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 trata Datos Personales o Confidenciales de Microsoft y/o utiliza sistemas de IA en relación con las actividades realizadas por dicho proveedor (por ejemplo, prestación de servicios, licencias de software o servicios en la nube) según sus condiciones contractuales con Microsoft (por ejemplo, términos de Órdenes de Compra y contrato marco) ("**Actividad**", "**Actividades**" o "**Realización de Actividades**").

- En caso de conflicto entre los DPR y los requisitos que se especifican en los acuerdos contractuales celebrados entre el proveedor y Microsoft, prevalecerán los DPR, a menos que el proveedor identifique en el contrato la disposición correcta que sustituya el requisito de protección de datos aplicable (en cuyo caso, prevalecerán los términos del contrato).
- Si hubiera algún conflicto entre los requisitos que se incluyen en el presente y cualquier requisito legal o reglamentario, prevalecerán estos últimos.
- En caso de que el proveedor de Microsoft actúe como Responsable del Tratamiento, el proveedor puede tener requisitos reducidos 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 podrían reducir sus requisitos.
- La sección K (sistemas de IA) del DPR solo es aplicable a los proveedores que presten servicios relacionados con Sistemas de IA a Microsoft.

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 Tipo o, a discreción de Microsoft, otros mecanismos adecuados de transferencia transfronteriza aprobados por una autoridad de protección de datos competente o por la Comisión Europea,
según corresponda, y adoptados o acordados por Microsoft. Las Cláusulas Contractuales Tipo sucesoras adoptadas por (i) la Comisión Europea o adoptadas por el Supervisor Europeo de Protección de Datos y aprobadas por la Comisión Europea; (ii) el Reino Unido en virtud de la Ley Federal General de Protección de Datos del Reino Unido; (iii) Suiza en virtud de la Ley Federal de Protección de Datos de Suiza; o (iv) las cláusulas que rigen la transferencia internacional de datos personales, adoptadas oficialmente por un gobierno en una jurisdicción distinta de Suiza, el Reino Unido y las jurisdicciones que comprenden la Unión Europea/Espacio Económico Europeo, se incorporarán y serán vinculantes para el proveedor a partir del día de su adopción. Asimismo, el proveedor se asegurará de que todos y cada uno de los subencargados del Tratamiento (tal y como se definen en las Cláusulas Contractuales Tipo) también las cumplan.

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.

"**Sistemas de IA**" se refiere a un sistema de ingeniería que aplica un modelo optimizado para que el sistema pueda, para un conjunto determinado de objetivos definidos por el ser humano, hacer predicciones*, brindar

recomendaciones o tomar decisiones que influyan en los entornos con los que interactúa. Un sistema de este tipo puede funcionar con distintos niveles de automatización. *Las predicciones pueden referirse a diversos tipos de análisis o producción de datos (como la traducción de textos, la creación de imágenes sintéticas o el diagnóstico de un fallo eléctrico previo).

"**Responsable del Tratamiento**" se refiere a 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 que los sitios web y/o las aplicaciones almacenan en los dispositivos y 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 ilegal, la destrucción, la pérdida, la alteración,
la divulgación no autorizada o el acceso no autorizado a los Datos Personales de Microsoft o a los Datos Confidenciales de Microsoft transmitidos, almacenados o procesados de otro modo por el proveedor o sus subcontratistas, o a (2) una vulnerabilidad de la seguridad relacionada con el manejo por parte del proveedor de los
Datos Personales de Microsoft o los Datos Confidenciales de Microsoft o incidente de confidencialidad según se define en el Proyecto de ley 64 (2021, capítulo 25).

"**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.

"**Usos previstos**" se refiere a los fines principales para los que se espera que los clientes, proveedores o usuarios finales utilicen el sistema. Puede tratarse de un solo uso o de varios en el caso de los sistemas multiuso.

"**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. "**Ilegal**" 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 de Microsoft 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 "Tratamiento", "Tratar" y

“Tratado” tendrán los significados correspondientes.

“**Encargado del Tratamiento**” se refiere a la 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.

“**Información Médica Protegida**” (o “**PHI**”, por sus siglas en inglés) se refiere a los Datos Personales de Microsoft protegidos por la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA, por sus siglas en inglés).

“**Red Teaming**” es un enfoque en el que un grupo de probadores se reúnen y prueban intencionadamente un sistema para identificar sus limitaciones, superficie de riesgo y vulnerabilidades. Más información en https://aka.ms/CustomerRedTeamingGuide.

"**Uso Sensible**" de la IA se refiere a cuando el uso razonablemente previsible o el uso indebido de un Sistema de IA podría afectar a una persona de las siguientes maneras:

- Incidencia en la posición jurídica o en las oportunidades vitales.
- Riesgo de lesiones físicas o psicológicas.
- Amenaza a los derechos humanos.

Por "**Subcontratista**" se entiende un tercero al cual el proveedor delega sus obligaciones en relación con el contrato que ampara sus Actividades, incluyendo 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 confirman anualmente 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	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 Personales o Confidenciales 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. 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, la duración, la naturaleza y la finalidad del Tratamiento, el tipo de Datos Personales de Microsoft y las categorías de Personas Interesadas, así como las obligaciones y los derechos de Microsoft.	El proveedor debe presentar el contrato aplicable entre Microsoft y el proveedor. 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). Si Microsoft confirma que sus compromisos implican el tratamiento de PHI, el proveedor debe tener un Contrato de Socio Comercial y/u otro contrato vigente con Microsoft. Nota: Las empresas que tengan órdenes de compra en proceso pueden solicitar que la descripción necesaria de las actividades de Tratamiento se agregue más tarde en el proceso de compra.
2	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. Nota: Microsoft publicará esta designación en su perfil cuando corresponda.	Cláusulas Contractuales Tipo, Adenda de Datos de Clientes en Línea, Adenda de Tratamiento de Datos de Servicios Profesionales del Proveedor o Socio y/o Contrato de Socio Comercial.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección A: Administración (continuación)	
3	Establecer, mantener y llevar a cabo una capacitación anual sobre privacidad y seguridad para cualquier persona (administradores de sistemas, personal de operaciones, directivos, terceros, etc.) que vaya a tener acceso a los Datos Personales o Confidenciales de Microsoft. Nota: Es posible que el personal de los proveedores deba tomar cursos adicionales de capacitación impartidos por las divisiones de Microsoft.	Los registros anuales de asistencia están disponibles y pueden proporcionarse a Microsoft si lo solicita. El contenido de la capacitación se actualiza periódicamente e incluye principios de privacidad y seguridad, como la concienciación sobre la prevención de incidentes, incluida la protección de contraseñas, la supervisión del inicio de sesión, los riesgos asociados a la descarga de software malicioso y otros recordatorios de seguridad pertinentes. 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. Capacitación sobre respuesta a incidentes, y simulaciones de incidentes y mecanismos automatizados para facilitar una respuesta eficaz ante las situaciones de crisis. Si los Datos Personales de Microsoft tratados por el proveedor incluyen PHI, el contenido de la capacitación debe incluir formación sobre la HIPAA, incluidos los usos y divulgaciones permitidos por el proveedor según lo previsto en el Contrato de Socio Comercial.
4	Aplicar sanciones apropiadas contra los empleados que no cumplan con las políticas de privacidad y seguridad del proveedor o con las políticas aplicables de Microsoft si se está trabajando dentro de un entorno corporativo de Microsoft.	Documentación de las políticas de privacidad y seguridad que describan las sanciones por incumplimiento (por ejemplo, hasta el despido).
5	Tratar los Datos Personales de Microsoft únicamente de acuerdo con las instrucciones documentadas por Microsoft. Esto incluye 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 proveedor (Encargado del Tratamiento o el Subencargado del Tratamiento) deberá informar a Microsoft (el responsable del tratamiento) dicho requisito legal antes del Tratamiento, a menos que dicha Legislación prohíba dicha información por motivos importantes de interés público.	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.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección B: Aviso	
6	El proveedor debe utilizar la Declaración de Privacidad de Microsoft cuando recopile Datos Personales en nombre de Microsoft. El aviso de privacidad debe ser obvio y estar disponible para las Personas Interesadas para ayudarlas a decidir si entregan sus Datos Personales al proveedor. Nota: Si su empresa es la Responsable del tratamiento de los datos, por ejemplo, cuando un sitio web no tenga la marca Microsoft, el proveedor puede mostrar su propio aviso de privacidad.	El proveedor utiliza un fwdlink para la Declaración de Privacidad de Microsoft publicada actualmente. La Declaración de Privacidad se publica en cualquier contexto en el que se recopilen los Datos Personales de un usuario. Si corresponde, existe una versión sin conexión que se facilita antes de la recopilación de datos. Toda Declaración de Privacidad sin conexión utilizada será la versión publicada más reciente y estará debidamente fechada. Para los servicios de los empleados de Microsoft, se utiliza el Aviso de Privacidad de Datos de Microsoft.
	Sección C: Elección y consentimiento	
7	Antes de recopilar los Datos Personales, 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). 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.	El proveedor debe poder 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. El proveedor debe poder demostrar cómo una Persona Interesada retira su consentimiento para una actividad de Tratamiento. El proveedor debe poder demostrar cómo se comprueban las preferencias antes de iniciar una nueva actividad de Tratamiento. 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.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección C: Elección y consentimiento (continuación)	
8	Los sitios web que utilizan cookies (y/o tecnologías similares que almacenan o recuperan datos de un dispositivo o que permiten el rastreo del usuario de manera similar) deben obtener los consentimientos que exige la ley de las personas interesadas antes de utilizar o colocar las cookies en relación con los navegadores o dispositivos de las personas interesadas. 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. 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.	El propósito de cada cookie debe estar documentado y debe informar el tipo de cookie implementado. • Las cookies persistentes no deben utilizarse cuando las cookies de sesión sean 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. Validar el cumplimiento de las leyes de la UE según corresponda, como: • 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.
	Sección D: Recopilación	
9	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.	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. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
10	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.	El proveedor puede aportar documentación que demuestre el consentimiento de los padres o tutores. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
11	Cuando el proveedor reciba un conjunto de datos de Microsoft con identificabilidad reducida, incluido un seudónimo, persona no identificable (NPI, por sus siglas en inglés), seudónimo no vinculado, agregado, anónimo o cualquier término que se relacione con una de esas clasificaciones (como no identificado), el proveedor mantendrá los datos en el estado en que se recibieron.	El proveedor no aumentará la identificabilidad de los conjuntos de datos (es decir, no reidentificará a las personas que forman parte de un conjunto de datos mediante la unión a otros conjuntos de datos, etc.). El proveedor dispone de una política/proceso de eliminación de identificación/anonimización de datos.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección E: Conservación	
12	Garantizar que los Datos Personales y Confidenciales de Microsoft no se conserven 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.	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). El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
13	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. 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. 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.	Mantener un registro de la disposición de los Datos Personales y Confidenciales de Microsoft (esto puede incluir la devolución a Microsoft para su destrucción). Si Microsoft exige o solicita la destrucción, proporcionar un certificado de destrucción firmado por un funcionario del proveedor.
	Sección F: Personas Interesadas	
	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:	

14	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. 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.	El proveedor mantendrá pruebas de los procesos y procedimientos documentados para respaldar la ejecución de los Derechos de las Personas Interesadas. El proveedor mantendrá evidencia documental de las pruebas realizadas. La evidencia estará disponible a petición de Microsoft.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección F: Personas Interesadas (continuación)	
15	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.	El proveedor ha documentado el método utilizado para identificar a las Personas Interesadas de Microsoft. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
16	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.	El proveedor mantendrá pruebas documentales de los procedimientos implementados para determinar si se conservan los Datos Personales de Microsoft y proporcionará la documentación a Microsoft si esta lo solicita. El proveedor mantiene un registro que demuestra las medidas adoptadas para satisfacer las solicitudes de Derechos de las Personas Interesadas. La documentación incluye: • Fecha y hora de la solicitud, • Las medidas adoptadas para responder a la solicitud y el registro de cuándo se le informó a Microsoft. El proveedor proporcionará a Microsoft pruebas de la conservación de los registros cuando se le solicite.

17	El proveedor comunicará a las Personas Interesadas los pasos que deben seguir para acceder a sus Datos Personales de Microsoft o para ejercer sus derechos con respecto a sus datos.	El proveedor mantendrá pruebas documentales de las comunicaciones y procedimientos de acceso a los Datos Personales de Microsoft. El proveedor mantendrá pruebas documentales y proporcionará dichas pruebas a Microsoft cuando se le solicite.
18	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. Si su solicitud es denegada, a instancias de Microsoft, proporcionar a la Persona Interesada una explicación por escrito. Proporcionar los registros de las solicitudes de las Personas Interesadas a Microsoft cuando lo solicite.	El proveedor mantiene registros de las solicitudes de acceso/borrado y documenta los cambios realizados en los Datos Personales de Microsoft. Documentar los casos en los que se deniegan las solicitudes y conservar las pruebas de la revisión y aprobación de Microsoft. El proveedor proporcionará pruebas de la conservación de registros de solicitudes y denegaciones de acceso a los Datos Personales de Microsoft.
19	El proveedor debe brindar acceso a Microsoft u obtener una copia de los Datos Personales de Microsoft solicitados para la Persona Interesada autentificada 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.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección F: Personas Interesadas (continuación)	
20	El proveedor debe tomar precauciones razonables para garantizar que los Datos Personales de Microsoft entregados a Microsoft o a una Persona Interesada autentificada no puedan ser utilizados para identificar a otra persona.	El proveedor mantendrá pruebas documentales 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.	El proveedor documenta los casos de desacuerdo y eleva la cuestión a Microsoft. El proveedor proporcionará a Microsoft las pruebas documentales cuando se le solicite.
22	Por lo que respecta a las solicitudes de acceso de las Personas Interesadas, el proveedor deberá mantener un registro de todos los destinatarios con los que haya compartido o vaya a compartir Datos Personales de Microsoft.	Previa solicitud, el proveedor puede proporcionar una lista de todos los destinatarios reales y posibles terceros destinatarios de los Datos Personales de Microsoft.
	Sección G: Subcontratistas	

	Si el proveedor pretende utilizar a un Subcontratista para el Tratamiento de los Datos Personales o Confidenciales de Microsoft, deberá:	
23	Notificar a Microsoft antes de subcontratar servicios o realizar cualquier cambio relativo a la adición o sustitución de subcontratistas.	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.
24	Exigir que el subcontratista acepte por escrito términos que no sean menos protectores para Microsoft que los términos del contrato del proveedor con Microsoft, incluyendo los términos de privacidad y protección de datos.	El proveedor proporcionará a Microsoft los contratos celebrados con los subcontratistas cuando se le solicite.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección G: Subcontratistas (continuación)	
25	Documentar la naturaleza y el alcance de los Datos Personales y Confidenciales de Microsoft tratados por los subcontratistas para garantizar que la información recopilada sea necesaria para la Realización de la Actividad.	El proveedor mantiene la documentación relativa a los Datos Personales y Confidenciales de Microsoft divulgados o transferidos a los subcontratistas. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
26	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. Si los Datos Personales de Microsoft son PHI, celebre también un Contrato de Socio Comercial con el Subcontratista que limite el Tratamiento de los Datos Personales de Microsoft por parte del Subcontratista y proteja la confidencialidad y seguridad de los Datos Personales de Microsoft del mismo modo que el Contrato de Socio Comercial entre Microsoft y el proveedor.	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. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite, incluido el Contrato de Socio Comercial, si corresponde.
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.	El proveedor ha proporcionado las instrucciones y los medios para que un subcontratista informe el uso indebido de los datos de Microsoft. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
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.	El proveedor puede proporcionar la documentación de la diligencia debida realizada en relación con las políticas y prácticas de protección de datos del tercero. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección H: Calidad	
29	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.	El proveedor puede demostrar que existen procedimientos para validar los Datos Personales de Microsoft cuando se recopilan, crean y actualizan. El proveedor puede demostrar que existen procedimientos de monitoreo, revisión de la actividad del sistema de información y muestreo para verificar la precisión de forma continua y corregirla, si es necesario. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
	Sección I: Monitoreo y aplicación de la ley	
30	El proveedor tiene un plan de respuesta ante 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. El proveedor debe, a petición o según la indicación de Microsoft, cooperar con Microsoft 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. También puede ser necesario facilitar acceso al personal del proveedor o al hardware necesario para llevar a cabo una revisión forense. Los proveedores llenarán los campos de contacto de seguridad en SupplierWeb con los datos del personal apropiado para permitir la participación inmediata en caso de un incidente de seguridad. Nota: Consulte la Guía del programa SSPA para saber cómo notificar un incidente a Microsoft.	El proveedor tiene un plan de respuesta ante incidentes que incluye un paso para notificar a los clientes (Microsoft) como se describe en esta sección. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.

31	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.	El proveedor ha documentado los procedimientos que seguirá para responder a un Incidente de Datos hasta su cierre, que incluyen actualizaciones oportunas a Microsoft hasta que se resuelva el problema y proporciona una revisión posterior al incidente. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección I: Monitoreo y aplicación de la ley (continuación)	
32	Cuando Microsoft sea el Responsable del Tratamiento de los Datos Personales de Microsoft, establecerá un proceso de queja formal para responder a todas las quejas de protección de datos que impliquen Datos Personales de Microsoft.	El proveedor dispone de medios para recibir quejas relacionadas con los Datos Personales de Microsoft y cuenta con un procedimiento de quejas documentado para atender las reclamaciones. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
	Sección J: Seguridad	
	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. El programa de seguridad del proveedor debe cumplir con las normas que se indican a continuación, requisitos 33-49. Si los Datos Personales de Microsoft son PHI, el proveedor también deberá realizar una evaluación periódica técnica y no técnica en respuesta a los cambios ambientales y operativos que afecten a la seguridad de la PHI que establezca hasta qué punto las políticas y procedimientos del proveedor cumplen los requisitos de la Norma de Seguridad de la HIPAA.	Una certificación ISO 27001 válida es un sustituto aceptable de la Sección J: Seguridad. Nota: Tendrá que cargar el certificado para aplicar la sustitución.

33	Realizar evaluaciones anuales de la seguridad de la red que incluyan lo siguiente: • La evaluación de los riesgos y vulnerabilidades potenciales para la confidencialidad, integridad y disponibilidad de los Datos Personales de Microsoft y la aplicación de medidas para reducir los riesgos, • La revisión de cambios importantes en el entorno, como un nuevo componente del sistema, la topología de la red o las reglas del cortafuegos, y • El mantenimiento de los registros de cambios.	El proveedor ha documentado las evaluaciones de la red, los registros de cambios y los resultados de los escaneos. 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. Los registros de los últimos 90 días están disponibles previa solicitud.
34	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.	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.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
35	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.	Inventario de los activos de los dispositivos utilizados para apoyar la Realización de la Actividad, la seguridad y las operaciones. El inventario de estos activos debe incluir lo siguiente: • 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. • Todos los dispositivos físicos y virtuales utilizados por el personal del proveedor con credenciales @microsoft.com para acceder a los datos de Microsoft deben estar totalmente gestionados únicamente por Microsoft, sin ningún software de seguridad adicional instalado más allá de lo que Microsoft ha proporcionado.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
36	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.	El proveedor demuestra que ha implementado un plan de gestión de derechos de acceso que incluye lo siguiente: • Procedimientos de control de acceso, • Procedimientos de identificación, • Procedimientos de bloqueo después de intentos fallidos, • Cierre automático de sesión tras inactividad, • Parámetros robustos para seleccionar las credenciales de autenticación, y • Desactivación de las cuentas de los usuarios (incluidas las cuentas utilizadas por empleados o subcontratistas) 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 eviten su reutilización. • Uso de la autenticación multifactorial (AMF) para las identidades. 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: • 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. • Prohibición estricta de compartir cuentas o contraseñas

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
37	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: • Realizar escaneos de vulnerabilidad todos los meses con un informe de cumplimiento de alto nivel que muestre los escaneos mensuales de los 12 meses anteriores, • 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.	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: • Las definiciones de gravedad están documentadas y se asignan a las actualizaciones para informar sobre la priorización de la implementación. • Procedimiento documentado para implementar parches de emergencia. • Registros de gestión de parches que realizan un seguimiento de las aprobaciones y excepciones, e incluyen datos de cumplimiento de parches. Los registros de los últimos 90 días están disponibles previa solicitud.
38	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. El software antivirus y antimalware debe parchearse y actualizarse con frecuencia. Actualizar diariamente las definiciones del antimalware o según las indicaciones del proveedor de antivirus/antimalware. Nota: Esto se aplica a todos los sistemas operativos, incluido Linux.	Existen registros que demuestran que el uso de software antivirus y antimalware está activo. Nota: Este requisito se aplica a todos los sistemas operativos.
39	Los proveedores que desarrollan software para Microsoft deben incorporar los principios de seguridad por diseño en el proceso de construcción.	Los documentos de especificaciones técnicas de los proveedores incluyen puntos de control para la validación de la seguridad en sus ciclos de desarrollo. El proveedor utiliza algún tipo de escáner de código para alertar sobre fallos evidentes.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
40	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 a nivel de aplicación, sistema e infraestructura. 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: • Exige el uso de Sistemas de Protección contra Intrusiones ("IDS", por sus siglas en inglés) estándar del sector basados en host, red y nube si conserva 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 • Exige comunicaciones (a todos los empleados y subcontratistas del proveedor que se desvinculen del rendimiento del proveedor) en relación con la descarga y el uso no autorizados de Datos Personales o Confidenciales de Microsoft.	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).

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
41	El proveedor debe asegurarse de que los secretos no estén incrustados o codificados en el software en ninguna fase del proceso de desarrollo.	El proveedor cuenta con procedimientos documentados para garantizar que secretos como nombres de usuario, contraseñas, claves SSH, tokens de acceso a API, etc., nunca se incorporaron a archivos fuente o de configuración, ni en entornos de prueba ni de producción. El proveedor puede demostrar: • Uso de una versión compatible y actual de una herramienta de prevención de exposición de credenciales como GitHub Advanced Security (GHAS) o un servicio o una herramienta similar. • Garantía de que si los archivos fuente o de configuración incluían secretos por error, dichos secretos quedaban documentados como revocados tras su descubrimiento. • Garantía de que cualquier credencial de sustitución o secundaria no se reintrodujo en el código. • Documentación de los falsos positivos y su corrección.
42	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.	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. 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.

43	Establecer y probar los planes de continuidad del negocio y de recuperación de desastres.	Un plan de recuperación de desastres debe incluir lo siguiente: • 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 garantice 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)	
44	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.	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. Debe exigir el uso de una autenticación multifactor (MFA, por sus siglas en inglés), como una llave de seguridad, un autenticador basado en teléfono o una tarjeta inteligente. 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 de mayor duración de lo necesario para apoyar la Realización de la Actividad.

45	Los proveedores verificarán a lo largo del proceso de contratación y asignación, mediante la voz y la apariencia visual, que el empleado al que entrevistaron, contrataron y asignaron a Microsoft es la misma persona. La información de la dirección del empleado debe coincidir con su información bancaria y la ubicación para cualquier envío de equipos.	Antes de empezar a trabajar, el empleado debe reunirse con su contacto principal en Microsoft junto con la persona del proveedor que entrevistó y contrató al empleado. El contacto principal en Microsoft debe mantener interacciones periódicas en tiempo real con el empleado a través de audio y video durante el horario laboral normal. Para cualquier envío de equipos, el proveedor documentará la confirmación de que el lugar a donde se hará el envío es una residencia real y habitable (es decir, no un punto de transbordo) y que coincide con la dirección que el empleado proporcionó para los servicios bancarios.
46	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**"). Estos métodos se describen en los documentos NIST 800-52 y NIST 800-57; también puede utilizarse una norma industrial equivalente. El proveedor debe rechazar la entrega de cualquier Dato Personal o Confidencial de Microsoft transmitido por medios no cifrados.	El proceso de creación, implementación y sustitución de certificados TLS o de otro tipo debe definirse y aplicarse.
47	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 de disco completo.	Cifrado de todos los dispositivos para cumplir con BitLocker u otra solución de cifrado de disco completo equivalente en el sector para todos los dispositivos de los clientes utilizados para manejar Datos Personales o Confidenciales de Microsoft.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
48	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, entre otros: • 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 de la seguridad social o del permiso 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 física personal (no comercial) • Números de teléfono personales (no comerciales) • Religión • Opciones políticas • Orientación o preferencia sexual • Respuestas a la pregunta de seguridad (por ejemplo, autenticación de 2 factores, restablecimiento de la contraseña)	Comprobar que los Datos Personales y Confidenciales de Microsoft estén cifrados en reposo.

	• Nombre de soltera de la madre	

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
49	Anonimizar todos los Datos Personales de Microsoft utilizados en un entorno de desarrollo o prueba.	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. Nota: Los datos anonimizados son distintos de los datos seudonimizados. Los datos anonimizados son aquellos que no se refieren a una persona física identificada o identificable en los que la Persona Interesada no es identificable o deja de serlo. Si los datos personales de Microsoft son PHI, la anonimización debe cumplir la norma de eliminación de identificación de la HIPAA.
	Sección K: Sistemas de IA	
50	Cuando se incluyan sistemas de IA en relación con la prestación de un servicio, el proveedor deberá haber suscrito con Microsoft las condiciones aplicables a los sistemas de IA. Cualquier cambio en los usos previstos debe divulgarse sin demora indebida y revisarse al menos una vez al año para comprobar su exactitud y cumplimiento.	Condiciones contractuales de los Sistemas de IA presentes en el contrato entre Microsoft y el proveedor.
51	Asigne la responsabilidad y la obligación de rendir cuentas de la resolución de problemas, la gestión, el funcionamiento, la supervisión y el control del Sistema de IA durante y después de la implementación, a una persona o grupo designado dentro de la empresa.	Indicar la función de la persona o el grupo encargado de garantizar el cumplimiento de los Sistemas de IA. Documento que describe la autoridad y responsabilidad de esta persona o grupo.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección K: Sistemas de IA (continuación)	
52	Establecer, mantener y llevar a cabo una capacitación anual en materia de privacidad y seguridad para cualquier persona que vaya a tener acceso o a procesar datos dentro de los Sistemas de IA por parte del proveedor en relación con la Realización de la Actividad.	Los registros anuales de asistencia están disponibles y pueden proporcionarse a Microsoft si lo solicita. 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 para el uso continuado de los Sistema de IA. El contenido de la capacitación se valida anualmente.
53	El proveedor cuenta con un plan de respuesta a incidentes del Sistema de IA que exige al proveedor notificar a Microsoft según los requisitos contractuales, según lo descrito por la ley de privacidad aplicable o sin demoras indebidas, lo que ocurra antes, al tener conocimiento de un Incidente de Datos o un fallo descubierto que pudiera afectar negativamente a cualquiera de los usos previstos y usos sensibles enumerados para un Sistema de IA. Nota: Consulte la Guía del Programa SSPA para saber cómo notificar un incidente a Microsoft.	El proveedor dispone de un plan de respuesta a incidentes del Sistema de IA que incluye lo siguiente en todos los puntos finales: • Un paso para notificar a los clientes (Microsoft) tal y como se describe en este requisito. • Plan de reversión del sistema, incluido el tiempo transcurrido hasta que se pueda revertir todo el sistema. • Asistencia de desactivar funciones, incluido el tiempo transcurrido hasta que se puede desactivar la función. • El proceso de actualización y publicación de las actualizaciones de cada modelo, incluido el tiempo transcurrido hasta la actualización del sistema. • El proceso relativo a cómo se notificarán a los clientes, los socios y los usuarios finales los cambios en el sistema, la comprensión actualizada de los fallos y sus mejores mitigaciones. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
54	El proveedor debe disponer de Red Teaming de los Sistemas de IA. Las vulnerabilidades deben abordarse antes del despliegue del Sistema de IA.	El proveedor dispone de documentación para lo siguiente: • Existen procesos de Red Teaming. • Se han abordado las vulnerabilidades.

55	El proveedor cuenta con un programa de IA responsable para garantizar el cumplimiento de los datos mediante la divulgación y la documentación, que incluye lo siguiente (requisitos 56-61).	El proveedor dispone de documentación que describe el programa de IA responsable. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
56	El proveedor cuenta con las divulgaciones sobre la Transparencia de Usos Previstos.	Las divulgaciones sobre la Transparencia de Usos Previstos se proporcionan a Microsoft previa solicitud.
#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección K: Sistemas de IA (continuación)	
57	**Contrato firmado**: Al contratar proveedores de IA, las organizaciones deben establecer condiciones contractuales claras en un contrato firmado. Dichos contratos deben abordar explícitamente el tratamiento de datos, la confidencialidad, los derechos de propiedad intelectual, la responsabilidad, la respuesta a incidentes y cualquier uso sensible aplicable.	El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite, incluido el Contrato de Socio Comercial, si corresponde.
58	**Obligación**: Definir líneas claras de obligaciones y responsabilidades para la implementación de la IA y la gestión de riesgos dentro de la organización. Las organizaciones deben identificar a las partes responsables de los resultados de los Sistemas de IA. Esto incluye abordar las preocupaciones éticas, los prejuicios y cualquier problema que pueda surgir con el tiempo. La supervisión y auditoría periódicas de los modelos de IA son esenciales para mantener el cumplimiento de las directrices éticas.	El proveedor dispone de un documento en el que se describe el programa de IA responsable, que incluye las obligaciones y las responsabilidades de la persona o el grupo. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
59	**Evaluación de riesgos**: Hacer una evaluación de los riesgos de privacidad, seguridad y/o responsabilidad de la IA para analizar posibles sesgos, vulnerabilidades de seguridad y consecuencias imprevistas. Si se pretende algún uso sensible, deben incluirse orientaciones sobre los controles o las mitigaciones necesarias.	El proveedor mantendrá pruebas de las evaluaciones de riesgos o documentación o informes similares que incluyan pruebas, supervisión de la evolución del sistema y mantenimiento continuo anual para mejorar los errores conocidos o descubiertos, impactos dispares en grupos demográficos, alucinaciones y otras correcciones o controles técnicos necesarios para mantener el cumplimiento de la seguridad y la privacidad. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
60	**Transparencia y explicabilidad**: Los Sistemas de IA deben ser transparentes y explicables. El proveedor debe proporcionar información sobre cómo se toman	El proveedor debe registrar todos los informes de fallos del sistema, corrupción, alucinaciones o informes de uso indebido que se desvíen de la finalidad prevista

	las decisiones. La divulgación debe fomentar la transparencia en la arquitectura de los modelos, los datos de capacitación y los procesos de toma de decisiones.	y aportar pruebas de las medidas adoptadas para resolver los problemas. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
61	**Monitoreo y adaptación**: El proveedor debe demostrar una supervisión continua de los Sistemas de IA y adaptarlos y actualizarlos a medida que surjan nuevos riesgos.	El proveedor debe registrar todos los informes de fallos del sistema, corrupción, alucinaciones o informes de uso indebido que se desvíen de la finalidad prevista y aportar pruebas de las medidas adoptadas para resolver los problemas. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección K: Sistemas de IA (continuación)	
62	El proveedor debe proporcionar las divulgaciones, los informes u otra documentación similar necesaria con todos los tipos de error, definiciones de métricas de rendimiento, indicadores de rendimiento de datos, seguridad y fiabilidad que se requieran para cada uso previsto.	• Definir y proporcionar márgenes de error aceptables para cada factor operativo que pueda afectar a cada uno de los usos previstos, así como cualquier factor operativo adicional que pueda reducir los márgenes aceptables o disminuir los porcentajes de error aceptables (incluidos los porcentajes de error falso positivo y falso negativo) que puedan afectar a dichos usos previstos. • Identificar los factores operativos y/o los usos previstos, incluida la calidad de la entrada del sistema, el uso y el contexto operativo es fundamental para gestionar un uso confiable y seguro del sistema en su contexto de implementación. • Divulgar y documentar los casos de uso sensibles. • Documentar la aplicación de controles eficaces en el diseño del sistema para desalentar el sesgo de automatización (la posible tendencia a confiar demasiado en los resultados producidos por el sistema). • Documentar cualquier limitación del sistema, limitaciones del modelo de datos de entrada o salida, o fallos previsibles, incluidos los usos para los que no se diseñó o evaluó el sistema que puedan afectar a los usos previstos. • Documentar las mitigaciones y los controles implementados para los riesgos conocidos de la IA, como la manipulación de inferencias (los “jailbreaks”), la manipulación de modelos (por ejemplo, el envenenamiento de datos) y la divulgación de información inferencial (por ejemplo, la extracción de indicios). • Pruebas de la precisión y el rendimiento del sistema, además de la medida en que estos resultados son generalizables a otros casos de uso.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección K: Sistemas de IA (continuación)	
63	El proveedor actualizará las divulgaciones de transparencia, incluido el uso sensible y los usos previstos, y notificará a Microsoft si: • Se añaden nuevos usos, • Cambia la funcionalidad, • El producto pasa a una nueva fase de lanzamiento, • Se descubre o aplica nueva información sobre prestaciones fiables y seguras que afecten al uso previsto, • Se dispone de nueva información sobre la precisión y el rendimiento del sistema.	El proveedor tiene un plan de respuesta ante incidentes que incluye un paso para notificar a Microsoft como se describe en esta sección.
64	Como parte de las divulgaciones de transparencia, el proveedor debe documentar un procedimiento operativo estándar y un plan de acción de supervisión del estado del sistema para cada modelo de datos o sistema de IA que incluya lo siguiente: • Los procesos de reproducción de fallos del sistema para apoyar la resolución de problemas y la prevención de futuros fallos, • Qué eventos se supervisarán, • Cómo se priorizarán los eventos para su revisión, • La frecuencia prevista de dichas revisiones, • Cómo se priorizarán los sucesos para la respuesta y el calendario para la resolución, • Los componentes de IA de terceros, incluido el software de código abierto, que se mantienen actualizados.	El proveedor ha documentado las políticas y los procedimientos de supervisión del estado del sistema que seguirá para cada Sistema de IA, tal y como se describe en esta sección. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
65	Establecer y documentar un inventario detallado de los métodos de supervisión de la salud del sistema que se utilizarán, entre los que se incluyen: • Los datos y las perspectivas generadas a partir de repositorios de datos, análisis de sistemas y alertas asociadas, • Los procesos mediante los cuales los clientes pueden enviar información sobre fallos y preocupaciones, y • Los procesos por los que el público en general puede enviar sus comentarios.	El proveedor ha documentado los métodos de supervisión del estado del sistema descritos en esta sección. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección K: Sistemas de IA (continuación)	
66	Si se descubren pruebas de que el Sistema de IA no es apto para el uso o los usos previstos en cualquier momento antes o durante el uso del sistema, el proveedor hará lo siguiente: • Eliminará el uso previsto de los materiales de cara al cliente y advertirá a los clientes actuales del problema, tomará medidas para cerrar la brecha identificada o interrumpirá el sistema, • Revisará la documentación relacionada con el uso previsto, y • Publicará la documentación revisada a los clientes.	El proveedor ha documentado las políticas y los procedimientos que seguirá en caso de fallo del uso previsto, tal y como se describe en esta sección.
67	El proveedor deberá identificar y revelar todos los grupos demográficos conocidos, incluidos los grupos marginados, que puedan correr el riesgo de experimentar una calidad de servicio peor o adversa en función del uso o los usos previstos del Sistema de IA, las zonas geográficas en las que se desplegará el Sistema de IA o los sesgos inherentes al Sistema de IA. Entre los grupos demográficos figuran los siguientes: • Los grupos definidos por un único factor, y • Los grupos definidos por una combinación de factores.	El proveedor debe identificar y documentar cualquier factor justificable, como factores circunstanciales y otros factores operativos (por ejemplo, el “ruido de fondo” para los sistemas de reconocimiento de voz), que expliquen lo siguiente: • Cualquier incapacidad para alcanzar cualquier objetivo de nivel mínimo de rendimiento para cualquier grupo demográfico identificado, • Cualquier diferencia de rendimiento restante entre los grupos demográficos identificados. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.

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. Asimismo, al escribir su nombre en el formulario de SSPA certifican que han leído y entendido los DPR.

"**RDPUE**": Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo del 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**" es la persona que realiza tareas o servicios a solicitud, que se contratan a través de plataformas digitales u otros medios.

"**RGPD**" se refiere al 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).

"Supervisión Humana" es la categoría de Supervisión Humana designada por el proveedor y el nivel de intervención disponible si se detectan fallos en el sistema de IA para los usos previstos:

- "Human-in-the-loop" (capacidad de intervención humana en cada ciclo de toma de decisiones del sistema).
- "Human-on-the-loop" (capacidad de intervención humana durante el ciclo de diseño del sistema y la supervisión de su funcionamiento).
- "Human-in-command" (capacidad para supervisar la actividad general del sistema de IA y decidir cuándo y cómo utilizar el sistema de IA en una situación determinada).

"**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.

Las **"Cláusulas Tipo de la UE" y "Cláusulas Contractuales Tipo"** son (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 del 4 de junio de
2021; (ii) cualquier cláusula contractual tipo 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" es un servicio de alojamiento de sitios web 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 de sitios 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 publicidad.