Acuerdo de encargo de tratamiento de datos personales de acuerdo con el RGPD y las cláusulas contractuales tipo

El presente Acuerdo de encargo de tratamiento de datos personales de acuerdo con el RGPD (en adelante, "**ATD**") se celebra entre la entidad identificada como responsable (en adelante, el "**Responsable**") y Proofpoint, Inc., con domicilio en 925 W. Maude Avenue, Sunnyvale, CA 94085 (en adelante, el "**Encargado**" o "**Proofpoint**") y se adjunta: 1) bien al Contrato Marco de Suscripción de Proofpoint o a las Condiciones generales y los correspondientes anexos específicos para cada producto, 2) a un contrato de licencia de usuario final (el Contrato de Cliente *online*, un EULA, un Contrato *click-wrap*, en su caso, o un Contrato *click-through*) aceptado por el Responsable en el momento de su registro y acceso inicial al producto o servicio de Proofpoint, o bien 3) a cualquier otro acuerdo de licencia escrito y firmado por las partes en virtud del cual el Encargado suministre productos o servicios al Responsable (en adelante, el "**Acuerdo de Servicios**"). El presente ATD entrará en vigor a la fecha de su firma por parte del Responsable, pero únicamente en caso de que Proofpoint reciba la copia firmada del ATD de conformidad con las instrucciones indicadas más adelante.

El presente ATD establece las condiciones en las que el Encargado podrá recibir y tratar Datos Personales del Responsable. El presente ATD tiene en cuenta la naturaleza del Tratamiento según lo dispuesto en el Acuerdo de Servicios y describe las medidas técnicas y organizativas adecuadas adoptadas por el Encargado en el Tratamiento de Datos Personales.

Además, el presente ATD incorpora las cláusulas contractuales tipo anexas a la Decisión de la Comisión Europea (EU) 2021/914 (en adelante, las "**CCT**"). Además de las obligaciones de Proofpoint establecidas en el presente ATD, Proofpoint respetará las obligaciones correspondientes a un importador de datos, tal y como aparecen estipuladas en las CCT. Cualquier referencia al **Importador de Datos** deberá interpretarse como referencia a **Proofpoint, Inc. o al Encargado**; del mismo modo, cualquier referencia al **Exportador de Datos** o Responsable del Tratamiento se interpretará como una referencia al **Responsable** y a sus sociedades afiliadas en la Unión Europea. En virtud del presente documento, el Responsable acuerda y garantiza que tiene derecho y autoridad para concluir el presente ATD en su propio nombre y el de sus sociedades afiliadas.

Las partes del presente acuerdo aceptan en virtud del mismo las condiciones establecidas en el Anexo 1 (Condiciones de Tratamiento de datos) y sus apéndices, y en el Anexo 2 (Cláusulas contractuales tipo). El presente ATD ha sido previamente firmado por el Encargado, Proofpoint, Inc. Para que entre en vigor, el Responsable debe primero:

1. Cumplimentar y firmar el cuadro para la firma que figura a continuación con la razón social completa del Responsable, su domicilio y la información del apoderado firmante; y
2. Remitir el ATD debidamente cumplimentado y firmado a Proofpoint a través de correo electrónico a la dirección privacy@proofpoint.com.

En caso de que el Responsable elimine cualquier elemento o modifique de otro modo el presente ATD, dichas eliminaciones o modificaciones serán rechazadas y quedarán sin validez en virtud de esta disposición, a menos que hayan sido aprobadas por Proofpoint. La abajo firmante en representación del Responsable declara y garantiza que está capacitado para vincular al Responsable en virtud del presente ATD. El presente ATD quedará automáticamente resuelto cuando se rescinda o resuelva el Acuerdo de Servicios o antes si se rescinde o resuelve el presente de acuerdo con las disposiciones de este ATD.

Aceptado y aprobado por el Responsable:		Aceptado y aprobado por **Proofpoint, Inc.**: (**Encargado**)	
Firma:	_____	Firma:	DocuSigned by: Paul Auvil 2955B8CEBD2B45C...
Nombre:	_____	Nombre:	Paul Auvil, Director Financiero
Fecha:	_____		
Sociedad:	_____		
Domicilio:	_____		
	_____		

ANEXO 1

CONDICIONES DEL TRATAMIENTO DE DATOS

1. Definiciones.

a. Todos los términos que se emplean sin definición en el presente ATD tienen los significados que se les atribuyen: primero, en el Reglamento general de protección de datos (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 (en adelante, **RGPD**) y, segundo, en el Acuerdo de Servicios.

b. Por **Datos del Responsable** se entenderán los Datos Personales del Responsable, con el término «datos personales» conforme a la definición recogida en el RGPD.

c. Por **Legislación de protección de datos** se entenderán todas las leyes y reglamentos aplicables en materia de tratamiento de datos personales en la medida en que guarden relación con la prestación de servicios y productos de Proofpoint en el marco del Acuerdo de Servicios.

d. Por **Interesado** se entenderá la persona identificada o identificable a la cual hacen referencia los datos personales.

e. Por **Tratamiento** (y sus cognados) se entenderá lo dispuesto en el artículo 4.2 del RGPD.

f. Por **Subencargado** se entenderá cualquier encargado contratado por el Encargado para tratar datos personales.

g. Por **Autoridad de control** se entenderá una autoridad pública establecida por un Estado miembro de la UE con arreglo a lo dispuesto en el RGPD.

2. Tratamiento de datos personales.

a. Con respecto a las actividades descritas en el Apéndice 1, las partes convienen que el Responsable y sus sociedades afiliadas en la Unión Europea (o sus afiliadas o clientes) serán el Responsable de datos / exportador de datos y el Encargado será el encargado de datos / importador de datos en tanto y en cuanto trate Datos Personales. El Responsable acepta y garantiza que sus instrucciones al Encargado en relación con el Tratamiento de Datos Personales son y serán conformes a las disposiciones pertinentes de las normas aplicables en materia de protección de datos.

b. El objeto y la duración del Tratamiento de Datos Personales viene determinado en el Acuerdo de Servicios, en el cual se describe la prestación del servicio al Responsable. La naturaleza y la finalidad de este Tratamiento, los tipos de Datos Personales y las categorías de Interesados se definen en el Apéndice 1 al presente ATD.

c. El Responsable estará a cargo de la exactitud, la calidad y la legalidad de los Datos Personales, así como de la de los medios a través de los cuales los adquirió.

d. En virtud de la presente disposición, el Acuerdo de Servicios y el presente ATD constituyen las instrucciones del Responsable para el Encargado en relación con: 1) el Tratamiento de Datos Personales, y 2) la transferencia de dichos Datos Personales a cualquier país o territorio cuando resulte razonablemente necesario para la prestación del servicio.

3. Evaluación de impacto relativa a la protección de datos ("EIPD")

Teniendo en cuenta la naturaleza del Tratamiento, el Encargado podrá prestar al Responsable cooperación y asistencia razonables que resulten necesarias para que este cumpla con sus obligaciones derivadas del RGPD a fines de llevar a cabo una evaluación de impacto sobre la protección de datos relativos al uso que el Responsable hace del Servicio, en la medida en que el Responsable no tenga de otro modo acceso a la información pertinente, y en la medida en que dicha información esté disponible para el Encargado. El Encargado prestará al Responsable asistencia razonable en la cooperación o consulta previa con la autoridad de control en la ejecución de las actividades derivadas de la obligación de EIPD del Responsable, en la medida en que así lo exija el RGPD.

4. **Derechos de los interesados.** En la medida en que la ley lo permita, el Encargado notificará con prontitud al Responsable en caso de recibir una solicitud de un Interesados para ejercitar sus derechos de acceso, rectificación, limitación del Tratamiento, derecho al olvido, a la portabilidad de datos, de oposición y/o de no ser objeto de decisiones individuales automatizadas. Teniendo cuenta la naturaleza del Tratamiento, el Encargado asistirá al Responsable a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a la solicitud del Interesado.

5. **Uso limitado de Datos Personales y Personal.** Excepto donde el Acuerdo de Servicios establezca lo contrario, i) el Encargado no adquirirá derecho alguno sobre los Datos Personales; y ii) el Encargado y sus sociedades afiliadas tomarán los pasos razonables para garantizar la fiabilidad de cualquier empleado, agente o contratante de cualquier subencargado contratado que pueda tener acceso a los Datos Personales, asegurando en todos los casos que el acceso se limite estrictamente a las personas que precisan conocer / tener acceso a los Datos Personales en cuestión, por resultar estrictamente necesario para los propósitos del Acuerdo de Servicios, así como para respetar las leyes aplicables en materia de protección de datos y derecho a la intimidad, asegurándose de que todas estas personas hayan contraído compromisos de confidencialidad o tengan obligaciones profesionales o legales de confidencialidad.

6. **Subencargados**.

a. **Designación de Subencargados**. El Responsable da su consentimiento general al Encargado para que recurra a Subencargados. El Responsable reconoce y acepta a) que las sociedades afiliadas del Encargado pueden designarse como Subencargados; y b) que el Encargado y sus sociedades afiliadas pueden contratar respectivamente a terceros Subencargados en relación con la prestación del Servicio. El Encargado o su(s) sociedad(es) afiliada(s) han celebrado un acuerdo escrito con cada Subencargado en el que se incluyen obligaciones en materia de protección de datos de tal modo que la protección que brindan no sea menos protectora que las obligaciones descritas en el presente ATD en lo que respecta a la protección de los datos del Responsable en la medida en que resulte aplicable a la naturaleza del servicio prestado por dicho Subencargado. El Encargado tendrá plena responsabilidad ante el Responsable por el cumplimiento de las obligaciones de los Subencargados, de acuerdo con el contrato celebrado entre el Subencargado y el Encargado.

b. **Lista**. La lista actualizada de Subencargados para el Servicio está disponible en la página web Trust Site de Proofpoint, en la dirección: https://www.proofpoint.com/us/legal/trust. En caso de que el Encargado efectúe cambios o adiciones a dicha lista, deberá informar al Responsable por correo electrónico de dichos cambios en la medida en que el Responsable se haya suscrito para recibir notificaciones de dicha página web. Las partes acuerdan que esta notificación satisface los requisitos de notificación dispuestos en el artículo 28.2 del RGPD y en la cláusula contractual tipo número 9.

c. **Oposición**. El Responsable podrá oponerse al recurso a un nuevo Subencargado por parte del Encargado mediante notificación a este por escrito y con prontitud a la dirección privacy@proofpoint.com. En caso de que el Responsable se oponga a un nuevo Subencargado, el Encargado, previa recepción de la oposición por escrito tal y como se establece en la frase anterior, determinará de manera razonable si es posible poner a disposición del Responsable adaptaciones para evitar el Tratamiento de Datos Personales por parte del nuevo Subencargado al que se opone el Responsable, sin que ello suponga una carga indebida para el Responsable. En caso de que el Encargado no sea capaz de poner en práctica dichos cambios en un período razonable de tiempo, que no excederá los treinta (30) días, el Responsable podrá rescindir la orden de compra en cuestión, para lo cual dará aviso por escrito al Encargado en el plazo de treinta (30) días a partir de la decisión del Encargado. Dicha rescisión se aplicará únicamente al Servicio que no puede prestar el Encargado sin recurrir al Subencargado objetado.

7. **Categorías especiales de datos personales**. El Responsable (y sus sociedades afiliadas en la Unión Europea) tendrá toda la responsabilidad del cumplimiento de la normativa en materia de privacidad y protección de datos, en la medida en que sea aplicable al Responsable (y sus sociedades afiliadas en la Unión Europea), incluidos cualesquiera Datos Personales que requieran un tratamiento especial o categorías especiales de Datos Personales como, a título meramente enunciativo, las relativas a la raza o etnicidad de la persona, sus opiniones políticas, creencias religiosas o filosóficas, pertenencia a sindicatos, salud, vida sexual o finanzas personales.

8. Seguridad de los datos personales.

a. El Encargado deberá como mínimo implementar las medidas técnicas y organizativas especificadas en el Apéndice 2 para garantizar la seguridad de los Datos Personales. Esto incluye la protección de los Datos Personales contra cualquier violación de la seguridad que conlleve una destrucción, pérdida, alteración, divulgación o acceso no autorizados a los Datos Personales, ya sea de manera accidental o ilícita. A la hora de determinar el nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del Tratamiento, y los riesgos que entraña para los Interesados.

b. El Encargado permitirá el acceso a los Datos Personales que estén siendo objeto de Tratamiento a los miembros de su personal, solo en tanto y en cuanto resulte necesario para la implantación, gestión y supervisión del Acuerdo de Servicios. El Encargado garantizará que las personas autorizadas para tratar los Datos Personales recibidos se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación legal adecuada de confidencialidad.

9. Cooperación con las autoridades de control. El Encargado prestará asistencia razonable al Responsable en la cooperación o consulta previa con la autoridad de control en el rendimiento de sus tareas derivadas del artículo 8 del presente ATD, en la medida en que así lo exija el tenor del RGPD. Además, en relación con la solicitud de la Autoridad de Control, y a expensas del Responsable, el Encargado empeñará medios razonables para lograr la cooperación y asistencia razonables de los Subencargados a fines de proporcionar acceso a la información relevante necesaria para cumplir las obligaciones del Responsable derivadas del RGPD.

10. Violación de datos personales.

a. Si el Encargado tuviera conocimiento de un uso, divulgación o adquisición no autorizados por parte de un tercero de Datos Personales que comprometa la seguridad, la confidencialidad o la integridad de los Datos Personales en posesión del Encargado (en adelante, una "Violación de seguridad"), el Encargado notificará al Responsable por escrito de dicha violación en el plazo de 48 horas y seguidamente proporcionará actualizaciones periódicas.

b. Dicha notificación incluirá al menos
   (i) una descripción de la naturaleza de la Violación de seguridad (en la que figuren, cuando sea posible, las categorías y el número aproximado de Interesados y registros de datos afectados);
   (ii) los datos de contacto donde se puedan obtener información adicional relativa a la violación de Datos Personales; y
   (iii) las consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la Violación de Seguridad, especialmente, en su caso, medidas para mitigar sus posibles efectos adversos.

c. Cuando y en la medida en que no se pueda proporcionar toda esta información al mismo tiempo, en la notificación inicial se proporcionará la información de la que se disponga en ese momento y, a medida que se vaya recabando, se irá proporcionando sin dilación indebida la información adicional.

11. Transferencia internacional de datos

a. **General**. El Encargado respetará los requisitos de las leyes de Protección de Datos aplicables en materia de transferencia internacional de Datos Personales desde el Espacio Económico Europeo. A los únicos efectos de prestar los Servicios al Responsable en el marco del Acuerdo de Servicios, será posible transferir y almacenar Datos Personales a cualquier otro país en el que opere el Encargado o sus Subencargados, lo cual puede incluir terceros países. Todas las transferencias de Datos Personales fuera del Espacio Económico Europeo se regirán por las Cláusulas Contractuales Tipo que las partes adoptan en virtud del presente ATD, al cual se incorporan como Anexo 2.

b. **Evaluación de transferencia de datos.** Varios de los servicios de seguridad prestados por el Encargado requieren la transferencia de un cierto volumen de Datos Personales a los Estados Unidos; así pues, en cumplimiento del apartado b) de la Cláusula Contractual Tipo 14, el Encargado ha realizado una valuación de transferencia de datos (también conocida como Evaluación de Impacto de Transferencia) accesible en https://www.proofpoint.com/sites/default/files/misc/pfpt-us-data-transfer-assessment-20201028.pdf.

12. Solicitudes gubernamentales.

a. En aplicación de la Cláusula Contractual Tipo número 15, el Encargado no divulgará a ningún organismo gubernamental o autoridad pública externos ningún Dato del Responsable, excepto en aquellos casos en que sea necesario para el cumplimiento de la ley o de una orden válida y vinculante de un órgano gubernamental (tal como un requerimiento o una orden judicial). En caso de que un órgano gubernamental envíe al Encargado una solicitud de Datos del Responsable, el Encargado intentará que el órgano gubernamental solicite estos datos al Responsable directamente. En tal sentido, el Encargado podrá proporcionar al órgano gubernamental la información básica de contacto del Responsable. En caso de que se vea compelido a divulgar Datos del Responsable a un órgano gubernamental, salvo que tenga la prohibición legal de hacerlo, el Encargado comunicará al Responsable en un plazo razonable dicha solicitud para permitirle solicitar medidas cautelares u otras medidas adecuadas. De acuerdo con lo dispuesto en la Ley de Vigilancia de la Inteligencia Extranjera de los Estados Unidos (FISA, *Foreign Intelligence Surveillance Act*), el Encargado es un "servicio informático remoto" y no un prestador de servicios de telecomunicaciones, por lo cual no es probable (en opinión del Encargado) que este sea objeto de un requerimiento gubernamental en aplicación de dichas leyes.

b. Con el fin de garantizar que el Responsable sea y permanezca consciente de los riesgos que conlleva la transferencia de datos a un tercer país, el Encargado del tratamiento podrá, puntualmente, previa solicitud razonable por parte del Responsable, que no podrá exceder de una vez por año natural, dar respuesta a un cuestionario estructurado del Responsable sobre las leyes y reglamentos del país de destino aplicables al Encargado o a sus Subencargados que permitirían el acceso de las autoridades públicas a los Datos del Responsable que sean objeto de la transferencia, en particular, en los ámbitos de la información, la aplicación de la ley y la supervisión administrativa y normativa aplicables a los datos transferidos. El Encargado debe estar en condiciones de proporcionar al Responsable este tipo de información a su leal saber y entender y tras haber hecho todo lo posible por obtenerla.

13. Verificación y auditoría

a) De acuerdo con lo dispuesto en la letra h) del apartado 3 del artículo 28 del RGPD, el Encargado pondrá a disposición del Responsable –previo aviso razonable por escrito y con sujeción a la celebración de un acuerdo de confidencialidad específico– información referente al Tratamiento de Datos Personales del Responsable que resulte necesaria para demostrar que el Encargado cumple con sus obligaciones derivadas del presente ATD. El Encargado permitirá las solicitudes de inspección in situ por parte del Responsable o de un auditor independiente en relación con el Tratamiento de Datos Personales, con objeto de verificar que el Encargado esté cumpliendo con lo dispuesto en el presente ATD, siempre y cuando: a) el Encargado no haya aportado evidencia escrita suficiente de su cumplimiento de las medidas técnicas y organizativas; b) se haya producido una Violación de Seguridad; c) la Autoridad de Control del Responsable haya solicitado oficialmente una inspección; o d) la Ley de Protección de Datos proporciona al Responsable un derecho imperativo de inspección in situ; y siempre que el Responsable no ejerza este derecho más de una vez al año, salvo que la Ley de Protección de Datos exija inspecciones más frecuentes. Cualquier información proporcionada por el Encargado y/o por las auditorías llevadas a cabo en virtud de este artículo estará sujeta a la celebración de un acuerdo de confidencialidad específico. Dichas inspecciones de las instalaciones se llevarán a cabo de tal manera que no afecten la seguridad, confidencialidad, integridad, disponibilidad, continuidad y resiliencia ininterrumpida de las instalaciones inspeccionadas, ni expongan o comprometan de ningún otro modo cualesquiera datos confidenciales que en ellas se traten.

b) Cada una de las partes asumirá sus propios costes asociados a toda auditoría o inspección. Esto también será aplicable a cualquier suministro de información o auditoría derivada de lo dispuesto en las letras c) a e) del apartado 9 de la Cláusula Contractual Tipo 8.

14. Rescisión

El Responsable acepta y reconoce que, en caso de suspensión o rescisión de cualquier Tratamiento de datos en el marco del presente ATD o de la Cláusula Contractual Tipo número 18, el plazo de tiempo para que el Encargado cese todo Tratamiento y elimine los Datos Personales vendrá determinado en el Acuerdo de Servicios.

APÉNDICE 1 AL ATD – DETALLES DEL TRATAMIENTO

El presente Apéndice 1 incluye algunos detalles sobre el Tratamiento de los Datos Personales del Cliente tal y como establece el apartado 3 del artículo 28 del RGPD (o, en su caso, las disposiciones equivalentes de cualquier otra Ley de Protección de Datos).

Producto	Interesados	Categorías de Datos Personales tratados	Operaciones de tratamiento	Periodo de conservación
Archive	Empleados, contratistas y clientes	Cualquier Dato Personal incluido en el contenido recopilado (incluidos los correos electrónicos, los mensajes instantáneos, el contenido en redes sociales, la telemetría de los mensajes asociados y los archivos adjuntos)	• Archive es una solución de archivo en la nube diseñada con fines de detección legal, cumplimiento normativo y acceso a datos para los usuarios finales del Cliente y proporciona un repositorio central con capacidad de búsqueda que admite una amplia variedad de tipos de contenido.	Según determine el Responsable
CAD/CASB	Empleados, contratistas	Metadatos de titular de cuenta en la nube (direcciones de correo electrónico, nombres, cargos), metadatos de archivos y registros de acceso a cuentas en la nube	Cloud Account Defense ayuda al Cliente a detectar actividades sospechosas en torno a las cuentas en la nube del Cliente y a identificar las cuentas en la nube que se han visto de algún modo comprometidas. Cloud App Security Broker utiliza directivas para evitar la pérdida de los datos sensibles o confidenciales del Cliente contenidos en las cuentas en la nube del Cliente. CASB IaaS Protection ayuda al cliente a identificar sus recursos IaaS, a proteger los datos sensibles dentro del almacenamiento IaaS y a supervisar y detener los inicios de sesión no autorizados en las cuentas en la nube del Cliente	Hasta 180 días desde el final de la suscripción del Responsable como máximo
Cloudmark Active Filter, Authority, Content Categories, Insight Server y Sender Intelligence; Cloudmark Spam Reporting Service	Empleados, contratistas, clientes	Datos de telemetría asociados a mensajes de correo electrónico, SMS, MMS y RCS, incluidas direcciones de correo electrónico, direcciones IP, números de teléfono	Los productos Cloudmark aprovechan el análisis inteligente de amenazas para proporcionar seguridad en el correo electrónico y la mensajería móvil contra el spam y el malware.	30 días para los mensajes denunciados por el destinatario como potencialmente dañinos. 30 días para los mensajes notificados por el destinatario como no dañinos.

Cloudmark Safe Messaging Cloud, Cloudmark Safe Messaging Cloud Hybrid	Empleados, contratistas, clientes	Datos de telemetría asociados a mensajes de correo electrónico, SMS, MMS y RCS, incluidas direcciones de correo electrónico, direcciones IP, números de teléfono	Los productos Cloudmark aprovechan el análisis inteligente de amenazas para proporcionar seguridad en el correo electrónico y la mensajería móvil contra el spam y el malware.	30 días para los mensajes denunciados por el destinatario como potencialmente dañinos. 30 días para los mensajes notificados por el destinatario como no dañinos. Por lo demás, según lo negociado por el Responsable.
Compliance Gateway	Empleados, contratistas y clientes	Cualquier dato personal incluido en el contenido recopilado (incluidos los correos electrónicos, los mensajes instantáneos, el contenido en redes sociales, la telemetría de los mensajes asociados y los archivos adjuntos)	Compliance Gateway actúa como un eje central para filtrar y dirigir el contenido de los mensajes a los sistemas de archivo, supervisión y análisis del Cliente.	Hasta 14 días desde el final de la suscripción del Responsable como máximo
Content Capture	Empleados, contratistas y clientes	Cualquier dato personal incluido en el contenido recopilado (incluidos los correos electrónicos, los mensajes instantáneos, el contenido en redes sociales, la telemetría de los mensajes asociados y los archivos adjuntos)	Content Capture recopila el contenido de las plataformas de mensajería y de almacenamiento en la nube compatibles y ofrece servicios de cumplimiento normativo, como detección electrónica, archivado y supervisión.	Hasta 90 días desde el final de la suscripción del Responsable como máximo
Content Patrol	Empleados, contratistas y clientes	Cualquier dato personal incluido en el contenido recopilado (incluidos los correos electrónicos, los mensajes instantáneos, el contenido en redes sociales, la telemetría de los mensajes asociados y los archivos adjuntos)	Content Patrol permite a los clientes recopilar, supervisar, solucionar y generar informes de cumplimiento sobre las actividades de sus usuarios finales en las cuentas de redes sociales controladas por el Cliente.	Hasta 90 días desde el final de la suscripción del Responsable como máximo
Continuity	Empleados, contratistas y cualquier otra persona que envíe o reciba correos electrónicos a	Cualquier Dato Personal incluido en un correo electrónico	Continuity proporciona un almacenamiento temporal del correo electrónico entrante y saliente del Cliente dentro del correo electrónico web a demanda. Continuity sirve solo como opción secundaria de emergencia en caso de fallo del servicio de correo electrónico del Cliente, y no como	Los mensajes caducan a los 30 días.

	través del sistema de correo electrónico corporativo del Responsable		solución principal de archivado de correo electrónico ni como solución principal de emergencia	
Digital Discover, Digital Protection y Digital Compliance	Empleados, contratistas, clientes o cualquier otra persona que publique en las cuentas de redes sociales del Cliente	Nombres de usuario de cuentas corporativas de redes sociales, contenido en redes sociales, y opción de información biográfica si aparece reflejada en el perfil de cuenta del usuario corporativo	Escaneo de plataformas de redes sociales para encontrar cuentas afiliadas a clientes por cuentas falsas, fraudulentas y difamatorias en relación con el cliente. Análisis de contenido estático e interactivo. Conectores al servicio de archivo de redes sociales tal y como se requiera para su cumplimiento.	Hasta 90 días desde el final de la suscripción del Responsable como máximo
Email Data Loss Prevention (DLP)	Empleados, contratistas y cualquier otra persona que envíe o reciba correos electrónicos a través del sistema de correo electrónico corporativo del Cliente	Cualquier Dato Personal incluido en un correo electrónico	Email DLP utiliza directivas para evitar la pérdida de datos sensibles o confidenciales del Cliente a través del correo electrónico.	Hasta 366 días después de la recopilación, excepto en el caso de los análisis de amenazas, que se conservan hasta 18 meses después de la recopilación.
Email Fraud Defense	Empleados, contratistas, clientes y cualquier otra persona que envíe o reciba correos electrónicos a través del sistema de correo electrónico corporativo del Cliente	Información de encabezado de mensajes de correo electrónico, incluidas direcciones de correo electrónico, direcciones IP, nombres de remitente y destinatario.	EFD procesa la autenticación de mensajes basada en el dominio, la presentación de informes y la conformidad (DMARC) agrega informes y tráfico de muestras de mensajes forenses DMARC para los dominios de los clientes y evalúa la autenticidad de los remitentes basándose en la información de autenticación del remitente, y para destacar el tráfico enviado de fuentes no autenticadas y no autorizadas.	Los datos forenses de Cloudmark se conservan durante 30 días después de su recopilación. Los datos forenses de DMARC se conservan durante 90 días después de su recopilación.
Email Encryption	Empleados, contratistas, clientes y cualquier otra persona que envíe o reciba correos electrónicos a través del sistema de correo electrónico corporativo del Cliente	Cualquier Dato Personal incluido en un correo electrónico	Email Encryption ofrece una solución de cifrado y descifrado de mensajes totalmente integrada.	El contenido de los mensajes cifrados se conserva según lo determine el Responsable (hasta 366 días).
Email Protection	Empleados, contratistas y cualquier otra persona que envíe o reciba correos	Cualquier Dato Personal incluido en un correo electrónico	Email Protection incluye funciones como detección de spam para identificar y clasificar los mensajes de spam; funciones de protección antivirus para detectar y filtrar los mensajes que contienen virus conocidos; funciones antivirus de hora cero	Hasta 18 meses después de la recopilación

	electrónicos a través del sistema de correo electrónico corporativo del Responsable		para detectar y filtrar los mensajes con contenido sospechoso; una carpeta de cuarentena para analizar y eliminar el contenido sospechoso	
Endpoint Data Loss Protection	Empleados, contratistas	Metadatos registrados para los usuarios del Responsable	Endpoint Data Loss Prevention despliega un software (un agente) en los ordenadores de sobremesa y servidores propiedad del Cliente o controlados por este en plataformas compatibles. Estos agentes recopilan los metadatos registrados de las actividades de los usuarios con licencia y almacenan estos datos en el archivo de Endpoint Data Loss Prevention de Proofpoint.	Hasta 90 días desde el final de la suscripción del Responsable como máximo
Essentials	Empleados, contratistas, clientes	Cualquier Dato Personal incluido en un correo electrónico	• Escaneo, filtrado e itinerario de los mensajes de correo electrónico enviados y recibidos por partes externas al cliente, a través del sistema de correo electrónico corporativo del cliente. • Si se utiliza la función de archivo, véase "Archive" más arriba • Si se utiliza *sandboxing* TAP, véase "TAP" a continuación	Hasta 18 meses después de la recopilación.
Insider Threat Management SaaS	Empleados, contratistas: a) Analistas o administradores de ITM SaaS que usan el portal web. b) Los usuarios finales, valiéndose de parámetros de exportadores de datos en los que se instaló el agente ITM SaaS.	Dirección de correo electrónico, identificador de dispositivo como dirección IP, información de usuario como nombre e ID de usuario, información de página web como URL y nombre de la página, información de la aplicación como nombre de la aplicación, nombre del ejecutable y título de la ventana. Además, ITM permite capturar contenido de la pantalla, función configurada y controlada por el cliente. La captura de pantallas puede incluir cualquier dato personal adicional que aparezca en la pantalla del cliente.	ITM despliega un agente de extremo en el ordenador portátil, de sobremesa y servidores designados, propiedad del Responsable de datos o controlado por él. El agente recoge datos telemétricos sobre las actividades de los usuarios del dispositivo, las personas interesadas. En caso de que el Responsable de los datos lo permita, los agentes también podrán realizar capturas de pantalla de las actividades del dispositivo del usuario. El cliente se limita a determinar si permite la funcionalidad de captura de pantalla, así como el período de retención de datos para dicho contenido. Los datos de telemetría y de captura de pantalla se conservan en el almacenaje multiusuario ITM SaaS de Proofpoint.	De conformidad con el período de conservación seleccionado por el Responsable hasta un período máximo de 366 días.
Clasificación y protección inteligentes	Empleados, contratistas, clientes y cualquier persona que	Cualquier Dato Personal incluido en un documento.	Localiza e identifica automáticamente los datos sensibles y críticos para la empresa con el fin de mejorar las soluciones de protección de datos existentes, como el etiquetado, el cifrado, el control de accesos, la prevención de la pérdida de datos y el	Hasta 90 días desde el final de la suscripción del Responsable como máximo

	vea el documento.		CASB, y sugiere al Cliente reglas o directivas de protección	
Internal Mail Defense (IMD)	Empleados, contratistas	Cualquier Dato Personal incluido en un correo electrónico	IMD aprovecha las funciones de Email Protection y TAP para proteger las comunicaciones internas por correo electrónico del Cliente contra el spam y el contenido malicioso.	Hasta 18 meses después de la recopilación.
Browser Isolation y E-mail Isolation	Empleados y contratistas	Direcciones de correo electrónico, cookies de la web del usuario e historial de navegación, así como ubicación del centro de datos del contenedor de aislamiento.	Los productos Browser Isolation y E-mail Isolation establecen un navegador web remoto aislado o un entorno de correo electrónico web para proteger al Cliente de posibles amenazas cuando los Usuarios se conectan a Internet o a cuentas de correo electrónico basadas en la web en dispositivos propiedad del Cliente o del Responsable. El Cliente no permitirá que los Usuarios transmitan a través (o publiquen en) del producto ningún material infractor, difamatorio, amenazante u ofensivo.	Hasta 90 días desde el final de la suscripción del Responsable como máximo
NexusAI for Compliance	Empleados, contratistas y clientes	Cualquier dato personal incluido en el contenido recopilado (incluidos los correos electrónicos, los mensajes instantáneos, el contenido en redes sociales, la telemetría de los mensajes asociados y los archivos adjuntos)	NexusAI for Compliance utiliza el aprendizaje automático para evaluar los mensajes archivados compatibles (como el correo electrónico, las redes sociales, las plataformas de colaboración y los mensajes móviles) marcados para revisión del Cliente por el producto Intelligent Supervision de Proofpoint.	Hasta 24 horas desde el final de la suscripción del Responsable como máximo
Nexus People Risk Explorer	Empleados, contratistas	Nombres, direcciones de correo electrónico, cualquier Dato Personal contenido en Threat Analytics	Proofpoint Nexus People Risk Explorer aprovecha los datos de seguridad de personas de Proofpoint Targeted Attack Protection, Security Awareness Training, Cloud Account Defense y Cloud Account Security Broker para proporcionar información sobre los tipos, la gravedad y la frecuencia de las amenazas dirigidas al Cliente y sus empleados.	Hasta 90 días desde el final de la suscripción del Responsable como máximo
Suite Anti-Phishing (incluye PhishAlarm y PhishAlarmAnalyzer)	Empleados, contratistas	Nombre Dirección de correo electrónico Cualquier Dato Personal incluido en un correo electrónico	Enrutamiento y escaneo de correos electrónicos sospechosos denunciados por los usuarios finales con el botón PhishAlarm. PhishAlarm Analyzer ofrece una identificación de los ataques de phishing con gran capacidad de respuesta en tiempo real. Los correos electrónicos denunciados a través de PhishAlarm y PhishAlarm Analyzer son consultados y categorizados, y están inmediatamente disponibles para los equipos de respuesta del Cliente.	Hasta 30 días desde el final de la suscripción del Responsable como máximo; con la excepción de los Threat Analytics, que se conservan hasta 18 meses después de la recopilación
Proofpoint Security Awareness Training (PSAT)	Empleados, contratistas	Nombre, correo electrónico y otros campos de datos seleccionados por el cliente para su carga a PSAT a partir del directorio Active Directory del cliente	Los Datos Personales se usan para la implantación de la formación llamada Cyber Security Awareness, así como para evaluaciones y informes de seguridad de empleados	Hasta 90 días desde el final de la suscripción del Responsable como máximo; sin embargo, durante la suscripción del Responsable, los administradores de este pueden realizar

				cambios y eliminar usuarios.
Secure E-Mail Relay (SER)	Empleados Contratistas Todos los destinatarios de correos electrónicos masivos enviados a través del sistema de correo electrónico corporativo del Cliente	Nombre Dirección de correo electrónico Cualquier Dato Personal incluido en un correo electrónico	Secure Email Relay (SER) es una solución alojada y multilicencia que cede al cliente en control de las aplicaciones que envían correo electrónico utilizando los dominios propios o controlados por el Cliente. Añade una capa de seguridad a cada aplicación y distribuye el correo electrónico a Internet de una forma compatible con DMARC después de que se realicen las comprobaciones AS/AV de Proofpoint. SER se puede utilizar solo para el envío de correos electrónicos que cumplan con la legislación aplicable sobre mensajes masivos o no solicitados.	Hasta 30 días desde el final de la suscripción del Responsable como máximo
SecureShare	Empleados, contratistas, cualquier otra persona invitada a ver un archivo compartido	Nombre, direcciones de correo electrónico	SecureShare es un método seguro para compartir archivos y almacenarlos temporalmente.	Hasta 180 días después de la recopilación.
Targeted Attack Protection (TAP)	Empleados, contratistas, clientes y cualquier otra persona que envíe o reciba correos electrónicos a través del sistema de correo electrónico corporativo del Cliente	Nombre Dirección de correo electrónico Cualquier Dato Personal incluido en un correo electrónico	TAP identifica y protege contra las URL maliciosas y los archivos adjuntos maliciosos en los correos electrónicos utilizando un motor de análisis dinámico de malware.	Hasta 18 meses después de la recopilación.
Threat Response Auto-pull (TRAP)	Empleados, contratistas, clientes y cualquier otra persona que envíe o reciba correos electrónicos a través del sistema de correo electrónico corporativo del Cliente	Nombre Dirección de correo electrónico Cualquier Dato Personal incluido en un correo electrónico	TRAP es una plataforma de gestión de incidencias que incluye automatización para analizar y eliminar los correos electrónicos no deseados.	El periodo de conservación de los incidentes cerrados lo establece el Responsable. Todos los datos MIME de los mensajes se purgan cada 30 días para los incidentes cerrados.
ThreatSimulator	Empleados, contratistas	Nombre Dirección de correo electrónico	Los Datos Personales se utilizan para simular campañas de phishing. El Cliente solo podrá realizar simulaciones de correos electrónicos de phishing a dominios que sean de su propiedad o estén bajo su control.	A petición del cliente y dentro de los 90 días siguientes a dicha petición.
Zero Trust Network Access (antes Meta)	Empleados, contratistas	Dirección, nombre (y, en su caso, número de teléfono) del usuario, así como tráfico de eventos en intranet tales como aceptación o declinación de	Meta superpone una red de confianza cero a la red corporativa del cliente. Los usuarios acceden a la red corporativa conectándose a la capa de la red Meta a través de un VPN con sus credenciales de identificación. Una vez iniciada sesión en la red meta, a cada usuario se le asigna una identidad única que conecta a la red corporativa subyacente de exportadores de datos; el acceso a activos	Hasta 90 días desde el final de la suscripción del Responsable como máximo

		eventos y solicitudes de DNS (el cliente tiene la opción de activar o desactivar el registro de eventos de tráfico de internet)	dentro de la red corporativa del exportador de datos se realiza con base en la identidad única del usuario	

1. Subencargados

Pueden encontrar una lista actualizada de Subencargados en la dirección https://www.proofpoint.com/us/legal/trust.

APÉNDICE 2 AL ATD – SEGURIDAD DEL TRATAMIENTO

Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del Tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el Encargado del Tratamiento aplicará las medidas técnicas y organizativas descritas a continuación para garantizar un nivel de seguridad adecuado para la prestación de Servicios:

A. *Autenticación de usuario*

La dirección ha adoptado y aprobado un programa de seguridad de la información.
Se ha desarrollado un marco de directivas y normas de seguridad de la información que respalda los objetivos del programa de seguridad de la información.
Existen procedimientos para la autenticación y autorización de usuarios a los sistemas, y para garantizar su cumplimiento.
Existen procedimientos para garantizar la observación de las directivas a la hora de solicitar, establecer, emitir, suspender, eliminar y cerrar cuentas de usuario y sus privilegios de acceso asociados (p. ej., acceso al sistema concedido según el principio de privilegio mínimo necesario para una función).
Se dispone de un proceso para supervisar intentos fallidos de acceso. Se resuelven las violaciones de seguridad identificadas.
El acceso al entorno de producción del Encargado por parte de los empleados de este se concede en función de las necesidades empresariales. Se empleará una VPN con autenticación de dos factores.
Existen controles para limitar la introducción de cambios en la producción únicamente a personas autorizadas.

Tipo de acceso

Los distintos tipos de acceso de usuarios finales del cliente están documentados en las Guías del administrador de cada servicio, y los administradores del cliente se encargan de su control a través de un panel de servicio, interfaz de usuario o integración SAML.

B. *Realización de copias de seguridad*

Los datos de configuración y datos reportados por el cliente son sometidos a copias de seguridad periódicas y almacenados en un disco giratorio.

Se han documentado e implementado procedimientos de copia de seguridad y conservación de datos y programas.

C. *Ordenadores y terminales de acceso*

Los ordenadores utilizados por los empleados del Responsable para acceder a la infraestructura de este deben utilizar un túnel VPN seguro. Todos los terminales de empleados deben contar con aplicaciones antivirus actualizadas y existen políticas que restrinjan qué aplicaciones se pueden instalar en dichos equipos. Todos los empleados del Responsable deben autenticarse ante un sistema de autenticación centralizada para poder acceder a las redes productivas y corporativas del Responsable.

Controles del Encargado de datos

Los nuevos empleados deben firmar un acuerdo de confidencialidad relativo a aplicaciones exclusivas y a la confidencialidad de la información referente a los clientes.
Los nuevos empleados reciben también una copia del Código de Conducta de Seguridad del Encargado, un resumen del programa de seguridad de la información de Encargado, y deberán confirmar haberla recibido.
El acceso al entorno de producción del Encargado por parte de los empleados de este se concede en función de las necesidades empresariales. Se empleará una VPN con autenticación de dos factores.

Se utilizan herramientas de gestión centralizada de la configuración para garantizar que los terminales de los empleados estén configurados adecuadamente.

D. ***Registros de acceso***

En relación con los Servicios, existen al menos dos formas diferenciadas de registro de acceso:

Todos los intentos de acceso a los sistemas informáticos del Encargado de Datos se registran a nivel central y toda actividad inusual se reporta al grupo de Seguridad de la Información Global del Encargado. Además, el Encargado dispone de políticas de bloqueo de cuentas y requisitos de contraseña. Los registros de acceso de clientes a los Servicios se generan y almacenan según corresponda a cada Servicio.

Existen procedimientos para la autenticación y autorización de usuarios a los sistemas, y para garantizar su cumplimiento.
Existe un proceso de control que se sigue para revisar y confirmar de manera periódica que los privilegios de acceso siguen siendo autorizados y adecuados.
Se dispone de un proceso para supervisar intentos fallidos de acceso. Las violaciones de seguridad identificadas son investigadas y resueltas.
Los datos de eventos de las aplicaciones se almacenan para proporcionar registros e información cronológica que permitan la revisión, el examen, la reconstrucción de sistemas y de eventos en las aplicaciones y el tratamiento de datos.

E. ***Sistemas de telecomunicaciones***

Todas las instalaciones de producción del Encargado disponen de suministros de internet redundantes con distintos proveedores de banda ancha.

F. ***Formación del personal***

Todo el personal del Encargado debe completar un programa anual de formación en línea en materia de Seguridad y Sensibilización. Además, el personal puede recibir formación continua específica para sus puestos. Esta formación podrá ser proporcionada por Proofpoint o por otras organizaciones externas.

El Encargado cuenta con un plan organizativo que separa los roles y las obligaciones que resultan incompatibles para el personal pertinente.
La separación de roles de gestión y responsabilidades ha sido diseñada para segregar los roles de operaciones informáticas, desarrollo de sistemas y mantenimiento de las funciones corporativas generales del Encargado.
Los roles y las responsabilidades del personal están claramente definidos.

G. ***Uso de ordenadores***

El acceso remoto a las redes de producción del Encargado está restringido a sistemas que dispongan de una aplicación de seguridad aprobada y gestionada por el Encargado. Todos los sistemas del Encargado proporcionados al personal se gestionan a través de un sistema centralizado de configuración. Todos los empleados del Encargado son informados acerca de las políticas del Encargado de uso aceptable de ordenadores del Encargado, acceso a Internet y comunicaciones por correo electrónico. Los empleados del Encargado deben aceptar estas políticas y aceptan respetarlas.

Los nuevos empleados deben firmar un acuerdo de confidencialidad relativo a aplicaciones exclusivas y a la confidencialidad de la información referente a los clientes.

Los nuevos empleados revisarán y aceptarán el código de conducta en materia de seguridad del Encargado.

H. ***Impresión de datos***

Los datos de clientes se tratan en memoria y no están disponibles para su impresión. Además, no existen impresoras disponibles en los centros de datos de producción del Encargado y todos los servicios de impresión están inhabilitados por defecto en todos los servidores de producción.

K. ***Control de acceso físico***

Controles del Encargado de datos

Al alojar los productos en proveedores de ubicación conjunta, el Encargado mantiene controles sobre el acceso físico a los Infraestructura del Encargado. En el caso de productos alojados en proveedores de alojamiento AWS, Azure o Google Cloud, el control del acceso físico corresponde al proveedor de alojamiento.

L. **Medidas de seguridad física para centros de datos**

Los controles de seguridad física de las instalaciones de ubicación conjunta se ajustan a las normas de los centros de datos de nivel III, incluida la seguridad *in situ* en régimen ininterrumpido (24 horas al día), los puntos de acceso con personal, los mecanismos contra el fraude, la autenticación de dos factores y la vigilancia por circuito cerrado de televisión. Las instalaciones utilizadas por AWS, Azure o Google Cloud se conforman a los estándares aplicables a los centros de datos de nivel III.

M. ***Control de acceso a sistemas informáticos***

Controles del Encargado de datos

El Encargado de datos controla el acceso a los sistemas que proporcionan los Servicios por las siguientes vías:

1. Todos los empleados y contratistas del Encargado de datos disponen de identidades de usuario únicas. No está permitido compartir cuentas.
2. Los requisitos de contraseña vienen definidos y aplicados mediante una herramienta de sincronización de contraseñas. Los requisitos incluyen:
    a. Longitud mínima de 12 caracteres
    b. No debe aparecer en las listas públicas de contraseñas vulneradas
    c. Historial de las últimas 23
    d. Necesidad de cambiar cada 180 días
    e. Cuenta bloqueada tras cinco (5) intentos fallidos de acceso
3. Acceso lógico concedido en función del rol.
4. El VPN de acceso al entorno de producción del Encargado de Datos dispone de un sistema de registro de auditoría.
5. Los registros de auditoría son supervisados en tiempo casi real por medio de una herramienta de agregación y alerta de registros. Las alertas están configuradas para enviarse al grupo de Seguridad de la Información Global del Encargado de Datos.

N. ***Control de acceso a datos***

Los datos de Clientes no pueden permanecer en el entorno corporativo del Encargado. El acceso a los sistemas en que se alojen los Servicios está controlado de los siguientes modos:

1. Acceso basado en un rol definida por el Encargado.
2. El acceso privilegiado a un entorno de producción del Encargado solo se permitirá al personal autorizado de este.

O. El VPN y los sistemas del entorno de producción del Encargado disponen de un sistema de ***registro de auditoría***.

P. ***Implantación de control de acceso con privilegio mínimo***

El acceso al entorno de producción del Encargado se concede en función del rol.

Q. ***Seguridad durante la transferencia y el tratamiento***

El Encargado no permite que los datos de Clientes permanezcan en su entorno corporativo, en el cual residen sus empleados y contratistas. El entorno de producción del Encargado está segregado desde un punto de vista lógico y físico del entorno corporativo del Encargado:

1. El acceso al entorno de producción del Encargado se realiza a través de una VPN con autenticación de dos factores utilizando dispositivos aprobados por el Encargado y solo se concede a empleados y contratistas del Encargado cuya función requiera este acceso.
2. Existen cortafuegos conformes a las prácticas habituales en el sector instalados y configurados para permitir únicamente el tráfico en los puertos necesarios para el funcionamiento de los Servicios, siendo todos los demás denegados por defecto.
3. Todos los accesos de administrador a la interfaz web que aloja los Servicios están encriptados mediante HTTPS/TLS.

Control del acceso al sistema

1. Empleo de un protocolo LDAP para autenticar al personal del Encargado en los entornos de producción.
2. Solo se concede acceso privilegiado al personal autorizado del Encargado.

Seguridad de punto final

1. Los terminales utilizados para acceder al entorno de producción del Encargado de datos se gestionan de forma centralizada, tienen instalados los parches de seguridad aplicables, ejecutan software de seguridad estandarizado y se analizan periódicamente en busca de vulnerabilidades.

Seguridad de servidor

1. Los parches de seguridad aplicables se aplican en función de su carácter crítico.
2. Servicios innecesarios desconectados.
3. Contraseñas por defecto modificadas.

R. ***Seguridad durante la transmisión de datos en redes públicas***

1. Todos los accesos administrativos a los Servicios por parte de Encargado están encriptados mediante HTPS/TLS.

S. ***Controles en fase operativa y de implantación***

La funcionalidad que proporcionan los Servicios se efectúa de manera automática y no requiere intervención humana, excepto a los efectos de análisis y para resolver problemas en los Servicios. Los Servicios están designados para funcionar tal y como está descrito en el Acuerdo de Servicios.

T. ***Trazabilidad de cualquier acceso, cambio o eliminación***

El acceso a los sistemas usados por los Servicios está controlado de los siguientes modos:

1. El acceso se concede en base a la función definida por el Encargado.
2. Solo el personal autorizado tiene permiso para tener acceso privilegiado al entorno de producción del Encargado.
3. El VPN y los sistemas del entorno de producción del Encargado disponen de un sistema de registro de auditoría.

4. Los registros de auditoría generados por los Servicios capturan el acceso a los Servicios por parte del personal del Responsable de Datos.

U. *Garantía de tratamiento conforme de los datos*

Excepto a los efectos de análisis y para resolver problemas en los Servicios, el personal del Encargado de los Servicios no trata los datos de los Clientes de forma manual. Todos los datos de Clientes serán tratados de manera automática por los Servicios, tal y como se describe en la documentación de los Servicios.

V. *Garantía de disponibilidad*

Se consigue del siguiente modo:

1. La infraestructura de todos los centros de producción está configurada en modo de alta disponibilidad, incluidas fuentes de alimentación eléctrica dobles y un mínimo de dos conexiones diferenciadas a la red.
2. Las instalaciones de ubicación conjunta se ajustan a las normas aplicables a los centros de datos de nivel III, incluida la alimentación redundante y los controles ambientales redundantes.
3. Las instalaciones de ubicación conjunta disponen de generadores *in situ* con un suministro de combustible para un mínimo de dos (2) días.
4. Cada año se documenta y comprueba un Plan de Acción de Continuidad de Negocio para la protección del personal del Encargado de Datos y la recuperación de sus procesos empresariales.
5. Una infraestructura de seguimiento distribuida controla la disponibilidad y el rendimiento.
6. .

W. *Separación de datos*

Los Servicios mantienen la separación de los datos de clientes. Se consigue del siguiente modo:

1. El servicio mantiene la separación lógica utilizando algunos o todos los siguientes elementos:
   a. Identidades de Cliente únicas para cada cliente que se utilizan para etiquetar los datos del cliente dentro del servicio;
   b. IP únicas; o
   c. claves de cifrado únicas.

ANEXO 2

Cláusulas Contractuales Tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

CLÁUSULAS CONTRACTUALES TIPO

de responsable a encargado

SECCIÓN I

Cláusula 1

Finalidad y ámbito de aplicación

(a) La finalidad de estas cláusulas contractuales tipo es garantizar que se cumplan los requisitos que 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 (Reglamento general de protección de datos), exige para la transferencia de datos personales a un tercer país.

(b) Las partes:

(i) la(s) persona(s) física(s) o jurídica(s), autoridad(es) pública(s), servicio(s) u organismo(s) (en lo sucesivo, "entidad" o "entidades") que va(n) a transferir los datos personales, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo "exportador de datos"), y

(ii) la(s) entidad(es) en un tercer país que va(n) a recibir los datos personales del exportador de datos directamente o indirectamente por medio de otra entidad que también sea parte en el presente pliego de cláusulas, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo "importador de datos"), han pactado las presentes cláusulas contractuales tipo (en lo sucesivo, "pliego de cláusulas").

(c) El presente pliego de cláusulas se aplica a la transferencia de datos personales especificada en el anexo I.B.

(d) El apéndice del presente pliego de cláusulas, que contiene los anexos que se citan en estas, forman parte del pliego.

Cláusula 2

Efecto e invariabilidad de las cláusulas

(a) El presente pliego de cláusulas establece garantías adecuadas, incluidos derechos exigibles de los interesados y acciones judiciales eficaces, de conformidad con el artículo 46, apartado 1, y el artículo 46, apartado 2, letra c), del Reglamento (UE) 2016/679 y, en relación con las transferencias de datos de responsables a encargados o de encargados a otros encargados, de conformidad con las cláusulas contractuales tipo a que se refiere el artículo 28, apartado 7, del Reglamento (UE) 2016/679 siempre que no se modifiquen, salvo para seleccionar el módulo o módulos adecuados o para añadir o actualizar información del apéndice. Esto no es óbice para que las partes incluyan en un contrato más amplio las cláusulas contractuales tipo que contiene el presente pliego, ni para que añadan otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, al presente pliego de cláusulas ni perjudiquen los derechos o libertades fundamentales de los interesados.

(b) El presente pliego de cláusulas se entiende sin perjuicio de las obligaciones a las que esté sujeto el exportador de datos en virtud del Reglamento (UE) 2016/679.

Cláusula 3

Terceros beneficiarios

(a) Los interesados podrán invocar, como terceros beneficiarios, el presente pliego de cláusulas contra el exportador y/o el importador de datos y exigirles su cumplimiento, con las excepciones siguientes.

(i) Cláusulas 1, 2, 3, 6 y 7.

(ii) Cláusula 8 – Cláusula 8.1 letra b), y cláusula 8.9, letras a), c), d) y e);

(iii) Cláusula 9 – Cláusula 9, letras a), c), d) y e);

(iv) Cláusula 12 – Cláusula 12, letras a), d) y f);

(v) Cláusula 13;

(vi) Cláusula 15.1, letras c), d) y e);
(vii) Cláusula 16, letra e);
(viii) Cláusula 18 – Cláusula 18, letras a) y b)
(b) Lo dispuesto en la letra a) se entiende sin perjuicio de los derechos que el Reglamento (UE) 2016/679 otorga a los interesados.

Cláusula 4

Interpretación

(a) Cuando en el presente pliego de cláusulas se utilizan términos definidos en el Reglamento (UE) 2016/679, se entiende que tienen el mismo significado que en dicho Reglamento.

(b) El presente pliego de cláusulas deberá leerse e interpretarse con arreglo a las disposiciones del Reglamento (UE) 2016/679.

(c) El presente pliego de cláusulas no se podrá interpretar de manera que entre en conflicto con los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679.

Cláusula 5

Jerarquía

En caso de contradicción entre el presente pliego de cláusulas y las disposiciones de acuerdos conexos entre las partes que estuvieren en vigor en el momento en que se pactare o comenzare a aplicarse el presente pliego de cláusulas, prevalecerá el presente pliego de cláusulas.

Cláusula 6

Descripción de la transferencia o transferencias

Los datos de la transferencia o transferencias y, en particular, las categorías de datos personales que se transfieren y los fines para los que se transfieren se especifican en el anexo I.B.

Cláusula 7 (opcional)

Cláusula de incorporación (no aplicable)

SECCIÓN II: OBLIGACIONES DE LAS PARTES

Cláusula 8

Garantías en materia de protección de datos

El exportador de datos garantiza que ha hecho esfuerzos razonables para determinar que el importador de datos puede, aplicando medidas técnicas y organizativas adecuadas, cumplir las obligaciones que le atribuye el presente pliego de cláusulas.

Transferencia de responsable a encargado

8.1 **Instrucciones**

(a) El importador de datos solo tratará los datos personales siguiendo instrucciones documentadas del exportador de datos. El exportador de datos podrá dar dichas instrucciones durante todo el período de vigencia del contrato.

(b) El importador de datos informará inmediatamente al exportador de datos en caso de que no pueda seguir dichas instrucciones.

8.2 **Limitación de la finalidad**

El importador de datos tratará los datos personales únicamente para los fines específicos de la transferencia indicados en el anexo I.B, salvo cuando siga instrucciones adicionales del exportador de datos.

8.3 **Transparencia**

Previa solicitud, el exportador de datos pondrá gratuitamente a disposición del interesado una copia del presente pliego de cláusulas, incluido el apéndice cumplimentado por las partes. En la medida en que sea necesario para

proteger secretos comerciales u otro tipo de información confidencial, como las medidas descritas en el anexo II y datos personales, el exportador de datos podrá expurgar el texto del apéndice del presente pliego de cláusulas antes de compartir una copia, pero deberá aportar un resumen significativo si, de no hacerlo, el interesado no pudiere comprender el tenor del apéndice o ejercer sus derechos. Previa solicitud, las partes comunicarán al interesado los motivos del expurgo, en la medida de lo posible sin revelar la información expurgada. La presente cláusula se entiende sin perjuicio de las obligaciones que los artículos 13 y 14 del Reglamento (UE) 2016/679 atribuyen al exportador de datos.

8.4 **Exactitud**

Si el importador de datos tiene conocimiento de que los datos personales que ha recibido son inexactos o han quedado obsoletos, informará de ello al exportador de datos sin dilación indebida. En este caso, el importador de datos colaborará con el exportador de datos para suprimir o rectificar los datos.

8.5 **Duración del tratamiento y supresión o devolución de los datos**

El tratamiento por parte del importador de datos solo se realizará durante el período especificado en el anexo I.B. Una vez se hayan prestado los servicios de tratamiento, el importador de datos suprimirá, a petición del exportador de datos, todos los datos personales tratados por cuenta del exportador de datos y acreditará al exportador de datos que lo ha hecho, o devolverá al exportador de datos todos los datos personales tratados en su nombre y suprimirá las copias existentes. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país. Lo anterior se entiende sin perjuicio de la cláusula 14 y, en particular, de la obligación que esta impone al importador de datos de informar al exportador de datos durante todo el período de vigencia del contrato si tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la Cláusula 14, letra a).

8.6 **Seguridad del tratamiento**

(a) El importador de datos y, durante la transferencia, también el exportador de datos, aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos; en particular, la protección contra violaciones de seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados (en lo sucesivo, "violación de la seguridad de los datos personales"). A la hora de determinar un nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados. Las partes deberán considerar, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento. En caso de seudonimización, la información adicional necesaria para atribuir los datos personales a un interesado específico quedará, en la medida de lo posible, bajo el control exclusivo del exportador de datos. Al cumplir las obligaciones que le impone el presente párrafo, el importador de datos aplicará, al menos, las medidas técnicas y organizativas que figuran en el anexo II. El importador de datos llevará a cabo controles periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.

(b) El importador de datos solo concederá acceso a los datos personales a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato. Garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

(c) En caso de violación de la seguridad de datos personales tratados por el importador de datos en virtud del presente pliego de cláusulas, el importador de datos adoptará medidas adecuadas para ponerle remedio y, en particular, medidas para mitigar los efectos negativos. El importador de datos también lo notificará al exportador de datos sin dilación indebida una vez tenga conocimiento de la violación de la seguridad. Dicha notificación incluirá los datos de un punto de contacto en el que pueda obtenerse más información, una descripción de la naturaleza de la violación (en la que figuren, cuando sea posible, las categorías y el número aproximado de interesados y registros de datos personales afectados), las consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, especialmente, en su

caso, medidas para mitigar sus posibles efectos negativos. Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

(d) El importador de datos deberá colaborar con el exportador de datos y ayudarle para que pueda cumplir las obligaciones que le atribuye el Reglamento (UE) 2016/679, especialmente en cuanto a la notificación a la autoridad de control competente y a los interesados afectados, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el importador de datos.

8.7 **Datos sensibles**

En la medida en que la transferencia incluya datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales (en lo sucesivo, "datos sensibles"), el importador de datos aplicará las restricciones específicas y/o las garantías adicionales descritas en el anexo I.B.

8.8 **Transferencias ulteriores**

El importador de datos solo comunicará los datos personales a un tercero siguiendo instrucciones documentadas del exportador de datos. Por otra parte, solo se podrán comunicar los datos a terceros situados fuera de la Unión Europea (4) (en el mismo país que el importador de datos o en otro tercer país; en lo sucesivo, "transferencia ulterior") si el tercero está vinculado por el presente pliego de cláusulas o consiente a someterse a este, con elección del módulo correspondiente, o si:

(i) la transferencia ulterior va dirigida a un país sobre el que haya recaído una decisión de adecuación, con arreglo al artículo 45 del Reglamento (UE) 2016/679, que abarque la transferencia ulterior;

(ii) el tercero aporta de otro modo garantías adecuadas, con arreglo a los artículos 46 o 47 del Reglamento (UE) 2016/679, respecto del tratamiento en cuestión;

(iii) si la transferencia ulterior es necesaria para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos; o

(iv) si la transferencia ulterior es necesaria para proteger intereses vitales del interesado o de otra persona física.

La validez de las transferencias ulteriores depende de que el importador de datos aporte las demás garantías previstas en el presente pliego de cláusulas y, en particular, la limitación de la finalidad.

8.9 **Documentación y cumplimiento**

(a) El importador de datos resolverá con presteza y de forma adecuada las consultas del exportador de datos relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.

(b) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen por cuenta del exportador de datos.

(c) El importador de datos pondrá a disposición del exportador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente pliego de cláusulas y, a instancia del exportador de datos, permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza un examen o una auditoría, el exportador de datos podrá tener en cuenta las certificaciones pertinentes que obren en poder del importador de datos.

(d) El exportador de datos podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías podrán consistir en inspecciones de los locales o instalaciones físicas del importador de datos y, cuando proceda, realizarse con un preaviso razonable.

(e) Las partes pondrán a disposición de la autoridad de control competente, a instancia de esta, la información a que se refieren las letras b) y c) y, en particular, los resultados de las auditorías.

_____

(4) El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el "Acuerdo EEE") dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

Cláusula 9

Recurso a subencargados

(a) AUTORIZACIÓN GENERAL POR ESCRITO: El importador de datos cuenta con una autorización general del exportador de datos para contratar a subencargados que figuren en una lista acordada. El importador de datos informará al exportador de datos específicamente y por escrito de las adiciones o sustituciones de subencargados previstas en dicha lista con al menos [especificar período de tiempo] de antelación, de modo que el exportador de datos tenga tiempo suficiente para formular objeción a tales cambios antes de que se contrate al subencargado o subencargados de que se trate. El importador de datos proporcionará al exportador de datos la información necesaria para que este pueda ejercer su derecho a formular objeción.

(b) Cuando el importador de datos recurra a un subencargado para llevar a cabo actividades específicas de tratamiento (por cuenta del exportador de datos), lo hará por medio de un contrato escrito que establezca, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al importador de datos en virtud del presente pliego de cláusulas, especialmente en lo que se refiere a los derechos de los interesados en cuanto que terceros beneficiarios. (8) Las Partes convienen que, al cumplir el presente pliego de cláusulas, el importador de datos también da cumplimiento a las obligaciones que le atribuye la cláusula 8.8. El importador de datos se asegurará de que el subencargado cumpla las obligaciones que le atribuya el presente pliego de cláusulas.

(c) El importador de datos proporcionará al exportador de datos, a instancia de este, una copia del contrato con el subencargado y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el importador de datos podrá expurgar el texto del contrato antes de compartir la copia.

(d) El importador de datos seguirá siendo plenamente responsable ante el exportador de datos del cumplimiento de las obligaciones que imponga al subencargado su contrato con el importador de datos. El importador de datos notificará al exportador de datos los incumplimientos por parte del subencargado de las obligaciones que le atribuye dicho contrato.

(e) El importador de datos pactará con el subencargado una cláusula de tercero beneficiario en virtud de la cual, en caso de que el importador de datos desaparezca de facto, cese de existir jurídicamente o sea insolvente, el exportador de datos tendrá derecho a rescindir el contrato del subencargado y ordenar a este que suprima o devuelva los datos personales.

(8) Este requisito podrá satisfacerse si el subencargado se adhiere al presente pliego de cláusulas, con elección del módulo correspondiente, con arreglo a la cláusula 7.

Cláusula 10

Derechos del interesado

(a) El importador de datos notificará con presteza al exportador de datos las solicitudes que reciba del interesado. No responderá a dicha solicitud por sí mismo, a menos que el exportador de datos le haya autorizado a hacerlo.

(b) El importador de datos ayudará al exportador de datos a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos que el Reglamento (UE) 2016/679 atribuye a los interesados. A este respecto, las partes establecerán en el anexo II medidas técnicas y organizativas apropiadas, teniendo en cuenta la naturaleza del tratamiento, por las que se garantice que se prestará ayuda al responsable a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.

(c) En el cumplimiento de las obligaciones que le atribuyen las letras a) y b), el importador de datos seguirá las instrucciones del exportador de datos.

Cláusula 11

Reparación

(a) El importador de datos informará a los interesados, de forma transparente y en un formato de fácil acceso, mediante notificación individual o en su página web, del punto de contacto autorizado para tramitar reclamaciones. Este tramitará con presteza las reclamaciones que reciba de los interesados.

(b) En caso de litigio entre un interesado y una de las partes en relación con el cumplimiento del presente pliego de cláusulas, dicha parte hará todo lo posible para resolver amistosamente el problema de forma oportuna. Las partes se mantendrán mutuamente informadas de tales litigios y, cuando proceda, colaborarán para resolverlos.

(c) El importador de datos se compromete a aceptar, cuando el interesado invoque un derecho de tercero beneficiario con arreglo a la cláusula 3, la decisión del interesado de:

(i) presentar una reclamación ante la autoridad de control del Estado miembro de su residencia habitual o su lugar de trabajo o ante la autoridad de control competente con arreglo a la cláusula 13;
(ii) ejercitar una acción judicial en el sentido de la cláusula 18.
(d) Las partes aceptan que el interesado pueda estar representado por una entidad, organización o asociación sin ánimo de lucro en las condiciones establecidas en el artículo 80, apartado 1, del Reglamento (UE) 2016/679.

(e) El importador de datos acepta acatar las resoluciones que sean vinculantes con arreglo al Derecho aplicable de la UE o del Estado miembro de que se trate.

(f) El importador de datos acepta que la elección del interesado no menoscabe sus derechos sustantivos y procesales a obtener reparación de conformidad con el Derecho aplicable.

Cláusula 12

Responsabilidad

(a) Cada parte será responsable ante la(s) otra(s) de cualquier daño y perjuicio que le(s) cause por cualquier vulneración del presente pliego de cláusulas.

(b) El importador de datos será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el importador de datos o su subencargado ocasionen al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas.

(c) A pesar de lo dispuesto en la letra b), el exportador de datos será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el exportador de datos o el importador de datos (o su subencargado) ocasionen al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas. Lo anterior se entiende sin perjuicio de la responsabilidad del exportador de datos y, cuando el exportador de datos sea un encargado que actúe por cuenta de un responsable, de la responsabilidad del responsable con arreglo al Reglamento (UE) 2016/679 o el Reglamento (UE) 2018/1725, según cuál sea de aplicación.

(d) Las partes acuerdan que, si el exportador de datos es considerado responsable, de conformidad con la letra c), de los daños o perjuicios causados por el importador de datos (o su subencargado), estará legitimado para exigir al importador de datos la parte de la indemnización que sea responsabilidad del importador de los datos.

(e) Cuando más de una parte sea responsable de un daño o perjuicio ocasionado al interesado como consecuencia de una vulneración del presente pliego de cláusulas, todas las partes responsables serán responsables solidariamente.

(f) Las partes acuerdan que, si una parte es considerada responsable con arreglo a la letra e), estará legitimada para exigir a la otra parte la parte de la indemnización correspondiente a su responsabilidad por el daño o perjuicio.

(g) El importador de datos no puede alegar la conducta de un subencargado del tratamiento para eludir su propia responsabilidad.

Cláusula 13

Supervisión

(a) [Cuando el exportador de datos esté establecido en un Estado miembro de la UE:] La autoridad de control responsable de garantizar el cumplimiento por parte del exportador de datos del Reglamento (UE) 2016/679 en lo que respecta a la transferencia de datos, como se indica en el Anexo I.C, actuará como autoridad de control competente.
[Cuando el exportador de datos no esté establecido en un Estado miembro de la UE, pero entre en el ámbito territorial de aplicación del Reglamento (UE) 2016/679 de conformidad con su artículo 3, apartado 2, y haya designado un representante con arreglo al artículo 27, apartado 1, del Reglamento (UE) 2016/679:] La autoridad de control del Estado miembro en el que esté establecido el representante en el sentido del artículo 27, apartado 1, del Reglamento (UE) 2016/679, tal como se indica en el anexo I.C, actuará como autoridad de control competente. [Cuando el exportador de datos no esté establecido en un Estado miembro de la UE, pero entre en el ámbito territorial de aplicación del Reglamento (UE) 2016/679 de conformidad con su artículo 3, apartado 2, sin que, no obstante, tenga que designar un representante con arreglo al artículo 27, apartado 2, del Reglamento (UE) 2016/679:] La autoridad de control de uno de los Estados miembros en que estén situados los interesados cuyos datos personales se transfieran en virtud del presente pliego de cláusulas en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado, indicada en el anexo I.C, actuará como autoridad de control competente.

(b) El importador de datos da su consentimiento a someterse a la jurisdicción de la autoridad de control competente y a cooperar con ella en cualquier procedimiento destinado a garantizar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos se compromete a responder a consultas, someterse a auditorías y cumplir las medidas adoptadas por la autoridad de control y, en particular, las medidas correctivas e indemnizatorias. Remitirá a la autoridad de control confirmación por escrito de que se han tomado las medidas necesarias.

SECCIÓN III:DERECHO DEL PAÍS Y OBLIGACIONES EN CASO DE ACCESO POR PARTE DE LAS AUTORIDADES PÚBLICAS

Cláusula 14

Derecho y prácticas del país que afectan al cumplimiento de las cláusulas

(a) Las partes aseguran que no tienen motivos para creer que el Derecho y las prácticas del tercer país de destino aplicables al tratamiento de los datos personales por el importador de datos, especialmente los requisitos para la comunicación de los datos personales o las medidas de autorización de acceso por parte de las autoridades públicas, impidan al importador de datos cumplir las obligaciones que le atribuye el presente pliego de cláusulas. Dicha aseveración se fundamenta en la premisa de que no se oponen al presente pliego de cláusulas el Derecho y las prácticas que respeten en lo esencial los derechos y libertades fundamentales y no excedan de lo que es necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.

(b) Las partes declaran que, al aportar la garantía a que se refiere la letra a), han tenido debidamente en cuenta, en particular, los aspectos siguientes:
   (i) las circunstancias específicas de la transferencia, como la longitud de la cadena de tratamiento, el número de agentes implicados y los canales de transmisión utilizados; las transferencias ulteriores previstas; el tipo de destinatario; la finalidad del tratamiento; las categorías y el formato de los datos personales transferidos; el sector económico en el que tiene lugar la transferencia; el lugar de almacenamiento de los datos transferidos;
   (ii) el Derecho y las prácticas del tercer país de destino —especialmente las que exijan comunicar datos a las autoridades públicas o autorizar el acceso de dichas autoridades— que sean pertinentes dadas las circunstancias específicas de la transferencia, así como las limitaciones y garantías aplicables (12);
   (iii) las garantías contractuales, técnicas u organizativas pertinentes aportadas para complementar las garantías previstas en el presente pliego de cláusulas, especialmente incluidas las medidas aplicadas durante la transferencia y el tratamiento de los datos personales en el país de destino.

(c) El importador de datos asegura que, al llevar a cabo la valoración a que se refiere la letra b), ha hecho todo lo posible por proporcionar al exportador de datos la información pertinente y se compromete a seguir colaborando con el exportador de datos para garantizar el cumplimiento del presente pliego de cláusulas.

(d) Las partes acuerdan documentar la evaluación a que se refiere la letra b) y ponerla a disposición de la autoridad de control competente previa solicitud.

(e) El importador de datos se compromete a notificar con presteza al exportador de datos si, tras haberse vinculado por el presente pliego de cláusulas y durante el período de vigencia del contrato, tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la letra a), incluso a raíz de un cambio de la normativa en el tercer país o de una medida (como una solicitud de comunicación) que indique una aplicación de dicha normativa en la práctica que no se ajuste a los requisitos de la letra a).

(f) De realizarse la notificación a que se refiere la letra e) o si el exportador de datos tiene motivos para creer que el importador de datos ya no puede cumplir las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos determinará con presteza las medidas adecuadas (por ejemplo, medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad) que deberán adoptar el exportador de datos y/o el importador de datos para poner remedio a la situación. El exportador de datos suspenderá la transferencia de los datos si considera que no hay garantías adecuadas o si así lo dispone la autoridad de control competente. En este supuesto, el exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa. En caso de resolución del contrato en virtud de la presente cláusula, será de aplicación la cláusula 16, letras d) y e).

---

(12) Por lo que se refiere al efecto de dicho Derecho y prácticas en el cumplimiento del presente pliego de cláusulas, a la hora de realizar una valoración integral de esta cuestión pueden tenerse en cuenta distintos aspectos. Uno de estos aspectos puede ser que haya experiencia práctica pertinente y documentada en casos anteriores de solicitudes de comunicación por parte de las autoridades públicas, o la ausencia de tales solicitudes, en un período suficientemente representativo. Con esto se quiere decir, en particular, los registros internos u otra documentación elaborados de forma continua con la diligencia debida y certificados en los niveles más altos de la dirección siempre que esta información pueda compartirse legalmente con terceros. Cuando se use esta experiencia práctica para llegar a la conclusión de que el importador de datos no tendrá impedimento para cumplir el presente pliego de cláusulas, deberá estar respaldada por otros elementos pertinentes y objetivos; corresponde a las partes valorar minuciosamente si la suma de estos factores es suficientemente determinante, en términos de fiabilidad y representatividad, para respaldar esta conclusión. En particular, las partes deben tener en cuenta si su experiencia práctica está corroborada y no se ve desmentida, por información que sea fiable y de dominio público o accesible de cualquier otro modo acerca de la existencia o ausencia de solicitudes en el mismo sector o acerca de la aplicación de la normativa de que se trate en la práctica, como jurisprudencia e informes de organismos de supervisión independientes.

Cláusula 15

Obligaciones del importador de datos en caso de acceso por parte de las autoridades públicas

15.1 **Notificación**

(a) El importador de datos se compromete a notificar con presteza al exportador de datos y, cuando sea posible, al interesado (de ser necesario, con la ayuda del exportador de datos) si:

(i) recibe una solicitud jurídicamente vinculante de comunicación de datos personales transferidos con arreglo al presente pliego de cláusulas presentada por una autoridad pública (sobre todo, judicial) en virtud del Derecho del país de destino; dicha notificación contendrá información sobre los datos personales solicitados, la autoridad solicitante, la base jurídica de la solicitud y la respuesta dada; o

(ii) tiene conocimiento de que las autoridades públicas han tenido acceso directo a los datos personales transferidos con arreglo al presente pliego de cláusulas en virtud del Derecho del país de destino; dicha notificación incluirá toda la información de que disponga el importador de datos.

(b) Si se prohíbe al importador de datos enviar la notificación al exportador de datos y/o al interesado en virtud del Derecho del país de destino, el importador de datos se compromete a hacer todo lo posible para obtener una dispensa de la prohibición, con el fin de comunicar toda la información disponible y lo antes posible. El

importador de datos se compromete a documentar las actuaciones que realice a tal fin para poder justificar su diligencia si se lo pide el exportador de datos.

(c) En la medida en que lo permita el Derecho del país de destino, el importador de datos se compromete a proporcionar al exportador de datos, a intervalos regulares durante el período de vigencia del contrato, la mayor cantidad posible de información pertinente sobre las solicitudes recibidas (en particular, el número de solicitudes, el tipo de datos solicitados, la autoridad o autoridades solicitantes, la impugnación de las solicitudes, el resultado de tales impugnaciones, etc.).

(d) El importador de datos se compromete a conservar la información a que se refieren las letras a) a c) durante el período de vigencia del contrato y a ponerla a disposición de la autoridad de control competente previa solicitud.

(e) Las letras a) a c) se entenderán sin perjuicio de la obligación del importador de datos, contemplada en la cláusula 14, letra e), y en la cláusula 16, de informar con presteza al exportador de datos cuando no pueda dar cumplimiento al presente pliego de cláusulas.

15.2 **Control de la legalidad y minimización de datos**

(a) El importador de datos se compromete a controlar la legalidad de la solicitud de comunicación y, en particular, si la autoridad pública solicitante está debidamente facultada para ello, así como a impugnar la solicitud si, tras una valoración minuciosa, llega a la conclusión de que existen motivos razonables para considerar que la solicitud es ilícita con arreglo al Derecho del país de destino, incluidas las obligaciones aplicables en virtud del Derecho internacional y los principios de cortesía internacional. El importador de datos agotará, en las mismas condiciones, las vías de recurso. Al impugnar una solicitud, el importador de datos instará la aplicación de medidas cautelares para suspender los efectos de la solicitud hasta que la autoridad judicial competente se haya pronunciado sobre el fondo. No comunicará los datos personales solicitados hasta que se lo exija la normativa procesal aplicable. Estos requisitos se entienden sin perjuicio de las obligaciones que la cláusula 14, letra e), atribuye al importador de datos.

(b) El importador de datos se compromete a documentar sus valoraciones jurídicas y las impugnaciones de solicitudes de comunicación y a poner dicha documentación a disposición del exportador de datos en la medida en que lo permita el Derecho del país de destino. También pondrá dicha documentación a disposición de la autoridad de control competente previa solicitud.

(c) El importador de datos se compromete a proporcionar la mínima información posible al responder a las solicitudes de comunicación, basándose en una interpretación razonable de la solicitud.

SECCIÓN IV: DISPOSICIONES FINALES

Cláusula 16

Incumplimiento de las cláusulas y resolución del contrato

(a) El importador de datos informará con presteza al exportador de datos en caso de que no pueda dar cumplimiento al presente pliego de cláusulas por cualquier motivo.

(b) En caso de que el importador de datos incumpla las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos suspenderá la transferencia de datos personales al importador de datos hasta que se vuelva a garantizar el cumplimiento o se resuelva el contrato. Lo anterior se entiende sin perjuicio de la cláusula 14, letra f).

(c) El exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando:

(i) el exportador de datos haya suspendido la transferencia de datos personales al importador de datos con arreglo a la letra b) y no se vuelva a dar cumplimiento al presente pliego de cláusulas en un plazo razonable y, en cualquier caso, en un plazo de un mes a contar desde la suspensión;

(ii) el importador de datos vulnere de manera sustancial o persistente el presente pliego de cláusulas; o

(iii) el importador de datos incumpla una resolución vinculante de un órgano jurisdiccional o autoridad de control competente en relación con las obligaciones que le atribuye el presente pliego de cláusulas.

En este supuesto, informará a la autoridad de supervisión competente de su incumplimiento. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa.

(d) Los datos personales que se hayan transferido antes de la resolución del contrato con arreglo a la letra c) deberán, a elección del exportador de datos, devolverse inmediatamente al exportador de datos o destruirse en su totalidad. Lo mismo será de aplicación a las copias de los datos. El importador de datos acreditará la destrucción de los datos al exportador de datos. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales transferidos, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país.

(e) Ninguna de las partes podrá revocar su consentimiento a quedar vinculada por el presente pliego de cláusulas si:i) la Comisión Europea adopta una decisión de conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679 que regule la transferencia de datos personales a los que se aplique el presente pliego de cláusulas; o ii) el Reglamento (UE) 2016/679 pasa a formar parte del ordenamiento jurídico del país al que se transfieren los datos personales. Ello se entiende sin perjuicio de otras responsabilidades que sean de aplicación al tratamiento en cuestión en virtud del Reglamento (UE) 2016/679.

Cláusula 17

Derecho aplicable

El presente pliego de cláusulas se regirá por el Derecho de uno de los Estados miembros de la Unión Europea, siempre que dicho Derecho admita la existencia de derechos de los terceros beneficiarios. Las Partes acuerdan que se tratará de: a) el Derecho del país especificado en el Acuerdo de Servicios, en caso de que este se rija por el Derecho de un Estado miembro de la UE, o b) el Derecho del Reino de los Países Bajos en caso de que el Acuerdo de Servicios se rija por el Derecho de un tercer país.

Cláusula 18
Elección del foro y jurisdicción

Cualquier controversia derivada del presente pliego de cláusulas será resuelta judicialmente en un Estado miembro de la Unión Europea.

(a) Las partes acuerdan que se tratará de los tribunales i) indicados en el Acuerdo de Servicios, en caso de que este designe un tribunal ubicado en un Estado miembro de la UE, o ii) los tribunales de Ámsterdam, en caso de que el Acuerdo de Servicios designe un tribunal ubicado en un tercer país.

(b) Los interesados también podrán ejercer acciones judiciales contra el exportador de datos y/o el importador de datos en el Estado miembro en el que el interesado tenga su residencia habitual.

(c) Las partes acuerdan someterse a la jurisdicción de dicho Estado miembro.

NOTA ACLARATORIA:

APÉNDICE

Se debe poder distinguir claramente la información aplicable a cada transferencia o categoría de transferencias y, por tanto, determinar la función o funciones respectivas de las partes en cuanto exportador(as) de datos y/o importador(as) de datos. No es imprescindible cumplimentar y firmar apéndices separados por cada transferencia o categoría de transferencias y/o relación contractual si se puede lograr un nivel de transparencia equivalente cumplimentando un solo apéndice. No obstante, cuando sea necesario para garantizar claridad suficiente, deben utilizarse apéndices separados.

ANEXO I

A. **LISTA DE PARTES**

Exportador(es) de datos: La página 1 del presente ATD identifica al exportador de datos como el responsable.

Importador(es) de datos: El importador de datos es Proofpoint, Inc., un proveedor de servicios de seguridad de correo electrónico y medios sociales, análisis de amenazas y formación en materia de seguridad.

B. **DESCRIPCIÓN DE LA TRANSFERENCIA**

Los **interesados** son los empleados y contratistas del Responsable, así como los empleados y contratistas de los clientes y proveedores del Responsable

Categorías de datos: Las categorías de datos se identifican en el Apéndice 1 al presente ATD. El responsable no transferirá datos sensibles a Proofpoint.

Operaciones de tratamiento: La frecuencia de la transferencia, la naturaleza y la finalidad del tratamiento y el período de retención se identifican en el Apéndice 1 al presente ATD.

C. **AUTORIDAD DE CONTROL COMPETENTE Indíquese la autoridad o autoridades de control competentes de conformidad con la *Cláusula 13***

[Cuando el exportador de datos esté establecido en un Estado miembro de la UE:] La autoridad de control competente en el Estado miembro del domicilio social del exportador de datos.

[Cuando el exportador de datos no esté establecido en un Estado miembro de la UE, pero entre en el ámbito territorial de aplicación del Reglamento (UE) 2016/679 de conformidad con su artículo 3, apartado 2, y haya designado un representante de conformidad con el artículo 27, apartado 1, del Reglamento (UE) 2016/679:] La autoridad de control competente en el Estado miembro del domicilio social del exportador de datos.

[Cuando exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679, de conformidad con el artículo 3, apartado 2, sin tener no obstante que designar a un representante con arreglo al artículo 27, apartado 2, del Reglamento (UE) 2016/679]: la autoridad de control de los Países Bajos

ANEXO II

MEDIDAS TÉCNICAS Y ORGANIZATIVAS, EN ESPECIAL MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

Las medidas de seguridad, técnicas y organizativas se describen en el Apéndice 2 al presente ATD.

ANEXO III

LISTA DE SUBENCARGADOS

La lista actual de subencargados para el servicio está disponible en la página web Trust Site de Proofpoint en la dirección: https://www.proofpoint.com/us/legal/trust