

Requisitos de Protección de Datos para proveedores de Microsoft

Aplicabilidad

Los Requisitos de Protección de Datos (“DPR”, por sus siglas en inglés) para proveedores de Microsoft se aplican a cada proveedor de Microsoft que Trate Datos Personales o Datos Confidenciales de Microsoft en relación con la actividad de dicho proveedor (por ejemplo, prestación de servicios, licencias de software, servicios en la nube) en virtud de los términos de su contrato con Microsoft (por ejemplo, términos de la orden de compra, contrato marco, SOW) (la “Actividad”, las “Actividades” o la “Realización de la Actividad”).

- En caso de conflicto entre los DPR y los requisitos que se especifican en los acuerdos contractuales celebrados entre el proveedor y Microsoft, los DPR prevalecerán, a menos que el proveedor identifique en el contrato la disposición correcta que sustituya el requisito de protección de datos aplicables (en cuyo caso, los términos del contrato prevalecerán).
- Si hubiera algún conflicto entre los requisitos que se incluyen en el presente y cualquier requisito legal o reglamentario, estos últimos prevalecerán.
- En caso de que el proveedor de Microsoft opere como Responsable del Tratamiento de los Datos, se le podrían reducir los requisitos en los DPR.
- En caso de que el proveedor de Microsoft no Trate Datos Personales de Microsoft, sino únicamente Datos Confidenciales de Microsoft, con respecto a estos DPR, se le podrían reducir los requisitos.

Transferencia internacional de datos

Sin limitar el resto de sus obligaciones, el proveedor no realizará ninguna transferencia internacional de Datos Personales de Microsoft a menos que Microsoft lo haya autorizado previamente por escrito y, en todo caso, el proveedor deberá cumplir con los Requisitos de Protección de Datos, incluidas las Cláusulas Contractuales o, a discreción de Microsoft, otros mecanismos adecuados de transferencia transfronteriza aprobados por la autoridad de protección de datos competente o por la Comisión Europea, según corresponda, y adoptados o aceptados por Microsoft. Las Cláusulas Contractuales que en el futuro adopten (i) la Comisión Europea o el Supervisor Europeo de Protección de Datos y que sean aprobadas por la Comisión Europea, (ii) el Reino Unido de conformidad con la Ley Federal General de Protección de Datos del Reino Unido, (iii) Suiza, de conformidad con la Ley Federal de Protección de Datos de Suiza, o (iv) las cláusulas que rigen la transferencia internacional de datos personales adoptadas oficialmente por el gobierno de una jurisdicción distinta de Suiza, el Reino Unido y las jurisdicciones que comprenden la Unión Europea o el Espacio Económico Europeo, se incorporarán y serán vinculantes para el proveedor a partir del día de su adopción. Asimismo, el proveedor deberá garantizar que todos y cada uno de los Subencargados del Tratamiento (tal y como se definen en las Cláusulas Contractuales) también cumplan con estas disposiciones.

Definiciones clave

Los siguientes términos utilizados en estos DPR tienen el significado que se indica a continuación. Se interpreta que las listas de ejemplos que siguen a los términos “incluido/a(s)”, “como”, “por ejemplo” o similares utilizados a lo largo de estos DPR incluyen “de manera enunciativa mas no limitativa” o “entre otros”, a menos que se califiquen con palabras como “solamente” o “únicamente”. Para más definiciones, consulte el Glosario que se encuentra al final del presente documento.

“**Responsable del Tratamiento**” significa la entidad que determina los fines y los medios del Tratamiento de los Datos Personales. “**Responsable del Tratamiento**” se refiere a una Empresa, al Responsable del Tratamiento (tal y como se

define este término en el RGPD) y a términos equivalentes que se encuentran en las Leyes de Protección de Datos, según lo requiera el contexto.

Las **“Cookies”** son pequeños archivos de texto almacenados en los dispositivos electrónicos por los sitios web y/o las aplicaciones que contienen información utilizada para reconocer a una Persona Interesada o a un dispositivo.

“Incidente de Datos” se refiere a (1) una violación de la seguridad que provoque, de manera accidental o legal, la destrucción, la pérdida, la alteración, la divulgación no autorizada o el acceso a los Datos Personales de Microsoft o a los Datos Confidenciales de Microsoft transmitidos, almacenados o Tratados de alguna otra manera por el Proveedor o sus Subcontratistas, o (2) una vulnerabilidad de seguridad relacionada con el manejo de los Datos Personales de Microsoft o los Datos Confidenciales de Microsoft por parte del Proveedor.

“Persona Interesada” es una persona física identificable que se puede identificar, ya sea directa o indirectamente, en particular, haciendo referencia a un elemento de identificación, como un nombre, un número de identificación, datos de localización, un identificador en línea, o a uno o más aspectos específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física.

“Derecho de la Persona Interesada” significa el derecho de la Persona Interesada a acceder, eliminar, editar, exportar, restringir u oponerse al Tratamiento de los Datos Personales de Microsoft de dicha Persona Interesada, si así lo exigiera la Legislación.

“Legislación” significa todas las leyes, normas, estatutos, decretos, decisiones, órdenes, reglamentos, sentencias, códigos, promulgaciones, resoluciones y requisitos aplicables de cualquier autoridad de gobierno (ya sea federal, estatal, local o internacional) que tenga jurisdicción. El término **“legal”** se refiere a cualquier violación de la Legislación.

“Datos Confidenciales de Microsoft” se refiere a toda información que, de ponerse en riesgo su confidencialidad o integridad de la manera que fuere, puede suponer una pérdida considerable para Microsoft en términos financieros o de reputación. Esto incluye productos de hardware y software de Microsoft, aplicaciones internas de línea de negocio, materiales de comercialización previos al lanzamiento, claves de licencia de productos y documentación técnica relacionada con los productos y servicios de Microsoft.

“Datos Personales de Microsoft” significa cualquier Dato personal Tratado por Microsoft o en su nombre.

“Datos Personales” se refiere a toda información relativa a una Persona Interesada y cualquier otra información que constituya “datos personales” o “información personal” de conformidad con la Legislación.

“Tratamiento” significa cualquier operación o conjunto de operaciones que se realicen sobre Datos Personales o Datos Confidenciales de Microsoft, ya sea de manera automatizada o de cualquier otro modo, como la recopilación, el registro, la grabación, la organización, la estructuración, el almacenamiento, la adaptación o alteración, la recuperación, la consulta, el uso, la divulgación por transmisión, la difusión o puesta a disposición de cualquier otro modo, la alineación o combinación, la restricción, la eliminación o la destrucción. Los términos “Trato”, “Tratar” y “Tratado” tendrán los significados correspondientes.

“Encargado del Tratamiento” significa una entidad que Trata Datos Personales en nombre de otra entidad e incluye al Proveedor de Servicios, al Encargado del Tratamiento (tal como se define ese término en el RGPD) y a términos equivalentes que se encuentran en las Leyes de Protección de Datos, según lo requiera el contexto.

“Subcontratista” significa un tercero al cual el proveedor delega sus obligaciones en relación con el contrato que ampara su Actividad, incluida cualquier filial del proveedor que no haya celebrado un contrato directamente con Microsoft.

“**Subencargado del Tratamiento**” se refiere a un tercero que Microsoft contrata para la Realización de la Actividad en los casos en los que la Actividad incluye el Tratamiento de los Datos Personales de Microsoft para los cuales Microsoft es el Encargado del Tratamiento.

Respuesta del proveedor

Los proveedores anualmente confirmaran el cumplimiento de estos requisitos mediante un servicio en línea administrado por Microsoft. Consulte la [Guía del programa de la SSPA](#) para entender cómo se administra el cumplimiento.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
---	---	--------------------------

Sección A: Administración

1	<p>Cada contrato aplicable entre Microsoft y el proveedor (por ejemplo, contrato marco, declaración de trabajo, órdenes de compra y otros pedidos) contiene lenguaje de protección de datos de privacidad y seguridad con respecto a los Datos Confidenciales y Personales de Microsoft, según corresponda, incluidas las prohibiciones sobre la venta de Datos Personales de Microsoft y el Tratamiento de Datos Personales de Microsoft fuera de la relación comercial directa entre Microsoft y el proveedor.</p> <p>En el caso de las empresas que operan como Encargados o Subencargados del Tratamiento, con respecto a los Datos Personales de Microsoft, el contrato debe incluir el objeto y la duración del Tratamiento, la naturaleza y la finalidad del mismo, el tipo de Datos Personales de Microsoft y las categorías de Personas Interesadas, así como las obligaciones y los derechos de Microsoft.</p>	<p>El proveedor debe presentar el contrato aplicable entre Microsoft y el proveedor.</p> <p>En el caso de los Encargados y Subencargados del Tratamiento, las descripciones del Tratamiento se incluyen en el contrato aplicable (por ejemplo, declaración de trabajo, órdenes de compra).</p> <p>Nota: Las empresas que tengan órdenes de compra en proceso pueden solicitar que la descripción necesaria de las actividades de Tratamiento se agreguen más tarde en el proceso de compra.</p>
2	<p>Cuando Microsoft confirme que sus compromisos cumplen una función de Subencargado del Tratamiento, el proveedor debe contar con contratos de protección de datos aplicables celebrados con Microsoft.</p> <p>Nota: Microsoft publicará esta designación en su perfil cuando esto aplique.</p>	<p>Cláusulas Contractuales, Adenda de Datos de Clientes en Línea y/o Adenda de Tratamiento de Datos de Servicios Profesionales del Proveedor o Socio.</p>
3	<p>Asignar la responsabilidad y la obligación de rendir cuentas sobre el cumplimiento de los DPR a una persona o grupo designado dentro de la empresa.</p>	<p>Indicar la función de la persona o el grupo encargado de garantizar el cumplimiento de los DPR para proveedores de Microsoft.</p> <p>Un documento que describa la autoridad y la obligación de rendir cuentas de esta persona o grupo que demuestre una función de privacidad y/o seguridad.</p>
4	<p>Establecer, mantener y llevar a cabo una capacitación anual sobre privacidad y seguridad para los empleados que tendrán acceso a los Datos Personales Tratados por el proveedor en relación con la Realización de la Actividad o los Datos Confidenciales de Microsoft.</p> <p>Si su empresa no tiene contenido preparado, puede utilizar este esquema y adaptarlo a su empresa.</p> <p>Nota: Es posible que el personal de los proveedores deba realizar cursos adicionales de capacitación impartidos por las divisiones de Microsoft.</p>	<p>Los registros anuales de asistencia están disponibles y pueden proporcionarse a Microsoft si lo solicita.</p> <p>El contenido de la capacitación incluye principios de privacidad y seguridad.</p> <p>La documentación del cumplimiento de los requisitos de capacitación incluirá pruebas de la capacitación relacionada con los requisitos reglamentarios de privacidad, las obligaciones de seguridad y el cumplimiento de los requisitos y las obligaciones contractuales aplicables.</p>

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
---	---	--------------------------

Sección A: Administración (continuación)

5	<p>Tratar los Datos Personales de Microsoft únicamente de acuerdo con las instrucciones documentadas por Microsoft, incluyendo los escenarios con respecto a las transferencias de Datos Personales de Microsoft a un tercer país o a una organización internacional, a menos que lo exija la Legislación; en tal caso, el Encargado del Tratamiento o el Subencargado del Tratamiento (proveedor) informará al responsable del tratamiento (Microsoft) dicho requisito legal antes del Tratamiento, a menos que dicha Legislación prohíba dicha información por motivos importantes de interés público.</p>	<p>El proveedor recopila y mantiene todas las instrucciones documentadas por Microsoft (por ejemplo, el acuerdo, la declaración de trabajo o la documentación del pedido) de forma electrónica, en un lugar fácilmente accesible para los empleados y contratistas del proveedor que participan en la Realización de la Actividad.</p>
---	--	--

Sección B: Aviso

6	<p>El proveedor debe utilizar la Declaración de Privacidad de Microsoft cuando recopile Datos Personales en nombre de Microsoft.</p> <p>El aviso de privacidad debe ser obvio y estar disponible para las Personas Interesadas para ayudarlas a decidir si presentan sus Datos Personales al proveedor.</p> <p>Nota: Si su empresa es el Responsable del Tratamiento, deberá publicar su propio aviso de privacidad.</p>	<p>El proveedor utiliza un fwmlink para la Declaración de Privacidad de Microsoft publicada actualmente.</p> <p>La Declaración de Privacidad se publica en cualquier contexto en el que se recopilan los Datos Personales de un usuario.</p> <p>Si corresponde, existe una versión sin conexión que se facilita antes de la recopilación de datos.</p> <p>Toda Declaración de Privacidad sin conexión utilizada es la versión publicada más reciente y está debidamente fechada. Para los servicios de los empleados de Microsoft, se utiliza el Aviso de Privacidad de Datos de Microsoft.</p>
7	<p>Cuando se recopilen Datos Personales de Microsoft a través de una llamada de voz en directo o grabada, los proveedores deben estar preparados para comentar las prácticas de recopilación, tratamiento, uso y conservación de datos aplicables con las Personas Interesadas.</p>	<p>Una secuencia de datos para grabaciones de voz incluye cómo se Tratan los Datos Personales de Microsoft e incluye:</p> <ul style="list-style-type: none"> ▪ recopilación, ▪ uso y ▪ conservación

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
Sección C: Elección y consentimiento		
8	<p>Cuando corresponda, el proveedor debe obtener y registrar el consentimiento de la Persona Interesada para todas sus actividades de Tratamiento (incluida cualquier actividad de Tratamiento nueva y actualizada) antes de recopilar los Datos Personales de dicha Persona Interesada.</p> <p>El proveedor monitorea la eficacia de la gestión de las preferencias para garantizar que el plazo para cumplir con algún cambio de preferencia sea el más restrictivo de los requisitos legales locales que se aplican.</p>	<p>El proveedor puede demostrar cómo una Persona Interesada da su consentimiento para una actividad de Tratamiento y que el alcance del consentimiento ampara todas las actividades de Tratamiento del proveedor con respecto a los Datos Personales de dicha Persona Interesada.</p> <p>El proveedor puede demostrar cómo una Persona Interesada retira su consentimiento para una actividad de Tratamiento.</p> <p>El proveedor puede demostrar cómo se comprueban las preferencias antes de iniciar una nueva actividad de Tratamiento.</p> <p>Nota: Las pruebas pueden ser capturas de pantalla de la interacción con el usuario, la experiencia con el servicio o la oportunidad de ver la documentación técnica.</p>
9	<p>Los proveedores que crean y gestionan sitios web y/o aplicaciones de Microsoft o sitios que llevan la marca de Microsoft deben proporcionar a las Personas Interesadas un aviso transparente y la posibilidad de elegir sobre el uso de las cookies de acuerdo con los compromisos de la Declaración de Privacidad de Microsoft y los requisitos legales locales.</p> <p>A menos que la unidad de negocio contratante lo solicite específicamente, los proveedores deben utilizar el Banner estándar elaborado por 1ES para gestionar los controles de elección.</p> <p>Este requisito se aplica cuando los sitios se dirigen a usuarios dentro de la Unión Europea o el Espacio Económico Europeo y otras regiones con leyes de privacidad aplicables y siempre que se utilice la Declaración de Privacidad de Microsoft.</p> <p>Nota: Los patrocinadores comerciales de Microsoft deben registrar los sitios web de Microsoft en el portal interno de Cumplimiento web (http://aka.ms/wcp) para tener el inventario de cookies catalogado y administrado.</p>	<p>El propósito de cada cookie debe estar documentado y debe informar el tipo de <i>cookie</i> implementado.</p> <ul style="list-style-type: none"> ▪ Las cookies persistentes no deben utilizarse cuando las cookies de sesión son suficientes. ▪ Cuando se utilizan cookies persistentes, estas no deben tener una fecha de caducidad superior a 13 meses después de que el usuario haya visitado el sitio. <p>Validar el cumplimiento de las leyes de la UE según corresponda, como:</p> <ul style="list-style-type: none"> ▪ uso de la convención de etiquetado, “Privacidad y Cookies” para la declaración de privacidad, ▪ obtener el consentimiento afirmativo del usuario antes de utilizar cookies “no esenciales” para fines como la publicidad, y ▪ el consentimiento debe caducar o volver a obtenerse a más tardar cada 6 meses.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
Sección D: Recopilación		
10	El proveedor deberá supervisar la recopilación de Datos Personales y/o Confidenciales de Microsoft para garantizar que los únicos datos recopilados sean los necesarios para la Realización de la Actividad.	<p>El proveedor puede proporcionar documentación que demuestre que los Datos Personales y/o Confidenciales de Microsoft recopilados son necesarios para la Realización de la Actividad.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>
11	Antes de recopilar datos de niños (según la definición de la jurisdicción aplicable), el proveedor debe obtener el consentimiento según las leyes locales de privacidad.	<p>El proveedor puede aportar documentación que demuestre el consentimiento de los padres o tutores.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>
Sección E: Conservación		
12	Garantizar que los Datos Personales y Confidenciales de Microsoft no se conservan durante más tiempo del necesario para la Realización de la Actividad, a menos que la ley exija la conservación continuada de los Datos Personales y/o Confidenciales de Microsoft.	<p>El proveedor cumple con las políticas de conservación documentadas o los requisitos de conservación especificados por Microsoft en el contrato (por ejemplo, declaración de trabajo, orden de compra).</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>
13	<p>Garantizar que, a discreción de Microsoft, los Datos Personales y Confidenciales de Microsoft que estén en posesión del proveedor o bajo su control se devuelvan a Microsoft o se destruyan al finalizar la Realización de la Actividad o a petición de Microsoft.</p> <p>Dentro de las aplicaciones, deben existir procesos que garanticen que, cuando los datos sean eliminados de la aplicación, ya sea explícitamente por los usuarios o en función de otros factores desencadenantes, como la antigüedad de los datos, se eliminen de forma segura.</p> <p>Cuando sea necesaria la destrucción de Datos Personales o Confidenciales de Microsoft, el proveedor deberá quemar, pulverizar o triturar los activos físicos que contengan Datos Personales y/o Confidenciales de Microsoft de forma que la información no pueda ser leída o reconstruida.</p>	<p>Mantener un registro de la disposición de los Datos Personales y Confidenciales de Microsoft (esto puede incluir la devolución a Microsoft para su destrucción).</p> <p>Si Microsoft exige o solicita la destrucción, proporcione un certificado de destrucción firmado por un funcionario del proveedor.</p>

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
Sección F: Personas Interesadas		
	<p>Las Personas Interesadas tienen ciertos derechos conforme a la ley, incluido el derecho a acceder, eliminar, editar, exportar, restringir y oponerse al tratamiento de sus Datos Personales (“Derechos de las Personas Interesadas”). Cuando una Persona Interesada busca ejercer sus derechos en virtud de la Legislación con respecto a sus Datos Personales de Microsoft, el proveedor debe permitir a Microsoft hacer lo siguiente o realizar estas acciones en nombre de Microsoft:</p>	
14	<p>Ayudar a Microsoft, a través de medidas técnicas y organizativas apropiadas, cuando sea posible, a cumplir con sus obligaciones de responder a las solicitudes de las Personas Interesadas que buscan ejercer sus Derechos de las Personas Interesadas sin demoras indebidas.</p> <p>A menos que Microsoft indique lo contrario, el proveedor remitirá a todas las Personas Interesadas que se pongan en contacto con el proveedor directamente a Microsoft para que ejerzan los Derechos de las Personas Interesadas.</p>	<p>El proveedor mantendrá pruebas de los procesos y procedimientos documentados para respaldar la ejecución de los Derechos de las Personas Interesadas.</p> <p>El proveedor mantendrá pruebas documentadas de las pruebas. Las pruebas estarán disponibles a petición de Microsoft.</p>
15	<p>Cuando se responde directamente a la Persona Interesada o cuando el proveedor proporciona un mecanismo de autoservicio en línea, el proveedor cuenta con procesos y procedimientos para identificar a la Persona Interesada que realiza la solicitud.</p>	<p>El proveedor ha documentado el método utilizado para identificar a las Personas Interesadas de Microsoft.</p> <p>El proveedor proporcionará pruebas documentadas a Microsoft cuando se le solicite.</p>
16	<p>Si Microsoft le pide que localice Datos Personales de Microsoft sobre una Persona Interesada que no están disponibles a través de un mecanismo de autoservicio en línea, el proveedor hará un esfuerzo razonable para localizar los datos solicitados y mantendrá registros suficientes para demostrar que se hizo una búsqueda razonable.</p>	<p>El proveedor mantendrá pruebas documentadas de los procedimientos implementados para determinar si se conservan los Datos Personales de Microsoft y proporcionará la documentación a Microsoft si esta lo solicita.</p> <p>El proveedor mantiene un registro que demuestra las medidas adoptadas para satisfacer las solicitudes de Derechos de las Personas Interesadas.</p> <p>La documentación incluye:</p> <ul style="list-style-type: none"> ▪ fecha y hora de la solicitud, ▪ las medidas adoptadas para responder a la solicitud y el registro de cuándo se le informó a Microsoft. <p>El proveedor proporcionará a Microsoft pruebas de la conservación de los registros cuando se le solicite.</p>

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
Sección F: Personas Interesadas (continuación)		
17	El proveedor comunicará a las Persona Interesada los pasos que debe dar para acceder a sus Datos Personales de Microsoft o para ejercer sus derechos con respecto a sus datos.	El proveedor mantendrá pruebas documentadas de las comunicaciones y procedimientos de acceso a los Datos Personales de Microsoft. El proveedor mantendrá pruebas documentadas y proporcionará dichas pruebas a Microsoft cuando se le solicite.
18	<p>Registrar la fecha y la hora de las solicitudes de Derechos de las Personas Interesadas y las medidas adoptadas por el proveedor en respuesta a dichas solicitudes.</p> <p>Si su solicitud es denegada, a instancias de Microsoft, proporcionar a la Persona Interesada una explicación por escrito.</p> <p>Proporcionar los registros de las solicitudes de las Personas Interesadas a Microsoft cuando lo solicite.</p>	<p>El proveedor mantiene registros de las solicitudes de acceso/borrado y documenta los cambios realizados en los Datos Personales de Microsoft.</p> <p>Documentar los casos en los que se deniegan las solicitudes y conservar las pruebas de la revisión y aprobación de Microsoft.</p> <p>El proveedor proporcionará pruebas de la conservación de registros de solicitudes y denegaciones de acceso a los Datos Personales de Microsoft.</p>
19	El proveedor debe permitir a Microsoft u obtener una copia de los Datos Personales de Microsoft solicitados para la Persona Interesada autenticada en un formato apropiado impreso, electrónico o verbal.	El proveedor suministra los Datos Personales de Microsoft a la Persona Interesada en un formato comprensible y en una forma conveniente para la Persona Interesada y el proveedor.
20	El proveedor debe tomar precauciones razonables para garantizar que los Datos Personales de Microsoft entregados a Microsoft o a una Persona Interesada autenticada no puedan ser utilizados para identificar a otra persona.	El proveedor mantendrá pruebas documentadas de los procedimientos relacionados con las precauciones para evitar la identificación de la Persona Interesada en contra de los términos del contrato. El proveedor proporcionará las pruebas a Microsoft cuando se le solicite.
21	Si una Persona Interesada cree que sus Datos Personales de Microsoft no están completos y no son precisos, el proveedor debe elevar el problema a Microsoft y cooperar con Microsoft según sea necesario para resolver el problema.	<p>El proveedor documenta los casos de desacuerdo y eleva la cuestión a Microsoft.</p> <p>El proveedor proporcionará a Microsoft las pruebas documentales cuando se le solicite.</p>

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
Sección G: Subcontratistas		
	Si el proveedor pretende utilizar a un Subcontratista para el Tratamiento de los Datos Personales o Confidenciales de Microsoft, deberá:	
22	<p>Notificar a Microsoft antes de subcontratar servicios o realizar cualquier cambio relativo a la adición o sustitución de subcontratistas.</p> <p>Nota: Indique su aceptación de esta obligación, aunque no contrate actualmente a subcontratistas pero pueda hacerlo en el futuro.</p>	<p>Validar que los Datos Personales de Microsoft sean Tratados únicamente por empresas conocidas por Microsoft, tal y como se requiere en el contrato aplicable (por ejemplo, declaración de trabajo, adenda, orden de compra) o capturados en la base de datos de la SSPA. El proveedor puede publicar su lista de subcontratistas en línea e incluir un enlace a la página en la base de datos de la SSPA.</p>
23	<p>Documentar la naturaleza y el alcance de los Datos Personales y Confidenciales de Microsoft subtratados por los Subcontratistas, garantizando que la información recopilada sea necesaria para la Realización de la Actividad.</p>	<p>El proveedor mantiene la documentación relativa a los Datos Personales y Confidenciales de Microsoft divulgados o transferidos a los subcontratistas.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>
24	<p>Cuando Microsoft sea el Responsable del Tratamiento de los Datos Personales de Microsoft, garantizar que el subcontratista utilice los Datos Personales de Microsoft de acuerdo con las preferencias de contacto indicadas de la Persona Interesada.</p>	<p>Demostrar cómo los subcontratistas utilizan la preferencia de la Persona Interesada de Microsoft.</p> <p>Proporcionar documentación de apoyo (por ejemplo, captura de pantalla, SLA, SOW, etc.) que incluya el plazo para que un subcontratista cumpla con un cambio de preferencia.</p>
25	<p>Limitar el Tratamiento de los Datos Personales o Confidenciales de Microsoft por parte del subcontratista para los fines necesarios para cumplir el contrato del proveedor con Microsoft.</p>	<p>El proveedor puede proporcionar documentación que demuestre que los Datos Personales de Microsoft proporcionados a un subcontratista son necesarios para la Realización de la Actividad.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>
26	<p>Revisar las reclamaciones en busca de indicios de cualquier Tratamiento no autorizado o ilegal de los Datos Personales de Microsoft.</p>	<p>El proveedor puede demostrar que dispone de sistemas y procesos para atender las reclamaciones relativas al uso o divulgación no autorizados de los Datos Personales de Microsoft por parte de un subcontratista.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
---	---	--------------------------

Sección G: Subcontratistas (continuación)

27	Notificar a Microsoft de inmediato al enterarse de que un subcontratista ha Tratado Datos Personales o Confidenciales de Microsoft para cualquier propósito que no esté relacionado con la Realización de la Actividad.	<p>El proveedor ha proporcionado las instrucciones y los medios para que un subcontratista informe el uso indebido de los datos de Microsoft.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>
28	Si el proveedor recopila Datos Personales de terceros en nombre de Microsoft, deberá validar que las políticas y prácticas de protección de datos de terceros son coherentes con el contrato del proveedor con Microsoft y los DPR.	<p>El proveedor puede proporcionar la documentación de la diligencia debida realizada en relación con las políticas y prácticas de protección de datos del tercero.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>
29	Adoptar de inmediato medidas para mitigar cualquier daño real o potencial causado por el Tratamiento no autorizado o ilegal de los Datos Personales y Confidenciales de Microsoft por parte de un subcontratista.	El proveedor debe mantener pruebas documentales del plan y del procedimiento y proporcionar pruebas de la documentación a Microsoft cuando se le solicite.

Sección H: Calidad

30	El proveedor debe mantener la integridad de todos los Datos Personales de Microsoft, garantizando que sigan siendo precisos, completos y pertinentes para los fines declarados para los que fueron Tratados.	<p>El proveedor puede demostrar que existen procedimientos para validar los Datos Personales de Microsoft cuando se recopilan, crean y actualizan.</p> <p>El proveedor puede demostrar que existen procedimientos de monitoreo y muestreo para verificar la precisión de forma continua y corregirla, si es necesario.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>
----	--	--

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
Sección I: Monitoreo y aplicación de la ley		
31	<p>El proveedor tiene un plan de respuesta a incidentes que requiere que el proveedor notifique a Microsoft según los requisitos contractuales o sin demora indebida, lo que ocurra antes, al tomar conocimiento de un Incidente de Datos.</p> <p>El proveedor debe, a petición o según la indicación de Microsoft, cooperar con esta en cualquier investigación, mitigación o reparación del incidente, incluida la facilitación a Microsoft de datos, información, acceso al personal del proveedor o al hardware necesario para llevar a cabo una revisión forense.</p> <p>Nota: Consulte la Guía del programa SSPA para saber cómo notificar un incidente a Microsoft.</p>	<p>El proveedor tiene un plan de respuesta a incidentes que incluye un paso para notificar a los clientes (Microsoft) como se describe en esta sección.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>
32	<p>Aplicar un plan de corrección y supervisar la resolución de cada Incidente de Datos para garantizar que se tomen las medidas correctivas adecuadas en el momento oportuno.</p>	<p>El proveedor ha documentado los procedimientos que adoptará para responder a un Incidente de Datos hasta su cierre.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>
33	<p>Cuando Microsoft sea el Responsable del Tratamiento de los Datos Personales de Microsoft, establecerá un proceso de reclamación formal para responder a todas las reclamaciones de protección de datos que impliquen Datos Personales de Microsoft.</p>	<p>El proveedor dispone de medios para recibir reclamaciones relacionadas con los Datos Personales de Microsoft y cuenta con un procedimiento de reclamación documentado para atender las reclamaciones.</p> <p>El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.</p>

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
Sección J: Seguridad		
	<p>El proveedor debe establecer, implementar y mantener un programa de seguridad de la información que incluya políticas y procedimientos, para proteger y mantener seguros los Datos Personales y Confidenciales de Microsoft de acuerdo con las buenas prácticas de la industria y como lo exige la Legislación.</p> <p>El programa de seguridad del proveedor debe cumplir con las normas que se indican a continuación, requisitos 34-50.</p>	<p>Una certificación ISO 27001 válida es un sustituto aceptable de la Sección J. Póngase en contacto con la SSPA para aplicar esta sustitución.</p> <p>Nota: Deberá proporcionar la certificación.</p>
34	<p>Realizar evaluaciones anuales de la seguridad de la red que incluyan lo siguiente:</p> <ul style="list-style-type: none"> ▪ revisión de cambios importantes en el entorno, como un nuevo componente del sistema, la topología de la red o las reglas del cortafuegos, ▪ escaneos de vulnerabilidad, y ▪ el mantenimiento de los registros de cambios. 	<p>El proveedor ha documentado las evaluaciones de la red, los registros de cambios y los resultados de los escaneos.</p> <p>Mediante los registros de cambios requeridos se debe hacer un seguimiento de los cambios, proporcionar información sobre el motivo del cambio e incluir el nombre y el cargo del aprobador designado.</p>
35	<p>El proveedor debe definir, comunicar y aplicar una política de dispositivos móviles que proteja y limite el uso de los Datos Personales o Confidenciales de Microsoft a los que se accede o que se utilizan en un dispositivo móvil.</p>	<p>El proveedor demuestra el uso de una política de dispositivos móviles conforme cuando el Tratamiento de Datos Personales o Confidenciales de Microsoft requiere el uso de un dispositivo móvil.</p>
36	<p>Se debe rendir cuentas de todos los activos utilizados para apoyar la Realización de la Actividad, los cuales deben tener un propietario identificado. El proveedor es responsable de mantener un inventario de estos activos de información, establecer el uso aceptable y autorizado de los activos, y proporcionar el nivel apropiado de protección para los activos a lo largo de su ciclo de vida.</p>	<p>Inventario de los activos de los dispositivos utilizados para apoyar la Realización de la Actividad. El inventario de estos activos debe incluir lo siguiente:</p> <ul style="list-style-type: none"> ▪ ubicación del dispositivo, ▪ clasificación de los datos del activo, ▪ registro de la recuperación de activos tras la finalización del contrato de trabajo o del contrato comercial, y ▪ registro de la eliminación de los soportes de almacenamiento de datos cuando ya no son necesarios.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
Sección J: Seguridad (continuación)		
37	<p>Establecer y mantener procedimientos de gestión de derechos de acceso para evitar el acceso no autorizado a cualquier Dato Personal o Confidencial de Microsoft que esté bajo el control del proveedor.</p>	<p>El proveedor demuestra que ha implementado un plan de gestión de derechos de acceso que incluye lo siguiente:</p> <ul style="list-style-type: none"> ▪ procedimientos de control de acceso, ▪ procedimientos de identificación, ▪ procedimientos de bloqueo después de intentos fallidos, ▪ parámetros robustos para seleccionar las credenciales de autenticación, y ▪ desactivación de las cuentas de los usuarios en caso de cese de la relación laboral en un plazo de 48 horas, ▪ controles sólidos de las contraseñas en cuanto a su longitud y complejidad que evitan su reutilización. <p>El proveedor demuestra que cuenta con un proceso establecido para revisar el acceso de los usuarios a los Datos Personales y Confidenciales de Microsoft, y que aplica el principio de mínimo privilegio. El proceso incluye lo siguiente:</p> <ul style="list-style-type: none"> ▪ funciones de los usuarios claramente definidas, ▪ procedimientos para revisar y justificar la aprobación del acceso a las funciones, y ▪ comprobación de que los usuarios de las funciones con acceso a los datos de Microsoft tienen una justificación documentada para estar en el grupo/función.
38	<p>Definir e implementar procedimientos de gestión de parches que den prioridad a los parches de seguridad para los sistemas utilizados para tratar Datos Personales o Confidenciales de Microsoft. Estos procedimientos incluyen lo siguiente:</p> <ul style="list-style-type: none"> ▪ enfoque de riesgo definido para priorizar los parches de seguridad, ▪ capacidad para manejar e implementar parches de emergencia, ▪ aplicabilidad al sistema operativo y al software del servidor, como el servidor de aplicaciones y el software de base de datos, ▪ documentar el riesgo que el parche mitiga y hacer un seguimiento de las excepciones, y ▪ requisitos para la retirada del software que ya no cuente con el soporte de la empresa creadora. 	<p>El proveedor puede demostrar que ha implementado un procedimiento de gestión de parches que cumple con este requisito y que cubre, como mínimo, lo siguiente:</p> <ul style="list-style-type: none"> ▪ Asignación de la gravedad para informar sobre la priorización (las definiciones de gravedad están documentadas). ▪ Procedimiento documentado para implementar parches de emergencia. ▪ Validar que no se utilicen sistemas operativos que ya no sean compatibles con la empresa creadora. ▪ Registros de gestión de parches que hagan un seguimiento de las aprobaciones y excepciones.
#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento

Sección J: Seguridad (continuación)

39	<p>Instalar software antivirus y antimalware en los equipos conectados a la red utilizados para el Tratamiento de los Datos Personales y Confidenciales de Microsoft, incluidos los servidores y las computadoras de producción y de capacitación, a fin de protegerlos contra los virus potencialmente dañinos y las aplicaciones de software malintencionado.</p> <p>Actualizar diariamente las definiciones del antimalware o según las indicaciones del proveedor de antivirus/antimalware.</p> <p>Nota: Esto se aplica a todos los sistemas operativos, incluido Linux.</p>	<p>Existen registros que demuestran que el uso de software antivirus y antimalware está activo.</p> <p>Nota: Este requisito se aplica a todos los sistemas operativos.</p>
40	<p>Los proveedores que desarrollan software para Microsoft deben incorporar los principios de seguridad por diseño en el proceso de construcción.</p>	<p>Los documentos de especificaciones técnicas de los proveedores incluyen puntos de control para la validación de la seguridad en sus ciclos de desarrollo.</p>
41	<p>Se debe emplear un programa de Prevención de Pérdida de Datos (“DLP”, por sus siglas en inglés) para evitar intrusiones, pérdidas y otras actividades no autorizadas. Los datos deben estar debidamente clasificados, etiquetados y protegidos, y el proveedor debe monitorear los sistemas de información en uso en los que se Traten Datos Personales o Confidenciales de Microsoft para evitar intrusiones, pérdidas y otras actividades no autorizadas. El programa DLP, como mínimo:</p> <ul style="list-style-type: none"> ▪ exige el uso de Sistemas de Detección de Intrusiones (“IDS”, por sus siglas en inglés) basados en el host, la red y la nube que normalmente se utilicen en el sector, si se conservan los Datos Personales o Confidenciales de Microsoft, ▪ requiere la implementación de Sistemas de Protección contra Intrusiones (“IPS”, por sus siglas en inglés) avanzados configurados para monitorear y detener activamente la pérdida de datos, ▪ requiere un análisis del sistema (en caso de que sea vulnerado) para garantizar que también se resuelva cualquier vulnerabilidad residual, ▪ describe los procedimientos necesarios para monitorear las herramientas de detección de riesgos del sistema, ▪ establece un proceso de respuesta y gestión de incidentes que debe llevarse a cabo cuando se detecta un Incidente de Datos, y ▪ requiere comunicaciones (con todos los empleados del proveedor y los subcontratistas que se encuentren fuera de la Actividad del proveedor) en relación con la descarga y el uso no autorizados de Datos Personales o Confidenciales de Microsoft. 	<p>Programa DLP documentado e implementado con procedimientos para prevenir intrusiones, pérdidas y otras actividades no autorizadas (y como mínimo, todos los elementos especificados en esta sección).</p>
#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento

Sección J: Seguridad (continuación)

42	Comunicar de inmediato los resultados de la investigación de la respuesta a incidentes a la alta dirección y a Microsoft.	Deben existir sistemas y procesos para comunicar a Microsoft los resultados de la investigación de la respuesta a incidentes.
43	Cada año, los administradores de sistemas, el personal de operaciones, la dirección y terceras partes deben recibir una capacitación en materia de seguridad.	<p>Se debe establecer un programa de capacitación en materia de seguridad que incluya lo siguiente:</p> <ul style="list-style-type: none"> ▪ capacitación anual sobre respuesta a incidentes, y ▪ simulaciones de incidentes y mecanismos automatizados para facilitar una respuesta eficaz ante las situaciones de crisis. ▪ creación de conciencia sobre la prevención de incidentes, como los riesgos relacionados con la descarga de software malintencionado.
44	El proveedor debe garantizar que los procesos de planificación de copias de seguridad protegen los Datos Personales y Confidenciales de Microsoft del uso, acceso, divulgación, alteración y destrucción no autorizados.	<p>El proveedor puede demostrar procedimientos documentados de respuesta y recuperación que detallen cómo la organización gestionará un evento perturbador y mantendrá su seguridad de la información a un nivel predeterminado basado en los objetivos de continuidad de la seguridad de la información aprobados por la dirección.</p> <p>El proveedor puede demostrar que ha definido e implementado procedimientos para realizar periódicamente copias de seguridad, almacenar de forma segura y recuperar eficazmente los datos críticos.</p>
45	Establecer y probar los planes de continuidad del negocio y de recuperación de desastres.	<p>Un plan de recuperación de desastres debe incluir lo siguiente:</p> <ul style="list-style-type: none"> ▪ Criterios definidos para determinar si un sistema es crítico para el funcionamiento de la empresa del proveedor. ▪ Enumerar los sistemas críticos en función de los criterios definidos que deben ser objeto de recuperación en caso de un desastre. ▪ Procedimiento de recuperación de desastres definido para cada sistema crítico que garantiza que un ingeniero que no conozca el sistema pueda recuperar la aplicación en menos de 72 horas. ▪ Pruebas y revisiones anuales (o más frecuentes) de los planes de recuperación de desastres para garantizar que los objetivos de recuperación se puedan cumplir.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
Sección J: Seguridad (continuación)		
46	<p>Autenticar la identidad de una persona antes de concederle acceso a los Datos Personales o Confidenciales de Microsoft y garantizar que el acceso se limite al ámbito de actividad de la persona en particular que tiene permiso para apoyar la Realización de la Actividad.</p>	<p>Asegurarse de que todos los identificadores de usuario sean únicos y que cada uno tenga un método de autenticación estándar de la industria, como Azure Active Directory.</p> <p>El acceso elevado (privilegios administrativos o de otro tipo) debe requerir el uso de un segundo factor, como una tarjeta inteligente o un autenticador basado en el teléfono.</p> <p>Programa documentado de seguridad de la información que cubra el proceso para garantizar que el acceso de todos los empleados y subcontratistas del proveedor a los Datos Personales o Confidenciales de Microsoft no sea mayor o más largo de lo necesario para apoyar la Realización de la Actividad.</p>
47	<p>El proveedor debe proteger todos los datos Tratados en relación con la Realización de la Actividad en tránsito a través de las redes con un cifrado que utilice Transport Layer Security (“TLS”) o Internet Protocol Security (“IPsec”).</p> <p>Estos métodos se describen en los documentos NIST 800-52 y NIST 800-57; también puede utilizarse una norma industrial equivalente.</p> <p>El proveedor debe rechazar la entrega de cualquier Dato Personal o Confidencial de Microsoft transmitido por medios no cifrados.</p>	<p>El proceso de creación, implementación y sustitución de certificados TLS o de otro tipo debe definirse y aplicarse.</p>
48	<p>Todos los dispositivos de los proveedores (computadoras portátiles, estaciones de trabajo, etc.) que accedan o manejen Datos Personales o Confidenciales de Microsoft deben emplear un cifrado basado en disco.</p>	<p>Cifrar todos los dispositivos para cumplir con BitLocker u otra solución de cifrado de disco equivalente en el sector para todos los dispositivos cliente utilizados para manejar Datos Personales o Confidenciales de Microsoft.</p>

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
Sección J: Seguridad (continuación)		
49	<p>Deben existir sistemas y procedimientos (que utilicen los estándares actuales del sector, como los descritos en la norma NIST 800-111) deben estar implementados para cifrar en reposo (cuando se almacenan) todos y cada uno de los Datos Personales o Confidenciales de Microsoft. Los ejemplos incluyen, pero no se limitan a lo siguiente:</p> <ul style="list-style-type: none"> ▪ Datos de credenciales (por ejemplo, nombre de usuario o contraseñas), ▪ datos de los instrumentos de pago (por ejemplo, números de tarjetas de crédito y cuentas bancarias), ▪ datos personales relacionados con la inmigración, ▪ datos de perfiles médicos (por ejemplo, números de historiales médicos o marcadores o identificadores biométricos, como el ADN, las huellas dactilares, las retinas y los iris, los patrones de voz, los patrones faciales y las medidas de las manos, utilizados con fines de autenticación), ▪ datos de identificación emitidos por el Gobierno (por ejemplo, números del seguro social o de la licencia de conducir), ▪ datos pertenecientes a clientes de Microsoft (por ejemplo, SharePoint, documentos de O365, clientes de OneDrive), ▪ material relacionado con productos de Microsoft no anunciados, ▪ fecha de nacimiento, ▪ información sobre el perfil de los niños, ▪ datos geográficos en tiempo real, ▪ dirección personal física (no comercial), ▪ números de teléfono personales (no comerciales), ▪ religión, ▪ opiniones políticas, ▪ orientación o preferencia sexual, ▪ respuestas a la pregunta de seguridad (por ejemplo, 2fa, restablecimiento de la contraseña), ▪ nombre de soltera de la madre. 	<p>Comprobar que los Datos Personales y Confidenciales de Microsoft estén cifrados en reposo.</p>
50	<p>Anonimizar todos los Datos Personales de Microsoft utilizados en un entorno de desarrollo o prueba.</p>	<p>Los Datos Personales de Microsoft no deben utilizarse en entornos de desarrollo o de prueba; cuando no haya otra alternativa, deben anonimizarse para evitar la identificación de las Personas Interesadas o el uso indebido de los Datos Personales.</p> <p>Nota: Los datos anonimizados son distintos de los datos seudonimizados. Los datos anonimizados son datos que no se refieren a una persona física identificada o identificable cuando la Persona Interesada no es identificable o deja de serlo.</p>

Glosario

“Representante Autorizado” es una persona que tiene el nivel adecuado de autoridad para firmar en nombre de la empresa. Esta persona deberá tener los conocimientos necesarios sobre privacidad y seguridad o haber consultado a un experto en la materia antes de presentar su respuesta a una acción del programa SSPA. Además, al añadir su nombre a un formulario de la SSPA están certificando que han leído y entendido los DPR.

“RDPUE”: Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE.

“Trabajador Autónomo”: personas que realizan tareas o servicios a la carta, que se contratan a través de plataformas digitales u otros medios.

“RGPD” significa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

“Requisitos de Protección de Datos de Privacidad” significa el RGPD, el EUDPR, las Leyes Locales de Protección de Datos de la UE/EEE, la Ley de Privacidad del Consumidor de California, el Código Civil de California, sección § 1798.100 y siguientes (“CCPA”), la Ley de Protección de Datos del Reino Unido de 2018 y cualquier ley, reglamento y otros requisitos legales relacionados o subsiguientes aplicables en el Reino Unido, y cualquier ley, reglamento y otros requisitos legales aplicables relacionados con (a) la privacidad y la seguridad de los datos; o (b) el uso, la recopilación, la conservación, el almacenamiento, la seguridad, la divulgación, la transferencia, la eliminación y otro tratamiento de cualquier Dato Personal.

“Cláusulas Tipo de la UE” y “Cláusulas Contractuales Tipo”: i) las cláusulas tipo de protección de datos para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países que no garanticen un nivel adecuado de protección de datos, descritas en el artículo 46 del RGPD y aprobadas por la Decisión de la Comisión Europea (UE) 2021/914, de 4 de junio de 2021; (ii) cualquier cláusula contractual adoptada en el futuro por (a) la Comisión Europea, (b) el Supervisor Europeo de Protección de Datos y aprobada por la Comisión Europea, (c) el Reino Unido en virtud de la Ley Federal General de Protección de Datos del Reino Unido, (d) Suiza en virtud de la Ley Federal de Protección de Datos de Suiza, o (e) por un Gobierno en una jurisdicción distinta de Suiza, el Reino Unido y las jurisdicciones que comprenden la Unión Europea o el Espacio Económico Europeo, donde las cláusulas rigen la transferencia internacional de datos personales, que se incorporarán y serán vinculantes para el proveedor a partir del día de su adopción.

“Alojamiento de Sitios Web”: un servicio de alojamiento de sitios web es un servicio en línea que crea o mantiene sitios web en nombre de Microsoft bajo el dominio de Microsoft; es decir, el proveedor proporciona todos los materiales y servicios necesarios para crear y mantener un sitio y lo hace accesible en Internet. El “proveedor de servicios de alojamiento web” o “*web host*” es el proveedor que proporciona las herramientas y los servicios necesarios para que el sitio o la página web se vean en Internet, como, por ejemplo, las *cookies* o las balizas web (*web beacons*) para la publicidad.