualificado provee la firma PKI del documento objeto de firma y del documento de auditoría generado por ORIGINPATH.

- **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. Signyourdocs 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 el certificado de finalización.

c. DESCRIPCIÓN FUNCIONAL DEL PROCESO DE FIRMA A TRAVÉS DE SIGNYOURDOCS

○ 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, en caso de que la firma conlleve un proceso de firma OTP (*one-time password*), también el 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 Signyourdocs, para poder acceder a su contenido.

Dado que Signyourdocs 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.

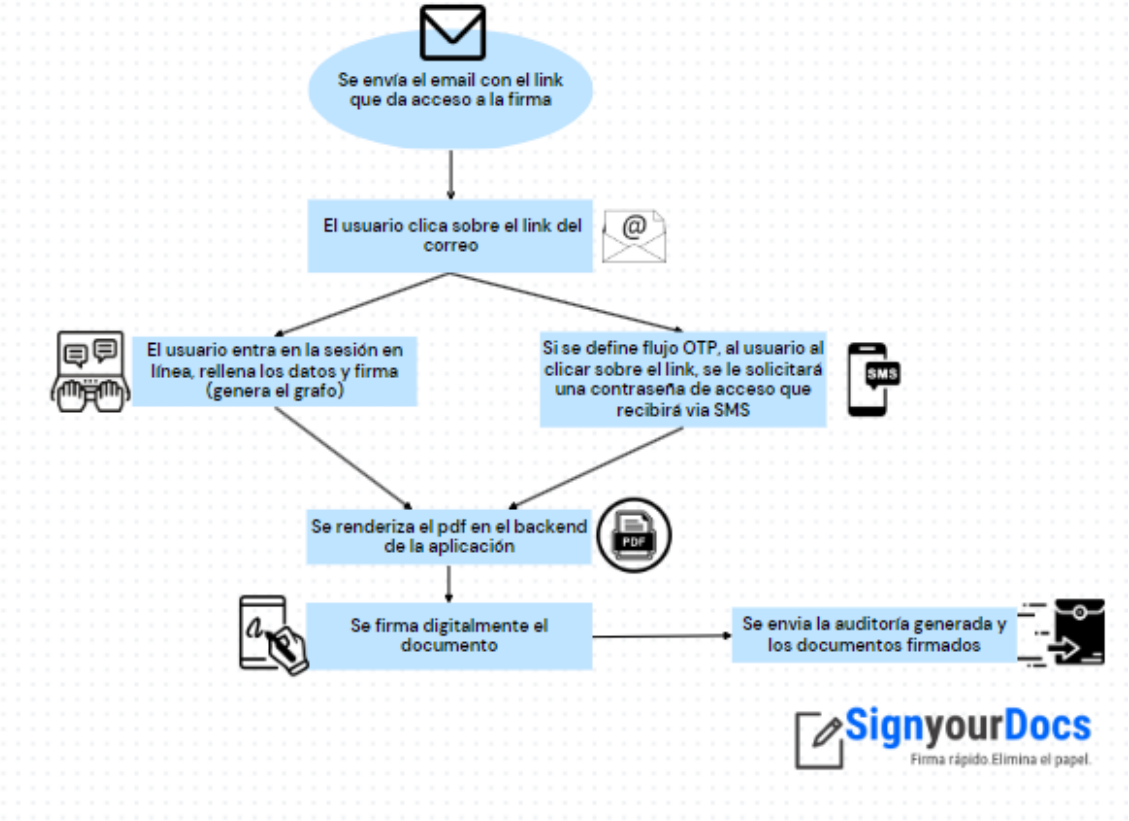

Figura 1 Flujo funcional de Signyourdocs

Con independencia del modo de acceso, el destinatario accede a un interfaz en la que cumplimentará los datos necesarios para la firma del documento, la cual puede realizarse **(i)** incluyendo la traza de la firma (grafo) o, en caso de haberse configurado durante el proceso de generación y envío del documento, **(ii)** mediante la introducción del código OTP enviado vía SMS.

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

- **FASE 4: 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 hora 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.

Adicionalmente, ORIGINPATH incluye en la auditoría del documento un sellado de tiempo (o *timestamp*) en el que refleja la fecha y hora de generación de dicho contenido.

- **FASE 5: 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

a. POR PARTE DE ORIGINPATH

i.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 Signyourdocs.
- 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:**

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 de protección de datos para aquellos tratamientos que puedan suponer un riesgo para los derechos de los usuarios.
- ORIGINPATH implementará 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 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, a la autoridad competente, ante la detección 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 según lo dispuesto en la normativa que en cada caso aplique.
- 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.

ii.RESPONSABILIDAD DE ORIGINPATH

De conformidad con el régimen de responsabilidad contemplado por la Ley 6/2020, 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, conforme a lo dispuesto en el art. 24 eIDAS, solo deberán suscribir una póliza de seguro los prestadores de servicios de confianza cualificados, 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.

b. POR PARTE DE LOS USUARIOS

i.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, archivan o firman 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.

ii.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.

c. 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 PRIVACIDAD

ORIGINPATH S.L. en cumplimiento de la normativa de protección de datos personales, informa al usuario de la plataforma de Signyourdocs, (en adelante "**la plataforma**") de las siguientes condiciones, que regirán el tratamiento de sus datos personales en el marco de su empleo e interacción con la misma.

6.1. Responsable del tratamiento de datos personales

El responsable del tratamiento es ORIGINPATH, S. L. (en adelante, "ORIGINPATH"), con domicilio social en domicilio social en C/ los Nardos 12, 3ºA, Alcorcón, 28925, Madrid (España), y con Número de Identificación Fiscal (NIF) B-87624888.

Puedes contactar con el Delegado de Protección de Datos de ORIGINPATH (DPO) en la dirección de correo electrónico rgpd@originpath.com

6.2. Finalidad del tratamiento de los datos y base de legitimación

Los datos personales facilitados con el registro e interacción en la plataforma, así como durante el proceso de prestación de los servicios, serán tratados por ORIGINPATH con las siguientes finalidades y sobre las siguientes bases de legitimación:

Finalidad 1: prestación del servicio electrónico de confianza

- **Datos tratados con esta finalidad:** datos identificativos y de contacto facilitados (nombre, apellidos, dirección de correo electrónico y/o número de teléfono de los usuarios del servicio), firma (grafo) del interesado, datos de navegación e información asociada a la auditoría del documento, conforme a lo detallado en la Declaración de Prácticas de Certificación del servicio (por ejemplo, información relativa a los hitos de envío y entrega de los correos electrónicos a través de la información generada en el proceso de firma, fecha y hora de los envíos, resultado de la comunicación, datos relativos al navegador empleado y/o dirección IP asociada a la navegación de cada usuario).

  Durante el proceso de generación de firma y prestación del servicio también podrán tratarse datos relativos a la geolocalización del firmante cuando, durante dicho proceso, se configure y habilite el parámetro de activación de

geolocalización, lo cual dependerá de que el usuario haya activado la funcionalidad de geolocalización en su dispositivo.

- **Descripción de la finalidad:** gestión y prestación del servicio electrónico de confianza.

- **Base de legitimación:** establecimiento de medidas precontractuales y ejecución de la relación suscrita al solicitar y ser usuario del servicio prestado, con base en las condiciones expuestas en la Declaración de Prácticas de Certificación.

Finalidad 2: resolución de consultas y atención de solicitudes

- **Datos tratados con esta finalidad:** datos identificativos y de contacto facilitados (nombre, apellidos, dirección de correo electrónico y/o número de teléfono de los usuarios del servicio),

- **Descripción de la finalidad:** atención de aquellas consultas y solicitudes de información que se dirijan a ORIGINPATH, en cualquier momento, a través de los canales de contacto habilitados.

- **Base de legitimación:** establecimiento de medidas precontractuales, en el contexto de consultas previas a la obtención de condición de usuario del servicio, y/o ejecución de la relación suscrita al solicitar y ser ya usuario efectivo del servicio prestado, con base en las condiciones expuestas en la Declaración de Prácticas de Certificación.

Finalidad 3: creación de cuentas de usuario registrado

- **Datos tratados con esta finalidad:** datos identificativos y de contacto facilitados (nombre, apellidos, dirección de correo electrónico y/o número de teléfono de los usuarios del servicio) al momento de solicitar, en su caso, el registro de una cuenta de usuario en la página web y/o plataforma del servicio, lo cual comprende también la solicitud de generación y tratamiento de una password.

- **Descripción de la finalidad:** habilitación, gestión y mantenimiento e la cuenta de usuario registrado.

- **Base de legitimación:** establecimiento de medidas precontractuales y ejecución de la relación derivada de la creación de cuenta de usuario registrado, conforme a las condiciones descritas en cada momento en los documentos de aviso legal

y/o condiciones particulares de uso que se identifiquen en la página web o plataforma del servicio.

Finalidad 4: elaboración de perfiles con fuentes internas

- **Datos tratados con esta finalidad**: datos identificativos y de contacto facilitados (nombre, apellidos, dirección de correo electrónico y/o número de teléfono de los usuarios del servicio), datos de navegación de interacción con la plataforma y el servicio (histórico de procesos ejecutados e intervenciones realizadas, por ejemplo).

- **Descripción de la finalidad**: elaborar perfiles entre los usuarios de la plataforma y del servicio mediante estudios de mercadotecnia, obtención e inferencia de conclusiones y aplicación de técnicas de segmentación que permitan, ulteriormente, modificar e introducir mejoras en la oferta de productos y servicios realizada, adaptándolas a las preferencias de cada perfil, así como introducir mejoras y actualizaciones en el diseño y conjunto de funcionalidades de la plataforma en sí misma.

  La elaboración de perfiles puede implicar tareas de extracción, agregación, almacenamiento y/o análisis de información, con base en la cual realizar la citada segmentación y clasificar a los interesados en función de determinados patrones, como serían por ejemplo los patrones de consumo o las reacciones a las distintas acciones, promociones y/o novedades que introduzca en sus procesos de negocio el ORIGINPATH.

- **Base de legitimación**: interés legítimo de ORIGINPATH en optimizar su oferta comercial, dirigiendo a aquellos clientes respecto de quienes se cuente con legitimación para el envío de comunicaciones comerciales, comunicaciones relativas a productos y servicios personalizados a sus preferencias, aumentando de esta forma la eficacia de las campañas de mercadotecnia realizadas.

  La finalidad descrita para el perfilado es independiente de la finalidad de envío de comunicaciones comerciales. Si desea obtener más información en relación con el interés legítimo invocado por ORIGINPATH, u oponerse al tratamiento descrito, puede contactar con nosotros en la siguiente dirección rgpd@originpath.com.

Finalidad 5: atención de incidencias y prevención del fraude

- **Datos tratados con esta finalidad**: datos identificativos, de contacto y relativos a transacciones efectuadas por el usuario.

- **Descripción de la finalidad**: solucionar todas aquellas incidencias que pudiesen sucederse en relación con el uso de la plataforma y desarrollo del servicio. Se podrá contactar con el usuario en caso de detectar o existir sospechas fundadas de potenciales fraudes o suplantaciones de identidad.

- **Base de legitimación**: interés legítimo de ORIGINPATH en garantizar un correcto desarrollo de la actividad organizada, evitando la ocasión de prácticas ilícitas y/o incorrectas.

Si desea obtener más información en relación con el interés legítimo invocado por ORIGINPATH, u oponerse al tratamiento efectuado, puede contactar con nosotros en la dirección rgpd@originpath.com

- **Finalidad 6: envío de comunicaciones comerciales propias**

  - **Datos tratados con esta finalidad**: datos identificativos y de contacto, tales como nombre, apellido, número de teléfono y dirección de correo electrónico.

  - **Descripción de la finalidad:** remitir comunicaciones comerciales relativas a productos y servicios propios de ORIGINPATH.

  - **Base de legitimación**: consentimiento del usuario.

- **Finalidad 7: cumplimiento de obligaciones legales**

  - **Datos tratados con esta finalidad**: cualesquiera categorías de datos de entre las tratadas en el contexto de las anteriores finalidades.

  - **Descripción de la finalidad:** cumplimiento con las obligaciones legales que resulten aplicables en cada momento, a ORIGINPATH.

  - **Base de legitimación**: cumplimiento de la obligación legal aplicable.

1. **Plazos de conservación de los datos personales**

Los datos personales objeto de tratamiento serán conservados durante el tiempo preciso

para cumplir la finalidad declarada en cada caso. A modo de referencia, pueden observarse los siguientes plazos de conservación:

(i) Habilitación de cuentas de usuario registrado → hasta el momento en que se solicite la supresión de la cuenta de usuario.

(ii) Resolución de consultas o atención de incidencias → los datos serán conservados durante el tiempo preciso para solventar aquella duda o cuestión planteada a ORIGINPATH, así como durante el tiempo preciso para gestionar las incidencias que se produzcan.

(iii) Gestión de campañas de mercadotecnia → los datos serán conservados durante el tiempo que se mantenga la circunstancia habilitadora del tratamiento, esto es: el consentimiento del usuario o su condición de cliente previo a los efectos de remitir comunicaciones comerciales propias sobre productos y servicios similares a los ya adquiridos.

El usuario puede contactar con el DPO de ORIGINPATH en caso de desear obtener mayor información sobre los plazos de conservación aplicables al empleo de la plataforma, dirigiéndose por escrito a rgpd@originpath.com.

Finalizado el plazo de conservación previsto (en función de la finalidad), los datos personales podrán ser conservados, debidamente bloqueados, durante los plazos de prescripción de las acciones y responsabilidades legales que se pudiesen derivar, en cada caso, de la concreta actividad de tratamiento realizada, tras lo cual se procederá con su completa eliminación.

Respecto de los datos tratados con fines de mercadotecnia, en caso de que usuario hubiese ejercitado su derecho de oposición a la recepción de comunicaciones comerciales, podrán conservarse sus datos identificativos a los efectos de evitar que en el futuro se dirijan más comunicaciones a sus direcciones electrónicas de contacto.

2. **Cesiones y destinatarios de los datos personales**

Los datos personales, en línea con las finalidades anteriormente indicadas, podrán ser comunicados a:

a) Proveedores de ORIGINPATH contratados en el marco de gestión y mantenimiento de la plataforma, que desarrollarán sus funciones en condición

de encargados del tratamiento, bajo las instrucciones y supervisión de ORIGINPATH.

b) Jueces, Tribunales o Administraciones Públicas a quienes ORIGINPATH se viera obligada a comunicar datos personales de algún usuario.

No se prevé la transferencia internacional de los datos personales de los usuarios. No obstante, en caso de efectuarse alguna transferencia internacional, se llevará a cabo atendiendo a los criterios y requisitos exigidos por la normativa vigente, por medio de la adopción de garantías jurídicas adecuadas, las cuales podrán consistir en la formalización con el destinatario de los datos de (i) Cláusulas Contractuales Tipo aprobadas por la Comisión Europea para legitimar la transferencia internacional de datos a terceros países o (ii) en otro instrumento jurídico válido que permita garantizar un nivel adecuado de protección equivalente al del Espacio Económico Europeo. (Revisar, AWS con CPD en Francia)

Si lo desea, puede obtener información adicional sobre las transferencias internacionales contactando con nuestro DPO en la dirección de correo electrónico rgpd@originpath.com

3. Derechos de los usuarios

El usuario de la plataforma e interesado cuyos datos son tratados podrá ejercitar ante ORIGINPATH , en caso de que resulten de aplicación, los derechos de acceso, rectificación o supresión, limitación de su tratamiento, oposición (especialmente, respecto de los tratamientos basados en interés legítimo), portabilidad y a oponerse a decisiones individuales automatizadas en el correo electrónico rgpd@originpath.com o en el domicilio social anteriormente indicado.

Asimismo, se informa que ORIGINPATH ha designado un Delegado de Protección de Datos (DPO) ante quien podrán plantearse cuestiones, relativas al tratamiento de datos personales, dirigiéndose por escrito al domicilio social de la compañía y/o al correo electrónico antes referido.

Adicionalmente, se informa al usuario del derecho que le asiste a interponer una reclamación ante la Agencia Española de Protección de Datos.

2. ENCARGO DEL TRATAMIENTO

Los servicios prestados por ORIGINPATH, que se desarrollan por petición expresa de una de las partes intervinientes, incluyen acciones y procesos de tratamiento de datos personales que, con independencia de los procesos de tratamiento propios de ORIGINPATH como responsable del tratamiento – conforme a la sección 6 de la DPC - tienen encaje en el desarrollo de una relación de encargo del tratamiento.

Ello obedece a la circunstancia de que la participación de ORIGINPATH implique que su intervención como Prestador de Servicios de Confianza quede supeditada a la ejecución de una tarea cuyos fines y medios son determinados por el cliente de ORIGINPATH, que ostenta la consideración de responsable del tratamiento. Debido a lo anterior, el tratamiento de dichos datos personales se regirá por las condiciones descritas a continuación.

El interviniente que inicia la acción y desarrollo de los servicios prestados por ORIGINPATH declara que cuenta con la habilitación y capacidad suficiente para vincular al responsable del tratamiento, al cual representa (en adelante, el "**RESPONSABL**E"), a dichas condiciones de tratamiento.

CONTRATO DE ENCARGO DE TRATAMIENTO

1. **Objeto.**

Definir las condiciones conforme a las cuales **ORIGINPATH** llevará a cabo el tratamiento de datos personales que resulten necesarios para la prestación del servicio electrónico de confianza.

En consecuencia, se autoriza, por parte del RESPONSABLE la realización de las siguientes operaciones de tratamiento: captación, almacenamiento, estructuración, conservación, modificación y/o supresión de los datos personales captados en el contexto de prestación del servicio (puesta en contacto, remisión y almacenamiento de documentación).

El tratamiento realizado por el ENCARGADO se llevará a cabo hasta alcanzar el servicio

contratado y solicitado en cada momento, el cual se encuentre sujeto a las presentes condiciones.

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.

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. Estas medidas se encuentran desarrolladas en la sección 8 de la DPC.

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 a los interesados en el momento de la recogida de los datos y garantizar la licitud del tratamiento.

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.
- **SENDINBLUE, Sociedad por Acciones Simplificada** inscrita en el Registro Mercantil de París con el número 498 019 298 y con domicilio social en 7 rue de Madrid, 75008 Paris, France

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. _____	D/Dña. _____
El RESPONSABLE	El ENCARGADO

12. 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) realizada.

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. Concretamente, se aplicarán al repositorio de passwords generadas por los usuarios registrados.
- 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.

13. 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.

15. 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 la normativa vigente en la materia.

16. 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.