Servicio de adquisiciones de Microsoft

Guía del programa “Garantía de la seguridad y privacidad del proveedor” (Supplier Security & Privacy Assurance, o SSPA)

Versión 9

Octubre de 2023

Índice

Introducción

En Microsoft creemos que la privacidad es un derecho fundamental. A fin de cumplir con nuestra misión de empoderar a las personas y las organizaciones para que obtengan mayores logros, trabajamos a diario con el objetivo de merecer y mantener la confianza de nuestros clientes.

Las buenas prácticas de seguridad y privacidad son críticas para nuestra misión, esenciales para la confianza de los clientes y, en varias jurisdicciones, un requisito legal. Las normas incluidas en las políticas de privacidad y seguridad de Microsoft reflejan nuestros valores como empresa y se hacen extensivas a nuestros proveedores (como su empresa) que tratan datos de Microsoft en nuestro nombre.

El programa "Garantía de seguridad y privacidad del proveedor" (Supplier Security and Privacy Assurance, o **SSPA**) es el programa corporativo de Microsoft que contiene las instrucciones básicas para el tratamiento de los datos que Microsoft ofrece a los proveedores en forma de "Requisitos de protección de datos" (Data Protection Requirements, o **DPR**), el cual puede consultarse en Microsoft.com/Procurement.. Se debe tener en cuenta que, independientemente de la SSPA, los proveedores podrían estar sujetos a otros requisitos organizativos establecidos y comunicados por el grupo de Microsoft responsable de la interacción con el proveedor.

Los términos clave de la SSPA están definidos en los DPR. Para obtener más información sobre el programa, consulte nuestras Preguntas más frecuentes (P+F) o comuníquese con nuestro equipo de asistencia global al correo electrónico SSPAHelp@microsoft.com.

Información general sobre el programa SSPA

El programa SSPA es una alianza entre los grupos de Adquisiciones, de Asuntos legales y externos corporativos, y de Seguridad corporativa de Microsoft con el objetivo de garantizar que los proveedores respeten los principios de seguridad y privacidad.

El SSPA es un programa global que cubre a los proveedores que tratan Datos Personales o Confidenciales de Microsoft 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**).

Los proveedores pueden seleccionar Perfiles de Tratamiento de Datos que se adecuen a los bienes y servicios contratados. Dichas selecciones van a determinar los requisitos que correspondan para proporcionar a Microsoft las garantías de cumplimiento.

Los proveedores que participen en el programa deberán completar una autocertificación de cumplimiento de los DPR cada año. El Perfil de Tratamiento de Datos elegido determinará si corresponde la totalidad de los DPR o si se deberá aplicar un subgrupo de requisitos más reducido. Los proveedores que procesan lo que Microsoft considera datos de mayor riesgo posiblemente

deban cumplir requisitos adicionales, tal como una verificación de cumplimiento independiente (consulte la Evaluación independiente). Aquellos proveedores que integren la lista de Subencargados publicada por Microsoft también deberán presentar una verificación de cumplimiento independiente.

Importante: Las actividades de cumplimiento determinarán si el proveedor tiene un estado de cumplimiento de la SSPA Verde (conforme) o Rojo (no conforme). Las herramientas de compra de Microsoft validan el estado Verde de cumplimiento de la SSPA (de cada proveedor dentro de su alcance) antes de autorizar la interacción.

Diagrama del proceso de SSPA – Inscripción de nuevo proveedor

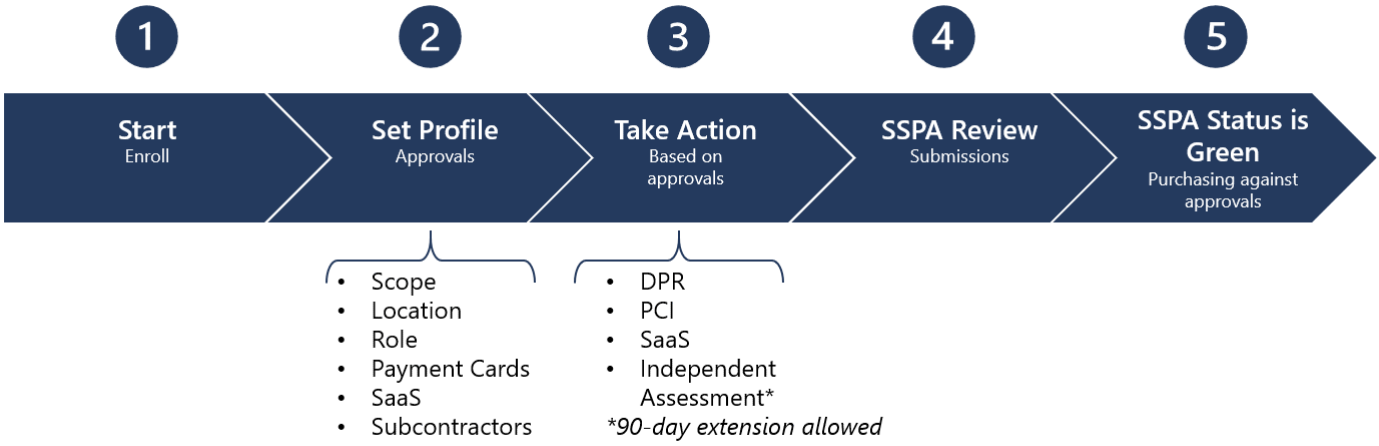
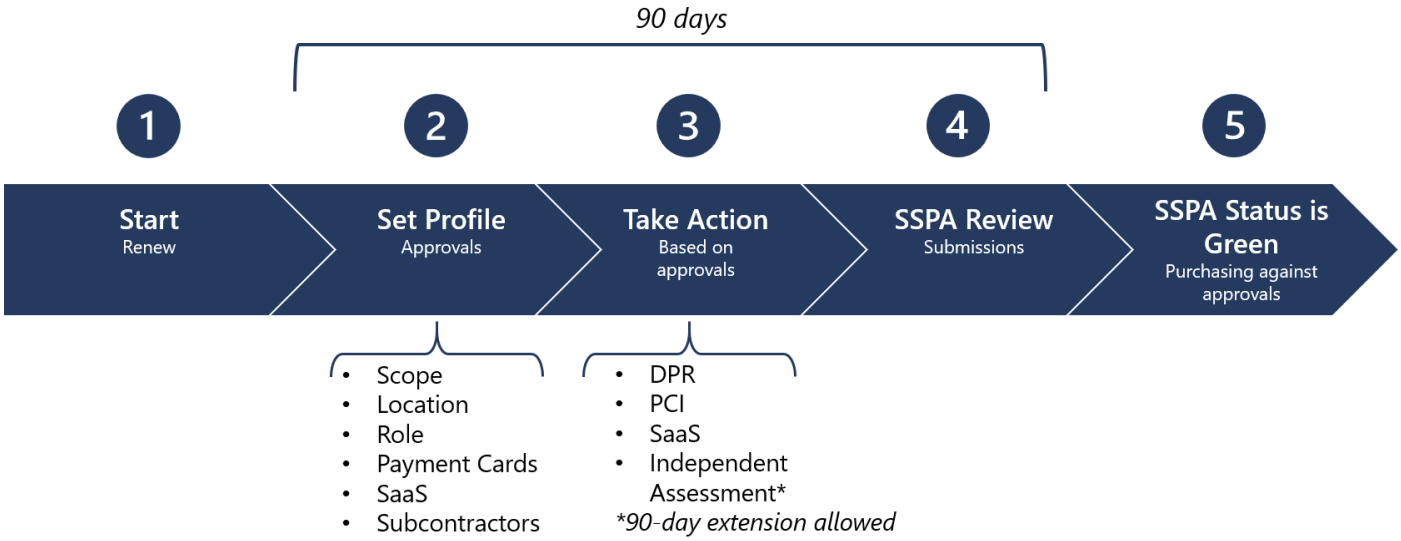


Diagrama del proceso de SSPA – Renovación anual de proveedor



Alcance de la SSPA

A fin de ayudar a determinar si usted (el proveedor) lleva a cabo el Tratamiento de Datos Personales y/o Datos Confidenciales de Microsoft, consulte la lista de ejemplos de las siguientes tablas. Hay que tener en cuenta que estos son solo algunos ejemplos y no una lista exhaustiva.
Nota: Todo propietario de un negocio de Microsoft puede solicitar su remoción de esta lista en caso de que los datos tratados sean de naturaleza confidencial.

Datos personales por tipo de datos

Los ejemplos incluyen, entre otros:

Datos sensibles
Datos relacionados con niños
Información genética, biométrica o médica
Origen racial o étnico
Creencias, opiniones o afiliaciones políticas, religiosas o filosóficas
Pertenencia a sindicatos
Vida u orientación sexual de personas físicas
Situación migratoria (visa, permisos de trabajo, etc.)
Documentación de identificación expedidos por el gobierno (pasaportes, licencias de conducir, visas, números de la seguridad social, números nacionales de identidad)
Datos de ubicación precisa del usuario (en un rango de 300 metros)
Números de cuentas bancarias personales
Número de tarjeta de crédito y fecha de caducidad; **o** código de seguridad/acceso o contraseña/credenciales que permiten el acceso a una cuenta
Información seudonimizada de usuario final (EUPI, por su sigla en inglés) (identificadores creados por Microsoft para identificar a sus usuarios de productos y servicios) • Identificador global único (GUID, por su sigla en inglés) • ID de usuario de Passport o Identificador único (PUID, por su sigla en inglés) • Información sobre seudónimos de usuario final con Hash (EUII, por su sigla en inglés) • ID de sesión • ID de dispositivo • Datos de diagnósticos • Datos de ingreso • Datos de clientes relacionados con casos de asistencia al cliente

Datos capturados y generados
Datos de ubicación imprecisa
Dirección IP
Preferencias y personalización de dispositivos
Uso de servicios en sitios web, rastreo de clics en páginas web
Datos sobre redes sociales, relaciones del grafo social
Datos de actividad de dispositivos conectados, como monitores de actividad física
Datos de contacto tales como nombre, dirección, número telefónico, dirección de correo electrónico, fecha de nacimiento, datos de las personas dependientes y contactos de emergencia
Evaluaciones de riesgo y fraudes, verificación de antecedentes
Información sobre seguros, pensiones, prestaciones
Currículums de candidatos, notas y comentarios de entrevistas
Metadatos y telemetría
Datos de cuenta
Datos sobre instrumentos de pago
Números de tarjeta de crédito y fecha de vencimiento
Datos para transferencias bancarias
Números de cuentas bancarias
Solicitudes de crédito o líneas de crédito
Documentos fiscales y de identificación
Datos sobre inversiones o gastos
Tarjetas corporativas
Datos de clientes en línea
Cliente empresarial en línea de Microsoft (inquilino de Azure, inquilino de M365, etc.)
Cliente de consumo de Microsoft (Xbox Live, OneDrive Consumer)
Cliente empresarial de Microsoft (cliente local)
Datos de soporte (el cliente origina un ticket)
Datos de la cuenta (datos de facturación, comercio electrónico)
Encuesta/registro en eventos/capacitación

Información médica protegida
Números de identificación nacional (incluidos los números tribales y los números de identificación de información médica)
Datos demográficos utilizados en un contexto de información médica protegida (PHI): • Fecha de nacimiento • Género • Etnia • Datos biométricos • Fotografías de la cara completa • Dirección (completa o parcial) • Información de contacto • Información de contacto de emergencia

Datos confidenciales de Microsoft

Los ejemplos incluyen, entre otros:

Altamente confidencial
Información relacionada con el desarrollo, prueba o fabricación de productos Microsoft o sus componentes *Todo software de Microsoft, servicio en línea o hardware comercializado a través de cualquier canal se considera un "**Producto de Microsoft**"* **Nota:** Para el desarrollo de productos de videojuegos, el propietario de un negocio de Microsoft puede indicar si el producto de trabajo debe tener una Clasificación de datos altamente confidencial o confidencial.
Información de marketing previa al lanzamiento de un dispositivo Microsoft
Información financiera corporativa de Microsoft no anunciada sujeta a la normativa de la SEC
Confidencial
Claves de licencias de productos Microsoft en nombre de Microsoft para distribución por cualquier medio
Información relacionada con el desarrollo o prueba de aplicaciones de líneas de negocios internas (LOB, por su sigla en inglés) de Microsoft
Materiales de marketing previos al lanzamiento de software y servicios de Microsoft como Office, SQL, Azure, etc.
Documentación escrita, de diseño, electrónica o impresa de cualquier servicio o producto de Microsoft, tal como dispositivos (guías de proceso o procedimiento, datos de configuración, etc.)

Importante: Todo propietario de un negocio de Microsoft podrá solicitar su participación en relación con datos no incluidos en esta lista.

Perfil de Tratamiento de Datos

Los proveedores de Microsoft tienen control sobre sus Perfiles de Tratamiento de Datos de SSPA.

Esto les permite decidir para qué interacciones desean postularse. Deben prestar especial atención a las selecciones y tener en cuenta la actividad de cumplimiento que se deberá completar para obtener la aprobación. **Véase la sección "Requisitos de garantía" a continuación y el Apéndice A**.

Los grupos comerciales de Microsoft solo podrán crear interacciones con proveedores para los cuales la actividad de tratamiento de datos coincida con las aprobaciones obtenidas.

Los proveedores podrán actualizar su Perfil de Tratamiento de Datos en cualquier momento del año **en caso de no haber tareas abiertas**. Cuando haya una modificación, se emitirá la actividad correspondiente, la cual deberá completarse antes de obtener las aprobaciones. Las aprobaciones existentes y completadas continuarán vigentes hasta que se completen los nuevos requisitos emitidos.

Si las tareas nuevas no se completan dentro del período de 90 días permitido, el estado de la SSPA pasará a Rojo (no conforme) y la cuenta correrá el riesgo de ser desactivada en el sistema de cuentas por pagar de Microsoft.

Aprobaciones para el tratamiento de datos	
1	Alcance del tratamiento de datos ▪ Confidencial ▪ Personal, confidencial
2	Ubicación del tratamiento de los datos ▪ En Microsoft o el Cliente ▪ En el Proveedor
3	Función del tratamiento de datos ▪ Responsable del Tratamiento ▪ Encargado ▪ Subencargado (designado por Microsoft)
4	Procesamiento de tarjetas de pago ▪ Sí ▪ No corresponde
5	Software como Servicio ▪ Sí ▪ No corresponde
6	Uso de Subcontratistas ▪ Sí

	▪ No corresponde

Consideraciones sobre la homologación y el perfil

Alcance del tratamiento de datos

Confidencial

Seleccione esta aprobación si la Actividad del proveedor involucrará el Tratamiento únicamente de Datos Confidenciales de Microsoft.

En caso de seleccionar esta aprobación, el proveedor no podrá solicitar interacciones para el Tratamiento de Datos Personales.

Personal, confidencial

Seleccione esta aprobación si la Actividad del proveedor involucrará el Tratamiento de Datos Personales y Datos Confidenciales de Microsoft.

Ubicación del Tratamiento de los datos

En Microsoft o el Cliente

Seleccione esta aprobación si la Actividad del proveedor involucrará el Tratamiento de datos dentro del entorno de red de Microsoft en el cual el personal use credenciales de acceso *@microsoft.com* o en el entorno del cliente de Microsoft.

No seleccione esta opción en las siguientes circunstancias:

- El proveedor administra un centro en el extranjero designado por Microsoft (OF, por su sigla en inglés).
- El proveedor suministra recursos a Microsoft y eventualmente trabaja dentro y fuera de la red de Microsoft. Para trabajos fuera de la red, la ubicación del tratamiento se considerará como la opción “en el Proveedor”.

En el Proveedor

Si la condición “En Microsoft o el Cliente” (según se describió anteriormente) no es aplicable, se deberá seleccionar esta opción.

Función del tratamiento de datos

Responsable del Tratamiento

Seleccione esta aprobación si **todos** los aspectos de las Actividades del proveedor cumplen con la definición de la función de tratamiento de datos del Responsable del Tratamiento (consulte los DPR).

En caso de seleccionar esta aprobación, el proveedor no podrá solicitar interacciones de tratamiento de Datos Personales dentro de la función "Encargado". Si el proveedor es tanto Encargado como Responsable del Tratamiento para Microsoft, no seleccione Responsable del Tratamiento, sino Encargado.

Encargado

Esta es la función de tratamiento de datos más común cuando el proveedor hace el Tratamiento de datos en nombre de Microsoft. Se debe revisar la definición de Encargado en los DPR.

Subencargado

Los proveedores no pueden identificarse a sí mismos como Subencargados en Microsoft porque ello requiere la aprobación previa de los equipos internos de Privacidad. Se debe revisar la definición de Subencargado en los DPR. Los Subencargados tendrán un contrato adicional y otros requisitos de cumplimiento, incluyendo un Addendum de Protección de Datos y una evaluación independiente (véase más adelante).

Procesamiento de tarjetas de pago

Seleccione esta aprobación si alguna parte de los datos tratados por el proveedor incluye información de soporte para el procesamiento de tarjetas de crédito u otras tarjetas de pago en nombre de Microsoft.

Esta aprobación permite al proveedor tener interacciones relativas al procesamiento de tarjetas de pago.

Software como Servicio (SaaS)

El Software como Servicio (SaaS) permite a los usuarios conectarse y usar en Internet aplicaciones basadas en la nube. Para fines del cumplimiento de la SSPA, se debe considerar el SaaS en forma amplia a fin de incluir la Plataforma como Servicio (PaaS) y la Infraestructura como Servicio (IaaS). (Para obtener más detalles sobre SaaS, consulte la siguiente explicación.)

Microsoft define el **Software como Servicio (SaaS)** como el software basado en un código común bajo un modelo "uno a varios" con pago por cada uso o como suscripción basada en métricas de uso. El proveedor del servicio de la nube desarrolla y hace el mantenimiento del software basado en la nube, ofrece actualizaciones automáticas y lo pone a disposición de sus clientes a través de internet bajo un formato "uno a varios" o "pague por lo que usa". Este método de entrega de software y licencias da acceso en línea a través de una suscripción en lugar de tener que comprarlo e instalarlo en cada computadora individualmente.

Nota: La mayoría de los proveedores de SaaS deberán tener una aprobación como Subcontratista en el portal de Cumplimiento de Proveedores de Microsoft en caso de que la información de los Datos

Personales o los Datos Confidenciales de Microsoft se alojen en la plataforma de algún tercero o en un proveedor de infraestructura en la nube.

Alojamiento de sitios web

Seleccione esta opción de perfil si el proveedor aloja sitios web en nombre de Microsoft (consulte las definiciones en los DPR).

Uso de Subcontratistas

Seleccione esta aprobación si el proveedor utiliza Subcontratistas para la Realización de las Actividades (consulte las definiciones en los DPR).

Los Freelancers también están incluidos en esta categoría (consulte los DPR).

Atención médica

Seleccione esta opción de perfil si el proveedor está obligado a procesar información médica protegida (consulte las definiciones en los DPR).

Requisitos de garantía

Requisitos según las aprobaciones de los perfiles

Las aprobaciones seleccionadas en su Perfil de Tratamiento de Datos ayudan a la SSPA a evaluar el nivel de riesgo en todas las interacciones que usted tiene con Microsoft. Los requisitos de cumplimiento de la SSPA difieren según el Perfil de Tratamiento de Datos y las aprobaciones relacionadas con él. Esta sección explica los diferentes requisitos de la SSPA.

También hay combinaciones que podrían incrementar o reducir los requisitos de cumplimiento. Estas combinaciones están detalladas en el Apéndice A y constituyen aquello que se puede ejecutar en el portal de Cumplimiento de Proveedores de Microsoft tras completar el perfil. Siempre se puede validar la forma en la cual la situación del proveedor se adapta a este marco solicitando una revisión al equipo de SSPA.

Qué hacer: Encontrar el perfil de aprobaciones en el Apéndice A y revisar los requisitos de garantía pertinentes y las opciones de garantía independiente, en su caso.

Importante: Si su perfil incluye Software como Servicio (SaaS), Subcontratistas, alojamiento de sitios web o tarjetas de pago, deberá contar con garantías adicionales.

Autocertificación de cumplimiento de los DPR

Todos los proveedores inscritos en el SSPA deben cumplimentar una autocertificación de cumplimiento de los DPR en un plazo de 90 días a partir de la recepción de la solicitud. Esta solicitud se facilitará anualmente, pero puede ser más frecuente si el Perfil de Tratamiento de Datos se actualiza a mitad de año. El estado de la SSPA en las cuentas de los proveedores cambiará a Rojo (no conforme) en caso de que se exceda dicho plazo de 90 días. Las compras nuevas comprendidas dentro del alcance de la SSPA no podrán procesarse hasta tanto el estado cambie a Verde (conforme).

Los proveedores nuevos deberán completar los requisitos a fin de obtener el estado Verde (conforme) de la SSPA antes de comenzar con las interacciones.

Importante: El equipo de SSPA no está autorizado a otorgar prórrogas para esta tarea.

Los proveedores deberán responder a todos los requisitos de los DPR aplicables según el Perfil de Tratamiento de Datos. Es de esperar que, dentro de los requisitos emitidos, algunos no se apliquen a los bienes o servicios que el proveedor suministra a Microsoft. Pueden marcarse como "no aplicable" con un comentario detallado para que los revisores de la SSPA lo validen.

El equipo del programa SSPA revisa la información de los DPR enviada para verificar si se ha seleccionado “no aplicable”, “conflicto legal local” o “conflicto contractual” en los requisitos. El equipo de la SSPA podrá solicitar la aclaración sobre una o varias selecciones. Los conflictos legales locales y contractuales solo se aceptan si contienen referencias de respaldo y el conflicto es evidente.

Los representantes autorizados que completen la autocertificación deberán asegurarse de contar con la suficiente información específica sobre el tema para responder a cada requisito con solvencia. Asimismo, el hecho de agregar su nombre al formulario de SSPA implica certificar que han leído y entendido los DPR. Los proveedores pueden agregar otros contactos en la herramienta en línea para obtener asistencia al momento de completar los requisitos.

El Representante Autorizado (consulte la definición en los DPR) deberá:

1. Determinar qué requisitos son aplicables.
2. Publicar una respuesta a cada requisito aplicable.
3. Firmar y enviar la certificación en el portal de Cumplimiento de Proveedores de Microsoft.

Nota: La SSPA podrá solicitar pruebas colaboradoras del cumplimiento de un determinado Requisito de Protección de Datos para respaldar las declaraciones de cumplimiento.

Requisito de evaluación independiente

Consulte los “Requisitos por aprobaciones” que se encuentran en el Apéndice A con el fin de conocer cuáles son las aprobaciones del tratamiento de datos que exigen el cumplimiento de este requisito.

Los proveedores pueden optar por cambiar las aprobaciones actualizando su Perfil de Tratamiento de Datos. Sin embargo, si el proveedor tiene la función de “Subencargado” del Tratamiento de Datos, no

podrá cambiar esta aprobación y deberá llevar a cabo una evaluación independiente cada año.

Para obtener las aprobaciones que requieren verificación de cumplimiento independiente, los proveedores deberán elegir a un evaluador independiente para validar el cumplimiento de los DPR. Este evaluador deberá redactar una carta dictamen que ofrezca garantías de cumplimiento a Microsoft. Dicha carta dictamen deberá hacerse sin reservas y todos los puntos no conformes deberán estar resueltos y subsanados antes de que la carta de confirmación sea enviada a través del portal de Cumplimiento de Proveedores de Microsoft para la revisión del equipo del programa SSPA. Los evaluadores podrán descargar un modelo aprobado de carta dictamen, que se adjunta al PDF "Evaluadores preferidos", disponible aquí.

El **Apéndice A** incluye alternativas de certificación aceptadas si se opta por no usar un evaluador independiente para verificar el cumplimiento de los DPR (cuando corresponda, como en el caso de los proveedores de SaaS, proveedores de alojamiento de sitios web o proveedores con Subcontratistas). Las certificaciones ISO 27701 (privacidad) e ISO 27001 (seguridad) se pueden tomar como base o punto de referencia, ya que consideran en forma minuciosa los DPR.

En los casos en los que el proveedor brinda servicios de salud en los Estados Unidos o es una entidad incluida en el alcance, se acepta el informe HITRUST para cobertura de privacidad y seguridad.

Si las circunstancias que van más allá de los desencadenantes estándar justifican una diligencia debida adicional, la SSPA puede requerir una evaluación independiente sin tener en cuenta el Perfil de Tratamiento de Datos. Algunos ejemplos son: solicitud de privacidad o seguridad de la división; la validación de la subsanación de incidentes de datos; o un requerimiento de ejecución automatizada de los derechos del interesado.

Guía para cumplir este requisito:

1. La interacción la debe efectuar un evaluador que cuente con la suficiente capacitación técnica y conocimiento del tema para evaluar adecuadamente el cumplimiento.
2. Los evaluadores deberán estar afiliados a la Federación Internacional de Contadores (International Federation of Accountants, IFAC) o en el Instituto Estadounidense de Contadores Públicos Certificados (American Institute of Certified Public Accountants, AICPA) o contar con certificaciones de otras organizaciones relevantes sobre privacidad y seguridad, como la Asociación Internacional de Profesionales de la Privacidad (International Association of Privacy Professional, IAPP) o la Asociación para la Auditoría y el Control de Sistemas Informáticos (Information Systems Audit and Control Association, ISACA).
3. El evaluador debe utilizar los DPR vigentes que incluyan la evidencia que debe presentarse como respaldo para cada requisito. **Los proveedores deberán proporcionarle al evaluador las respuestas de certificación de los DPR más recientemente aprobadas.**
4. En el caso de proveedores nuevos, el evaluador deberá probar el diseño de los controles de procesos. En todos los demás casos, el evaluador comprobará la eficacia de los controles.
5. El alcance de la interacción de evaluación se limita a Datos Personales y/o Datos Confidenciales de Microsoft relativos a la Actividad del proveedor.
6. El alcance de la interacción se limita a toda actividad pertinente de tratamiento de datos que se lleve a cabo en relación con el número de cuenta de proveedor que recibió la solicitud. Si el

proveedor opta por tener más de una cuenta de proveedor al mismo tiempo, la **carta de certificación deberá incluir la lista de cuentas de proveedor incluidas en la evaluación y las direcciones relacionadas con ellas.**

7. La carta enviada al programa SSPA no debe incluir ninguna declaración que implique que el proveedor no cumple con los Requisitos de Protección de Datos allí descritos. Estas cuestiones se deberán corregir antes de enviar la carta.

El programa SSPA tiene disponible una lista de evaluadores preferidos. Estas empresas están familiarizadas con las evaluaciones de la SSPA. Los proveedores deberán pagar esta evaluación, y los costos varían según la escala y el alcance del tratamiento de datos.

Requisito de certificación de la "Norma de seguridad de datos para la industria de tarjetas de pago" [PCI DSS]

La "Norma de seguridad de datos para la industria de tarjetas de pago" (PCI DSS, por sus siglas en inglés) es el marco para el desarrollo de una robusta seguridad de los datos de las tarjetas de pago que incluye prevención, detección y la adecuada reacción ante los incidentes de seguridad. Este marco fue desarrollado por el Consejo sobre Normas de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés), un organismo autónomo de la industria. El objetivo de los requisitos PCI DSS es identificar las vulnerabilidades de la tecnología y los procesos que ponen en riesgo la seguridad del titular de la tarjeta que se procesa.

Microsoft tiene la obligación de cumplir con estas normas. Si un proveedor gestiona información de tarjetas de pago en nombre de Microsoft, necesitamos contar con pruebas de su adhesión a estas normas. Consulte el sitio del Consejo sobre normas de seguridad de la industria de tarjetas de pago (PCI) para conocer los requisitos establecidos por el organismo de la industria de tarjetas de pago (PCI).

Dependiendo del volumen de transacciones procesadas, el proveedor deberá contratar a un Evaluador de seguridad calificado para que certifique el cumplimiento de la seguridad o responder un formulario del cuestionario de autoevaluación.

Las marcas de las tarjetas de pago establecen los requisitos mínimos para el tipo de evaluación, y en general son los siguientes:

- Nivel 1: presentar un certificado de cumplimiento de la industria de tarjetas de pago de un evaluador independiente (3rd Party Assessor PCI AOC).
- Nivel 2 o 3: presentar un cuestionario de autoevaluación sobre las normas de seguridad de datos para la industria de tarjetas de pago (PCI DSS Self-Assessment Questionnaire; SAQ) firmado por un directivo del proveedor.

Se deberá presentar la certificación pertinente que cumpla con los requisitos de la industria de tarjetas de pago (PCI). Los proveedores que procesen o almacenen datos de pago de clientes de Microsoft deben tener una certificación PCI de nivel 1 vigente como proveedor de servicios.

Requisitos del Software como Servicio

Los proveedores que cumplan con la definición de SaaS incluida en el Perfil de Tratamiento de Datos podrían tener que presentar una certificación ISO 27001 válida, si el "Contrato de servicios en la nube" de Microsoft así lo estipulara.

Los revisores de la SSPA validarán que la información enviada cumpla con esta obligación contractual.

Le pedimos no enviar certificaciones de centros de datos. Únicamente se acepta la certificación ISO 27001 aplicable a los servicios de software especificados en el contrato celebrado con Microsoft.

Uso de Subcontratistas

Microsoft considera que el uso de Subcontratistas es un factor de alto riesgo. Los proveedores que utilicen Subcontratistas para el Tratamiento de Datos Personales y/o Confidenciales de Microsoft deberán proporcionar la información de dichos Subcontratistas. Asimismo, el proveedor deberá informar en qué países tratará dichos datos personales cada Subcontratista.

Incidentes de Datos

En caso de que un proveedor tenga conocimiento de algún incidente en relación con la privacidad o seguridad de los datos, deberá informarlo a Microsoft según lo detallado y definido en los DPR.

Cualquier incidente de datos deberá reportarse a través del sitio SupplierWeb o al correo electrónico SuppIR@microsoft.com.

Asegúrese de incluir:

- Fecha del Incidente de Datos
- Nombre del proveedor
- Número de proveedor
- Contacto(s) de Microsoft notificado(s)
- Orden de Compra (PO, por sus siglas en inglés) aplicable, si corresponde o está disponible
- Resumen del Incidente de Datos

Apéndice A

Requisitos según las aprobaciones de los perfiles

#	Perfil	Requisitos de garantía	Opciones de garantía independiente
1	**Alcance**: Personal, confidencial **Ubicación del Tratamiento de los datos:** En Microsoft o el Cliente **Función del tratamiento:** Encargado o Responsable del Tratamiento **Clase de datos:** Confidenciales o Altamente Confidenciales **Tarjetas de pago:** N/A **SaaS:** N/A **Uso de Subcontratistas:** N/A **Alojamiento de sitios web:** N/A **Atención médica:** N/A	Autocertificación de cumplimiento de los DPR	
2	**Alcance:** Confidencial **Ubicación del Tratamiento de los datos:** En el Proveedor **Función del tratamiento:** N/A **Clase de datos:** Confidencial **Tarjetas de pago:** N/A **SaaS:** N/A **Uso de Subcontratistas:** N/A **Alojamiento de sitios web:** N/A **Atención médica:** N/A	Autocertificación de cumplimiento de los DPR	
3	**Alcance**: Confidencial **Ubicación del Tratamiento de los datos:** En el Proveedor **Función del tratamiento:** N/A **Clase de datos:** Altamente confidencial **Tarjetas de pago:** N/A **SaaS:** N/A	Autocertificación de cumplimiento de los DPR **y** Garantía de cumplimiento independiente	Opciones de garantía independiente: 1. Completar una Evaluación independiente según los DPR **o** 2. Enviar la certificación ISO 27001

	Uso de Subcontratistas: N/A **Alojamiento de sitios web:** N/A **Atención médica:** N/A		
#	Perfil	Requisitos de garantía	Opciones de garantía independiente
4	**Alcance:** Personal, confidencial **Ubicación del Tratamiento de los datos:** En el Proveedor **Función del tratamiento:** Encargado **Clase de datos:** Altamente confidencial **Tarjetas de pago:** N/A **SaaS:** N/A **Uso de Subcontratistas:** N/A **Alojamiento de sitios web:** N/A **Atención médica:** N/A	Autocertificación de cumplimiento de los DPR **y** Garantía de cumplimiento independiente	Opciones de garantía independiente: 1. Completar una Evaluación independiente según los DPR 2. Evaluación independiente según los artículos A-I de los DPR y la certificación ISO 27001 **o** 3. Enviar las certificaciones ISO 27701 **e** ISO 27001
5	**Alcance:** Personal, confidencial **Ubicación del Tratamiento de los datos:** En el Proveedor **Función del tratamiento:** Encargado **Clase de datos:** Confidencial **Tarjetas de pago:** N/A **SaaS:** N/A **Uso de Subcontratistas:** N/A **Alojamiento de sitios web:** N/A **Atención médica:** N/A	Autocertificación de cumplimiento de los DPR	
6	**Alcance:** Personal, confidencial **Ubicación del Tratamiento de los datos:** En el Proveedor **Función del tratamiento:** Responsable del Tratamiento **Clase de datos:** Altamente Confidenciales o Confidenciales	Autocertificación de cumplimiento de los DPR	

	Tarjetas de pago: N/A **SaaS:** N/A **Uso de Subcontratistas:** N/A **Alojamiento de sitios web:** N/A **Atención médica:** N/A		

#	Perfil	Requisitos de garantía	Opciones de garantía independiente
7	**Alcance:** Personal, confidencial **Ubicación del Tratamiento de los datos:** cualquiera **Función del tratamiento:** Subencargado (esta función está determinada por Microsoft; el perfil dirá "Aprobación de Subencargado: Sí") **Clase de datos:** Altamente Confidenciales o Confidenciales **Tarjetas de pago:** N/A **SaaS:** N/A **Uso de Subcontratistas:** N/A **Alojamiento de sitios web:** N/A **Atención médica:** N/A	Autocertificación de cumplimiento de los DPR **y** Garantía de cumplimiento independiente	Opciones de garantía independiente: 1. Completar Evaluación independiente según los DPR 2. Evaluación independiente según los artículos A-I de los DPR y la certificación ISO 27001 **o** 3. Enviar las certificaciones ISO 27701 **e** ISO 27001
Impacto de agregar SaaS, Subcontratistas, Alojamiento de sitios web, Atención médica			
8	**Alcance:** Personal, confidencial **Ubicación del Tratamiento de los datos:** En el Proveedor **Función del tratamiento:** Encargado **Clase de datos:** Altamente Confidenciales o Confidenciales **Tarjetas de pago:** N/A **Subcontratistas:** SÍ o **SaaS:** SÍ o **Alojamiento de sitios web:** SÍ o **Atención médica:** SÍ	Autocertificación de cumplimiento de los DPR **y** Garantía de cumplimiento independiente	Opciones de garantía independiente: 1. Completar Evaluación independiente según los DPR 2. Evaluación independiente según los artículos A-I de los DPR y la certificación ISO 27001 **o** 3. Enviar las certificaciones ISO 27701 **e** ISO 27001 **o** 4. Informe HITRUST (**solo** para una entidad cubierta o un proveedor de servicios de salud en los Estados Unidos)

#	Perfil	Requisitos de garantía	Opciones de garantía independiente
9	**Alcance:** Personal, confidencial **Ubicación del Tratamiento de los datos:** En el Proveedor **Función del tratamiento:** Responsable del Tratamiento **Clase de datos:** Altamente Confidenciales o Confidenciales **Tarjetas de pago:** N/A **Subcontratistas:** SÍ o **SaaS:** SÍ o **Alojamiento de sitios web:** SÍ o **Atención médica:** SÍ	Autocertificación de cumplimiento de los DPR	
Garantías adicionales para Tarjetas de Pago y SaaS			
10	Cualquiera de los perfiles anteriores y **Tarjetas de Pago**	Requisitos anteriores aplicables y garantía de la Industria de tarjetas de pago	Enviar certificación PCI DSS
11	Cualquiera de los perfiles anteriores y **Software como Servicio (SaaS)**	Requisitos anteriores aplicables **y** enviar certificación ISO 27001 exigible por contrato que cubra los servicios funcionales	Enviar certificación ISO 27001 que cubra funcionalmente el/los servicio(s) prestado(s).