Requisitos de protección de datos para proveedores de Microsoft

Aplicabilidad

Los requisitos de protección de datos para proveedores de Microsoft ("**DPR**") se aplican a cada proveedor de Microsoft que procesa datos personales o confidenciales de Microsoft en relación con la actividad de dicho proveedor (por ejemplo: provisión de servicios, licencias de software, servicios en la nube) según los términos de su contrato con Microsoft (por ejemplo: términos de pedidos de compra, acuerdo marco) ("**actividad**", "**actividades**" o "**rendimiento**").

- En caso de conflicto entre los requisitos aquí detallados o los requisitos especificados en los acuerdos contractuales entre el proveedor y Microsoft, el DPR prevalece a no ser que el proveedor pertinente identifique en el formulario de atestación de DPR la provisión correcta en el contrato que tiene el conflicto con la sección de DPR aplicable (en cuyo caso, los términos del contrato prevalecen).
- Si hubiera algún conflicto entre los requisitos que aquí se detallan y cualquier requisito legal o estatutario, estos últimos serán los que prevalecerán.
- En caso de que el proveedor de Microsoft ejerza de director con respecto a este DPR, solo se aplican los requisitos de las secciones J (Seguridad) y A (Gestión) con respecto a las actividades de procesamiento de dicho proveedor.
- En caso de que el proveedor de Microsoft no procese datos personales de Microsoft, sino solo confidenciales, con respecto a este DPR, solo se aplican los requisitos de las secciones A (Gestión), E (Conservación) y J (Seguridad) con respecto a las actividades de procesamiento de datos confidenciales de Microsoft por parte de dicho proveedor.

Transferencia internacional de datos

Sin limitación de sus otras obligaciones, el proveedor no realizará ninguna transferencia internacional de datos personales de Microsoft a no ser que Microsoft lo haya autorizado previamente por escrito, y deberá cumplir con los requisitos de protección de datos de cualquiera de los términos contractuales estándares, reglas corporativas vinculantes u otros esquemas aprobados por cualquier autoridad de protección de datos, el Consejo Europeo de Protección de Datos o la Comisión Europea y adoptados o aceptados por Microsoft, incluidos los acuerdos entre la Unión Europea y Estados Unidos y los acuerdos entre Suiza y Estados Unidos. Marcos del Escudo de privacidad y Reglamento General de la Unión Europea relativo a la Protección de Datos. El proveedor acepta la obligación de informar a Microsoft en el caso de determinar que no puede continuar cumpliendo sus obligaciones con el fin de proporcionar el mismo nivel de protección que requieren los principios del Escudo de Privacidad. El proveedor también garantizará que todos los subprocesadores (tal y como se definen en la cláusula 1(d) de las cláusulas contractuales estándar de 2010 publicadas como anexo a la Decisión de la Comisión Europea C(2010)593) también cumplen dichos requisitos.

Definiciones clave

Los siguientes términos usados en este DPR tienen estos significados. Se interpreta que los ejemplos que siguen a "incluido", "como", "p. ej.", "por ejemplo" o similares empleados en este DPR incluyan "sin limitaciones" "entre otros", a no ser que se especifique con palabras como "solo" o "únicamente".

"**Director**" hace referencia a la persona natural o legal, autoridad pública, agencia o cualquier otra entidad que, sola o junto con otros, determina los propósitos y medios del procesamiento de datos personales; en el caso de que dichos propósitos y medios los determine la Unión Europea ("**UE**") o legislaciones de los Estados miembros, el director (o los criterios para nominar al director) lo pueden designar dichas legislaciones.

La "**vulneración de datos**" es el incumplimiento de seguridad que conlleva, ya sea de forma accidental o ilícita, la destrucción, la pérdida, la alteración, la divulgación o el acceso no autorizados a los datos personales o confidenciales de Microsoft que se transmiten, almacenan o procesan de cualquier modo.

El "**derecho de persona interesada**" se referencia al derecho de una persona interesada a acceder, eliminar, editar, exportar, restringir u oponerse al procesamiento de los datos personales de Microsoft de dicha persona interesada si lo requiere la ley.

La "**ley**" hace referencia a todas las leyes aplicables, así como normas, estatutos, decretos, decisiones, órdenes, normativas, dictámenes, códigos, promulgaciones, resoluciones y requisitos de cualquier autoridad pública (federal, estatal, local o internacional) con jurisdicción. "**Ilegal**" supone cualquier infracción de la ley.

Los "**datos confidenciales de Microsoft**" son toda aquella información que, de ponerse en riesgo su confidencialidad o integridad de algún modo, puede suponer una pérdida considerable para Microsoft en términos financieros y de reputación. Aquí se incluyen productos de hardware y software de Microsoft, aplicaciones de línea de negocio internas, material de marketing preliminar, claves de licencia de productos y documentación técnica relacionada con los productos y servicios de Microsoft.

Los "**datos personales de Microsoft**" son todos aquellos datos personales procesados por Microsoft o en su nombre.

Los "**datos personales**" son toda aquella información relacionada con una persona física identificada o identificable ("**persona interesada**"). Una persona física identificable es aquella a quien se puede identificar de forma directa o indirecta teniendo en cuenta elementos de identificación como un nombre, un número de identificación, los datos de ubicación, una identificación electrónica o cualquier otro aspecto relacionado con la identidad física, fisiológica, genética, psíquica, económica, cultural o social específica de dicha persona física.

Por "**se procesa**" se entiende cualquier operación o conjunto de operaciones que se llevan a cabo en cualquier dato personal o confidencial de Microsoft, ya sea de forma automatizada o de cualquier otro modo, como son la recopilación, la grabación, la organización, la estructuración, el almacenamiento, la adaptación o la alteración, la recuperación, la consulta, el uso, la distribución o la divulgación de esta debida a su transmisión, así como ponerla a disposición de terceros, su alineación y combinación, su restricción, borrado o destrucción. "Procesamiento" y "procesado" tendrán su significado correspondiente.

"**Procesador**" hace referencia a una persona natural o legal, autoridad pública, agencia u otra entidad que procesa los datos personales en nombre del director.

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección A: Administración		
1	Todo acuerdo aplicable entre Microsoft y el proveedor (por ejemplo, un acuerdo marco, una declaración de trabajo, pedidos de compra y demás pedidos) contiene lenguaje de protección de datos de seguridad y privacidad con respecto a los datos confidenciales y personales de Microsoft, según corresponda. En el caso de las empresas que ejercen de procesadores, el acuerdo debe incluir la materia y la duración del procesamiento, la naturaleza y el propósito del procesamiento, el tipo de datos personales de Microsoft y las categorías de las personas interesadas, y las obligaciones y derechos de Microsoft.	El proveedor debe presentar el contrato pertinente entre Microsoft y el proveedor. Para los procesadores, las descripciones del procesamiento se incluyen en el acuerdo aplicable (*por ejemplo*, una declaración de trabajo, pedidos de compra, etc.). Nota: Las empresas con pedidos de compras en curso pueden tener la descripción necesaria de las actividades de procesamiento añadidas posteriormente en el proceso de compra.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
2	Se debe asignar a una persona o a un grupo específicos de la empresa la responsabilidad y la obligación de rendir cuentas con respecto al cumplimiento del DPR.	El nombre de la persona o grupo encargados de garantizar la conformidad con los DPR de proveedores de Microsoft. Documento en el que se describe la autoridad y responsabilidad de esta persona o grupo, y que demuestra una función de privacidad o seguridad.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
3	Se debe implantar un curso de formación sobre la privacidad y la seguridad para todos aquellos empleados que vayan a tener acceso a los datos personales o confidenciales de Microsoft, mantenerlo y llevarlo a cabo todos los años. Si su empresa no dispone de contenido preparado, puede usar este esquema del guion gráfico y adaptarlo a su empresa.	Los registros anuales de asistencia se encuentran disponibles. El contenido de aprendizaje incluye principios de privacidad y seguridad.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección A: Administración (cont.)		
4	Se deben procesar los datos personales de Microsoft únicamente con arreglo a sus instrucciones documentadas, incluidas las relativas a la transferencia de datos personales a un tercer país o a un organismo internacional, a menos que la ley lo requiera, en cuyo caso, la persona encargada de procesar la información (proveedor) deberá comunicar dicha obligación jurídica a su director (Microsoft) antes de hacerlo, excepto si la ley lo prohíbe por motivos relevantes de interés público.	Pruebas documentadas de dichas instrucciones, según están dispuestas en un contrato (por ejemplo, una declaración de trabajo o un pedido de compra) o su registro como parte de un sistema electrónico que se utilice para la actividad.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
	Sección B: Aviso		
5	El proveedor deberá utilizar la Declaración de privacidad de Microsoft siempre que recopile datos personales en su nombre. Deberán ponerse a disposición de las personas interesadas avisos de privacidad llamativos con el fin de ayudarles a decidir si quieren o no enviar al proveedor sus datos personales. Nota: Si su empresa es el director de la actividad de procesamiento, deberá publicar su propio aviso de privacidad. *Póngase en contacto con SSPAHelp@microsoft.com para acceder a los avisos correctos de Microsoft.*	El proveedor usa un fwdlink para la declaración de aviso de Microsoft actualmente publicada. La declaración de aviso se publica en cualquier contexto en el que se recopilan los datos personales de un usuario. Si procede, hay disponible una versión sin conexión que se facilita antes de la recopilación de datos. Cualquier declaración de privacidad sin conexión utilizada es la versión publicada más reciente y se fecha adecuadamente. Para los servicios de empleados de Microsoft, se utiliza el aviso de protección de datos de Microsoft.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
6	Cuando se recopilan datos personales de Microsoft a través de una llamada de voz en directo, los proveedores tienen la obligación de estar preparados para tratar con la persona interesada sobre las prácticas de recopilación, procesamiento, uso y conservación de datos.	Una secuencia de comandos para grabaciones de voz incluye cómo se procesan los datos, así como ▪ su recopilación, ▪ uso y ▪ retención.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección C: Elección y consentimiento		
7	En caso de que el proveedor se ampare en el consentimiento como fundamento jurídico para el procesamiento de datos, deberá recabar y registrar el consentimiento de la persona interesada para todas las actividades de procesamiento (incluida cualquier actividad nueva y actualizada) antes de recopilar su información personal.	El proveedor puede demostrar cómo una persona interesada da su consentimiento para una actividad de procesamiento y que el alcance de este abarque todas las actividades de procesamiento del proveedor con respecto a los datos personales de las personas interesadas. El proveedor puede demostrar cómo una persona interesada retira su consentimiento para una actividad de procesamiento. El proveedor puede demostrar cómo se comprueban las preferencias antes de lanzar una nueva actividad de procesamiento. El proveedor supervisa la eficacia de administración de preferencias para garantizar el periodo para asignar que un cambio de preferencia es el requisito legal local más restrictivo que se aplica. Nota: La prueba pueden ser capturas de interacción con el usuario, experimentación con el servicio o una oportunidad para ver la documentación técnica.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección C: Elección y consentimiento (cont.)		
8	Las cookies son pequeños archivos de texto que se almacenan en los dispositivos y que provienen de sitios web o aplicaciones en línea. Contienen información que se utiliza para reconocer a una persona interesada o un dispositivo. Los proveedores que se dedican a crear y administrar los sitios web y las aplicaciones de Microsoft deberán proporcionar con claridad a las personas interesadas tanto los avisos como la opción de decidir con respecto al uso de las cookies. Los proveedores que se dedican a crear y administrar los sitios web y las aplicaciones de Microsoft deberán garantizar que el uso de las cookies se ajusta a los compromisos definidos en la Declaración de privacidad de Microsoft y a obligaciones jurídicas locales como las normas establecidas por la UE.	Se deberá documentar la finalidad de todas las cookies e informar del tipo de cookie que se ha implementado. ▪ Las cookies persistentes no se deben usar cuando las cookies de sesión son suficientes. ▪ Cuando se utilizan cookies persistentes, estas no deben tener fecha de caducidad que superen los 2 años después de que un usuario haya visitado el sitio. Para los usuarios de la UE, la fecha de caducidad para una cookie persistente no debe superar los 13 meses. Se debe validar la conformidad con leyes de la UE según proceda, como ▪ el uso de los principios de clasificación "Privacidad y cookies" de la Declaración de privacidad y ▪ garantizar que el usuario ha dado su consentimiento antes de utilizar cookies con fines no esenciales como los de la publicidad.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección D: Recopilación		
9	El proveedor debe supervisar la recopilación de datos personales y confidenciales de Microsoft para garantizar que los únicos datos que se recopilan sean aquellos necesarios para la actividad.	El proveedor puede ofrecer documentación que muestra que los datos personales o confidenciales de Microsoft recopilados son obligatorios para la actividad.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
10	Si el proveedor recopila datos personales de terceros en nombre de Microsoft, está obligado a validar que las directivas y prácticas sobre la protección de datos implantadas por el tercero son conformes a lo estipulado en el contrato del proveedor con Microsoft y a los requisitos de DPR.	El proveedor ofrecer documentación de diligencia debida con respecto a las prácticas y políticas de protección de datos de terceros.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
11	Antes de recopilar datos personales de Microsoft a través de la instalación o del uso de software ejecutable en el dispositivo de la persona interesada, es obligatorio documentar la necesidad de llevar a cabo tal recopilación de datos en un acuerdo de proveedor registrado con Microsoft.	El acuerdo de Microsoft con el uso de software ejecutable en el dispositivo de una persona interesada consta en el contrato ejecutado.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
12	Antes de recopilar datos personales de Microsoft (datos que divulguen su raza u origen étnico, su inclinación política, sus creencias religiosas o filosóficas, su pertenencia a un sindicato, sus datos genéticos, biométricos o relacionados con su salud, así como los datos relacionados con sus preferencias o su vida sexual) es obligatorio documentar la necesidad de llevar a cabo dicha recopilación en un acuerdo de proveedor registrado con Microsoft.	La necesidad de recopilar datos personales de Microsoft confidenciales consta en el contrato ejecutado con Microsoft.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección E: Conservación		
13	Se deberá garantizar que los datos personales y confidenciales de Microsoft no se van a conservar durante más tiempo del que sea necesario para la actividad, a menos que la legislación vigente requiera una conservación prolongada de dichos datos.	El proveedor cumple con los requisitos o las directivas de conservación documentada que Microsoft haya especificado en el contrato (por ejemplo, una declaración de trabajo o un pedido de compra).	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
14	Se deberá garantizar que, a la entera discreción de Microsoft, los datos personales y confidenciales de Microsoft que se halle en manos del proveedor o bajo su control, se devuelve a Microsoft o se destruye tras la finalización de las actividades o a petición de Microsoft. Dentro de las aplicaciones deberán existir procesos para garantizar que se borran de forma totalmente segura aquellos datos que se han eliminado de la aplicación, ya sea por la actuación expresa del usuario o con base en otros elementos desencadenantes como la antigüedad de los datos. En caso de ser necesaria la destrucción de los datos personales y confidenciales de Microsoft, el proveedor tendrá la obligación de quemar, pulverizar o destruir los activos físicos que contengan datos personales o confidenciales de Microsoft de modo que sea imposible leer ni reconstruir dicha información.	Se debe conservar un registro de disposición de datos personales y confidenciales de Microsoft (se puede incluir volver a Microsoft para la destrucción). Si Microsoft requiere o solicita la destrucción, se debe proporcionar un certificado de destrucción firmado por un responsable del proveedor.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección F: Personas interesadas		
	Las personas interesadas tienen derecho a acceder, eliminar, actualizar, exportar, restringir y oponerse al procesamiento de sus datos personales ("**Derechos de la persona interesada**"). Si la persona interesada trata de ejercer sus derechos en relación con sus datos personales de Microsoft de acuerdo con la ley, el proveedor deberá:		
15	Se debe ayudar a Microsoft, en la medida de lo posible y por medio de las medidas técnicas y organizativas adecuadas, a cumplir la obligación de dar respuesta a las solicitudes de las personas interesadas que traten de ejercer sus derechos de personas interesadas.	Existen procesos y procedimientos para poder ejecutar los derechos de las personas interesadas.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
16	Se debe dar respuesta a todas las solicitudes relacionadas con los derechos de las personas interesadas sin demoras injustificadas.	El proveedor deberá llevar a cabo pruebas periódicas para garantizar que puede cubrir las necesidades derivadas de los derechos de las personas interesadas.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
17	El proveedor remitirá directamente a Microsoft a las personas interesadas que contacten con él para ejercer sus derechos de persona interesada, a menos que Microsoft indique lo contrario. El proveedor informará a la persona interesada de los pasos que debe seguir para obtener acceso a los datos personales de Microsoft o para ejercer sus derechos con respecto a esta. *Póngase en contacto con SSPAHelp@microsoft.com si necesita ayuda al respecto.*	El proveedor comunica los pasos necesarios para tener acceso a los datos personales, así como los métodos disponibles para actualizarlos.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
18	Se deberá validar la identidad de la persona interesada que ha presentado la solicitud en caso de responder directamente a esta persona.	El proveedor ha documentado el método utilizado para identificar a las personas interesadas de Microsoft.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección F: Personas interesadas (cont.)		
	Una vez que se ha autenticado a la persona interesada, el proveedor está obligado a lo siguiente:		
19	Se debe determinar si se conservan o controlan datos personales de Microsoft sobre la persona interesada.	El proveedor cuenta con procedimientos para determinar la conservación de los datos personales.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
20	Se debe hacer lo posible por localizar los datos personales de Microsoft solicitados y registrar las acciones llevadas a cabo que demuestren que se ha efectuado una búsqueda razonable.	El proveedor conserva un registro que demuestra los pasos dados para cumplir las solicitudes de derechos de las personas interesadas. En la documentación se incluye ▪ la fecha y la hora de la solicitud, ▪ las acciones tomadas para responder a la solicitud y ▪ el registro de cuándo se informó a Microsoft.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
21	Se debe registrar la fecha y la hora de las solicitudes de derechos de personas interesadas, así como las acciones llevadas a cabo por el proveedor para responder a dichas solicitudes. Si así se le solicita, a proporcionar los registros de las solicitudes de las personas interesadas a Microsoft.	El proveedor conserva registros de las solicitudes de acceso a los datos personales y documenta los cambios efectuados en estos.	
	Una vez que se ha autenticado a la persona interesada y el proveedor ha validado que tiene los datos personales de Microsoft solicitados, el proveedor está obligado a lo siguiente:		
22	Para las solicitudes cuyo fin es obtener una copia de los datos personales, deberá proporcionar a la persona interesada los datos personales de Microsoft en un formato adecuado, ya sea de forma impresa, electrónica o verbal.	El proveedor suministra datos personales a la persona interesada en un formato comprensible y de un modo adecuado tanto para el proveedor como para la persona interesada en cuestión.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección F: Personas interesadas (cont.)		
23	Si se deniega su solicitud por indicación de Microsoft, se debe proporcionar a la persona interesada una explicación por escrito conforme a las instrucciones relevantes que pudiera haber indicado previamente Microsoft. *Póngase en contacto con SSPAHelp@microsoft.com si necesita ayuda al respecto.*	Documentar los casos en los que se deniegan las solicitudes y conservar las pruebas de la revisión y aprobación de Microsoft.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
24	El proveedor debe adoptar las medidas de precaución que sean razonables para garantizar que los datos personales de Microsoft que se faciliten a la persona interesada no puedan usarse para identificar a otra persona distinta.	El proveedor debe demostrar que se adoptan las medidas de precaución razonables que impiden identificar a otra persona a partir de la información facilitada (por ejemplo, no se puede fotocopiar la página de datos en su totalidad cuando los datos personales solicitados por la persona interesada figura en una sola línea).	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
25	Si la persona interesada y un proveedor discrepan sobre la integridad y la precisión de los datos personales de Microsoft, el proveedor debe remitir el problema a Microsoft y prestarle la colaboración necesaria para solucionarlo. *Póngase en contacto con SSPAHelp@microsoft.com si necesita ayuda al respecto.*	El proveedor documenta los casos de desacuerdo y los remite a Microsoft.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección G: Divulgación a terceros		
	En caso de que el proveedor tenga la intención de llevar a cabo el procesamiento de los datos personales o confidenciales de Microsoft a través de un subcontratista, deberá asegurarse de:		
26	Se debe obtener el consentimiento expreso de Microsoft por escrito antes de subcontratar servicios o hacer cambios en cuanto a la incorporación o a la sustitución de subcontratistas. *Póngase en contacto con SSPAHelp@microsoft.com si necesita ayuda al respecto.*	Se debe validar que los datos personales de Microsoft los procesen solo las empresas que para Microsoft son requeridas en el contrato pertinente (por ejemplo: declaración de trabajo, anexo, pedido de compra, etc.) o que se capturan en la base de datos de SSPA.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
27	Se deben documentar la naturaleza y el alcance de los datos personales y confidenciales de Microsoft que van a procesar los subcontratistas y garantizar que la información recopilada es necesaria para llevarlo a cabo.	El proveedor conserva un registro documental de los datos personales y confidenciales de Microsoft divulgados o transferidos a los subcontratistas.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
28	Se debe garantizar que el subcontratista usa los datos personales de Microsoft con arreglo a las preferencias de contacto que han indicado las personas interesadas.	Se debe demostrar cómo los subcontratistas utilizan una preferencia de persona interesada de Microsoft. Se debe ofrecer documentación de ayuda que incluya el periodo en el que un subcontratista asigna un cambio preferencial.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
29	Se debe restringir el procesamiento de los datos personales de Microsoft por parte del subcontratista para aquellos fines que sean necesarios para cumplir con el contrato entre el proveedor y Microsoft.	El proveedor puede ofrecer documentación que muestra que los datos personales de Microsoft suministrados al subcontratista son obligatorios para la actividad.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
30	Se deben revisar las quejas formuladas por el procesamiento de los datos personales de Microsoft de forma ilícita o sin autorización.	El proveedor puede demostrar que hay sistemas y procesos que permiten administrar las quejas relativas a la divulgación o uso no autorizados de los datos personales de Microsoft por parte de un subcontratista.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección G: Divulgación a terceros (cont.)		
31	Se debe notificar a Microsoft, con la mayor brevedad, cuando tenga conocimiento de que un subcontratista ha procesado o divulgado datos personales o confidenciales de Microsoft para fines distintos de aquellos relacionados con la actividad.	El proveedor ha proporcionado las instrucciones y medios para que un subcontratista informe sobre el uso incorrecto de los datos de Microsoft.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
32	Se debe adoptar de inmediato medidas para mitigar cualquier daño, real o posible, que cause el procesamiento o la divulgación (de forma ilícita o sin autorización) por parte de un subcontratista de los datos personales y confidenciales de Microsoft.	El proveedor puede demostrar que tiene un plan y procedimientos en caso de que el subcontratista use incorrectamente los datos personales y confidenciales de Microsoft.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
	Sección H: Calidad		
33	El proveedor debe conservar la integridad de todos los datos personales de Microsoft y garantizar que es precisa, completa y relevante para los fines indicados para los que se ha procesado.	El proveedor puede demostrar que hay procedimientos para validar los datos personales de Microsoft cuando se recopilan, crean y actualizan. El proveedor puede demostrar que hay procedimientos de supervisión y muestreo para comprobar sobre la marcha el nivel de precisión y efectuar las correcciones que resulten necesarias.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección I: Supervisión y cumplimiento		
34	El proveedor tiene un plan de respuesta ante incidentes para el cual debe notificar a Microsoft sin demoras injustificadas si se tiene conocimiento de que se ha producido una vulneración de datos o vulnerabilidad de la seguridad en relación con la administración de los datos personales y confidenciales de Microsoft por parte del proveedor. *Póngase en contacto con SSPAHelp@microsoft.com para informar sobre un incidente.*	El proveedor tiene un plan de respuesta ante incidentes que incluye un paso para notificar a los clientes (Microsoft) según se describe en esta sección.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
35	Hay que abstenerse de emitir notas de prensa o avisos públicos relativos al incumplimiento que suponga una vulneración de datos personales o confidenciales de Microsoft sin contar con la aprobación previa de Microsoft, a menos que lo exija la ley.	El proveedor acepta cumplir este requisito si se da el caso.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
36	Se debe implementar un plan encaminado a solventar el problema y supervisar la resolución de filtraciones o vulnerabilidades relacionadas con datos personales o confidenciales de Microsoft con el fin de garantizar que se adoptan las medidas correctivas en un plazo oportuno.	El proveedor dispone de procedimientos documentados para responder al fin de una vulneración de datos.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
37	Se debe establecer un proceso formal de administración de quejas para dar una respuesta adecuada a todas las quejas sobre protección de datos relacionadas con los datos personales de Microsoft.	El proveedor dispone de los medios para recibir quejas acerca de los datos personales de Microsoft, así como un procedimiento para abordar quejas documentadas.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección J: Seguridad		
	El proveedor debe establecer, aplicar y mantener un programa de seguridad de la información que incluya políticas y procedimientos para proteger los datos personales y confidenciales de Microsoft conforme a las buenas prácticas del sector y tal y como lo exija la ley. El programa de seguridad que utilice el proveedor deberá cumplir con los estándares expuestos más abajo, en los requisitos 38 a 56.	Las medidas de seguridad pueden ser más amplias que las enumeradas si el cumplimiento de las normativas (como HIPPA o GLBA) o las cláusulas contractuales aplicables así lo requiriesen. La sección J puede sustituirse por un informe válido sobre la ISO 27001 o SOC 2. Póngase en contacto con SSPAHelp@microsoft.com para realizar esta sustitución. Nota: Deberá proporcionar documentación en la que se detalle el alcance de estas certificaciones o informes.	
38	Se deben llevar a cabo evaluaciones de seguridad de la red de forma anual que incluyan: ▪ La revisión de los cambios importantes realizados en el entorno, como los nuevos componentes del sistema, los llevados a cabo en la topología de la red o las modificaciones en las reglas de los firewalls ▪ El análisis de vulnerabilidades ▪ La conservación de los registros de cambios	El proveedor ha documentado las evaluaciones de la red, de los registros de cambios y de los resultados de los análisis. Los registros de cambios requeridos deben rastrear los cambios, ofrecer información sobre el motivo del cambio e incluir el nombre y el título del aprobador designado.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
39	El proveedor deberá establecer e implementar una directiva relacionada con los dispositivos móviles, así como informar sobre esta, para garantizar y restringir el uso de los datos personales y confidenciales de Microsoft que se utilizan en un dispositivo móvil o a los que se accede desde este.	El proveedor demuestra el uso de una política conforme sobre los dispositivos móviles en que el procedimiento de datos personales o confidenciales de Microsoft requiere el uso de un dispositivo móvil.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección J: Seguridad (cont.)		
40	Se deberán contabilizar todos los activos implicados en la actividad deberán contar con un propietario reconocido. El proveedor asumirá la responsabilidad de conservar un inventario de estos activos de información, de demostrar que su uso sea razonable y esté autorizado y de proporcionar el nivel de protección oportuno para estos a lo largo de su ciclo de vida.	Inventario de los activos de dispositivos empleados para la actividad. El inventario de los activos deberá incluir: ▪ La ubicación del dispositivo ▪ La clasificación de los datos que se encuentran en el activo ▪ El registro de la recuperación de activos una vez rescindido el contrato laboral o el acuerdo comercial ▪ El registro de la eliminación de los sistemas de almacenamiento de datos una vez dejen de ser necesarios	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección J: Seguridad (cont.)		
41	Se deben implantar y mantener los procedimientos correspondientes a la administración de los derechos de acceso con el fin de evitar el acceso no autorizado a cualquier dato personal y confidencial de Microsoft que se encuentra bajo el control del proveedor.	El proveedor demuestra que ha implementado un plan de administración de derechos de acceso que incluye: ▪ Los procedimientos de control de acceso ▪ Los procedimientos de identificación ▪ Los procedimientos de bloqueo posteriores a los intentos fallidos ▪ El restablecimiento de la contraseña siempre que sea necesario, pero sin superar un periodo de 90 días ▪ Unos parámetros sólidos a la hora de seleccionar las credenciales para la autenticación ▪ La desactivación de las cuentas de usuario dentro de un periodo máximo de 48 horas desde la rescisión del contrato de trabajo El proveedor demuestra que dispone de un proceso establecido para revisar el acceso de usuario a los datos personales y confidenciales de Microsoft por medio de la aplicación del principio de privilegios mínimos. Este proceso incluye: ▪ Una definición clara de los roles de usuario ▪ Los procedimientos dedicados a revisar y justificar la aprobación del acceso a los roles ▪ Verificación de que los usuarios incluidos en los roles que tienen acceso a los datos de Microsoft cuentan con una justificación documentada para pertenecer a dichos grupos o roles	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección J: Seguridad (cont.)		
42	Se deben establecer y aplicar procedimientos para la administración de revisiones que den prioridad a las revisiones de seguridad para aquellos sistemas que se utilicen para procesar los datos personales o confidenciales de Microsoft. Entre estos procedimientos, se incluyen los siguientes: ▪ Definición de un enfoque de riesgos para dar prioridad a las revisiones de seguridad ▪ Capacidad de administrar y aplicar las revisiones de emergencia ▪ Aplicabilidad al sistema operativo y al software de servidor como en el caso del servidor de aplicaciones y el software de base de datos ▪ Documentar el riesgo que mitiga la revisión y llevar a cabo un seguimiento de todas las excepciones ▪ Requisitos para la retirada de software que ya no cuenta con el soporte de la empresa que lo creó	El proveedor puede demostrar un procedimiento implementado de administración de revisiones que cumpla con este requisito y abarque, como mínimo, lo siguiente: ▪ Asignación de gravedad para informar sobre la prioridad (se documentan las definiciones de gravedad) ▪ Procedimiento documentado para implementar revisiones de emergencia ▪ Validación de que no se usan sistemas operativos que ya no disponen de soporte por parte de la empresa que los creó ▪ Registros de administración de revisiones que rastrean aprobaciones y excepciones	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
43	Se debe instalar software antivirus y antimalware en todos los equipos conectados a la red que se utilicen para procesar los datos personales y confidenciales de Microsoft, incluidos los servidores y los equipos de sobremesa de producción y aprendizaje. La finalidad es proteger a los equipos frente a virus y aplicaciones de software potencialmente malintencionados. Se deben actualizar diariamente, o cuando lo sugiera el proveedor del antivirus o del antimalware, las definiciones de antimalware. Nota: Esto se aplica a todos los sistemas operativos, incluido Linux.	Los registros existen para mostrar el uso activo de antivirus y software antimalware. Nota: Este requisito se aplica a todos los sistemas operativos.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
44	Los proveedores que desarrollan software para Microsoft deben incorporar principios de seguridad por diseño en el proceso de creación.	Entre las especificaciones técnicas del proveedor, se incluyen puntos de comprobación para validar la seguridad en los ciclos de desarrollo.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección J: Seguridad (cont.)		
45	Se debe emplear un programa de prevención de pérdida de datos ("**DLP**"). Los datos se deben clasificar, etiquetar y proteger adecuadamente, y el proveedor debe supervisar los sistemas en uso cuando se procesan los datos personales o confidenciales de Microsoft en busca de intrusiones, pérdidas u otras actividades no autorizadas. Como mínimo, el programa DLP: ▪ requiere el uso de sistemas de detección de intrusiones ("**IDS**") de normalización industrial basados en el host, la red y la nube si se conservan los datos personales o confidenciales de Microsoft. ▪ requiere la implementación de sistemas de detección de intrusiones ("**IPS**") avanzados y configurados para supervisar y detener las pérdidas de datos de forma activa. ▪ requiere el análisis del sistema (en caso de que este sufra una infracción) para garantizar que se tratan también todas las vulnerabilidades residuales. ▪ describe los procedimientos requeridos cuyo fin es supervisar las herramientas de detección de riesgos en el sistema. ▪ establece un proceso de respuesta ante incidentes y administración que debe llevarse a cabo cuando se detectan eventos de vulneraciones de datos.	Sistemas IDS/IPS documentados e implementados con procedimientos listos para responder directamente al detectar vulnerabilidad o vulneraciones de datos.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
46	Se deben comunicar de inmediato los resultados de las investigaciones sobre la respuesta a incidentes a la administración sénior y a Microsoft. *Póngase en contacto con SSPAHelp@microsoft.com para informar a Microsoft.*	Existen sistemas y procesos para comunicar a Microsoft los resultados de las investigaciones sobre las respuestas ante incidentes.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección J: Seguridad (cont.)		
47	Deberán llevar a cabo cada año un curso de formación sobre seguridad los administradores de sistemas, los empleados del departamento de operaciones, la dirección y terceras partes.	Se deberá crear un programa de formación sobre seguridad que incluya: ▪ Formación anual sobre respuesta ante incidentes ▪ Simulaciones de incidentes y mecanismos automatizados para facilitar una respuesta eficaz ante las situaciones de crisis Concienciación sobre la prevención de incidentes como los riesgos relacionados con la descarga de software malintencionado	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
48	El proveedor debe garantizar que existen procesos de planificación de copia de seguridad para proteger los datos personales y confidenciales de Microsoft frente al uso, acceso, divulgación, alteración y destrucción no autorizados.	El proveedor puede demostrar los procedimientos de respuesta y de recuperación detallando cómo actuaría la empresa a la hora de administrar un incidente perturbador y cómo conservaría un nivel de seguridad predeterminado para la información 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 crear copias de seguridad de los datos críticos, almacenarlos de forma segura y recuperarlos eficazmente, todo ello de forma regular.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección J: Seguridad (cont.)		
49	Se debe crear y verificar la continuidad del negocio y los planes de recuperación ante desastres.	Los planes de recuperación ante desastres deben incluir: ▪ Los criterios fijados para decidir si un sistema es vital para el funcionamiento del negocio del proveedor ▪ Una lista con los sistemas que se consideran vitales según los criterios fijados y que deberán ser objeto de la recuperación en caso de desastre ▪ Los procedimientos de recuperación ante desastres definidos para todos los sistemas críticos que garanticen que un ingeniero que no conozca el sistema será capaz de recuperar la aplicación en un plazo máximo de 72 horas ▪ Verificación y revisión anual (o con mayor asiduidad) de los planes de recuperación ante desastres que garantice que se cumplan los objetivos de recuperación	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección J: Seguridad (cont.)		
50	El proveedor debe autenticar la identidad de una persona antes de concederle acceso a datos personales y confidenciales de Microsoft.	Se deberá garantizar que los identificadores de usuario son únicos y que todos emplean un método de autenticación estándar del sector, como Azure Active Directory. El acceso con privilegios elevados (privilegios de tipo administrativo o mejoras de cualquier otro tipo) deberá ir acompañado de un segundo factor, como una tarjeta inteligente o un autenticador telefónico.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
51	El proveedor debe proteger la información personal y confidencial de Microsoft que se transmita entre redes a través del cifrado Seguridad de la capa de transporte ("**TLS**") o del protocolo de seguridad de Internet ("**IPsec**"). Estos métodos están establecidos en las normas NIST 800-52 y NIST 800-57. Existe la posibilidad de ajustarse a otros estándares equivalentes del sector. El proveedor no puede facilitar ningún dato personal o confidencial transmitido sin el uso del cifrado.	Se deberá establecer y respetar el proceso que se utilice para crear, desplegar y sustituir el certificado TLS o cualquier otro.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
52	Todos los dispositivos del proveedor (portátiles, estaciones de trabajo, etc.) que vayan a tener acceso o vayan a administrar datos personales y confidenciales de Microsoft deberán utilizar el cifrado basado en disco.	Se deberán cifrar todos los dispositivos para cumplir los criterios de Bitlocker o de cualquier otra solución de cifrado en disco equivalente del sector, en todos los dispositivos cliente que se empleen para administrar datos personales y confidenciales de Microsoft.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección J: Seguridad (cont.)		
53	Debe haber sistemas y procedimientos (que usen estándares del sector actuales como los descritos en la normativa NIST 800-111) con los que cifrar todos los datos personales o confidenciales de Microsoft en reposo (si están almacenados), incluidos los siguientes: ▪ Datos de credenciales (por ejemplo, nombres de usuario o contraseñas) ▪ Datos de los instrumentos de pago (por ejemplo, los números de las tarjetas de crédito o los números de la cuenta bancaria) ▪ Datos personales relacionados con la inmigración ▪ Datos de historiales médicos (por ejemplo: números de historiales médicos, o identificadores o marcadores biométricos, como ADN, huellas dactilares, retina e iris, patrones de voz, patrones faciales y medidas de la mano, empleados para la autenticación) ▪ Datos de identificador expedidos desde el Gobierno (por ejemplo, el número de la seguridad social o del carné de conducir) ▪ Datos pertenecientes a clientes de Microsoft (por ejemplo: Sharepoint, documentos O365, clientes de OneDrive) ▪ Material relacionado con productos de Microsoft no anunciados ▪ Fecha de nacimiento ▪ Información de perfil de hijos ▪ Datos geográficos en tiempo real ▪ Dirección personal física (no empresarial) ▪ Números de teléfono personales (no empresariales) ▪ Religión ▪ Opiniones políticas ▪ Orientación o preferencia sexual ▪ Respuestas a las preguntas de seguridad (por ejemplo: autenticación de dos fases, restablecimiento de contraseña) o Apellido de soltera de la madre	Compruebe que los datos personales y confidenciales de Microsoft en esta fila se cifran en reposo.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*

N.º	Requisitos de protección de datos para proveedores de Microsoft	Prueba de conformidad	Respuesta
	Sección J: Seguridad (cont.)		
54	A la hora de procesar tarjetas de crédito en nombre de Microsoft se deberá cumplir con los estándares de procesamiento de tarjetas de crédito aplicables de cada entidad emisora.	Se debe demostrar todos los años el cumplimiento de estos por medio de la certificación del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago ("**PCI-DSS**"). *Se deben enviar las certificaciones PCI DSS al SSPA. Póngase en contacto con SSPAHelp@microsoft.com* si tiene alguna pregunta.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
55	El proveedor debe almacenar activos físicos de Microsoft en un entorno de acceso controlado.	Deben existir sistemas y procesos que permiten administrar el acceso físico a las copias digitales, impresas, de archivo y de copia de seguridad que contienen los datos de Microsoft. Se deberá supervisar la cadena de custodia cuando se realicen movimientos o se destruyan los soportes físicos que contienen datos de Microsoft.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*
56	Se debe dar un tratamiento de anonimato a todos los datos personales de Microsoft que se usen en entornos de desarrollo o prueba.	Los datos personales de Microsoft no deben usarse en entornos de desarrollo o prueba; si no existiera otra alternativa, se garantizará su anonimato para evitar la identificación de las personas interesadas o el uso inapropiado de los datos personales. Nota: Los datos anonimizados son diferentes de los datos pseudonimizados. Los datos anonimizados son datos que no están relacionados con una persona natural identificada o identificable si la persona interesada de los datos personales no es identificable o ha dejado de serlo.	*<Conforme>* *<No conforme>* *<No aplicable>* *<Conflicto legal>* *<Conflicto contractual>*