Servicio de adquisiciones de Microsoft

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

Versión 10

Septiembre de 2024

Índice

Microsoft

Información general sobre el programa SSPA

El Programa "Garantía de seguridad y privacidad del proveedor" ("**SSPA**") es una alianza entre los grupos de Adquisiciones, Asuntos legales y externos corporativos, Seguridad corporativa y la Oficina de IA responsable de Microsoft con el objetivo de garantizar que los proveedores respeten los principios de privacidad, seguridad y de IA responsable. Este programa corporativo se implementó para proporcionar a nuestros proveedores en todo el mundo las instrucciones básicas para el tratamiento de datos en forma de "Requisitos de protección de datos" para los proveedores de Microsoft (*Data Protection Requirements*, o "DPR"), y se encuentra disponible en la página de SSPA en Microsoft.com/Procurement.

Los proveedores pueden seleccionar Perfiles de Tratamiento de Datos que se adecuen a los bienes y/o servicios contratados. Dichas selecciones determinarán los requisitos que correspondan para garantizar el cumplimiento a Microsoft.

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 traten datos considerados de mayor riesgo por Microsoft, posiblemente deban cumplir requisitos adicionales, tales como una verificación de cumplimiento independiente (véase Evaluación independiente). Es importante tomar en cuenta que es posible que los proveedores tengan que cumplir requisitos de nivel organizacional que el grupo de Microsoft responsable de la interacción con el proveedor decida y comunique independientemente de la SSPA.

Importante: Las actividades de cumplimiento completadas determinarán si el proveedor tiene un estado de cumplimiento de la SSPA Verde (conforme) o Rojo (no conforme), así como las aprobaciones del tratamiento de datos (véase a continuación el Perfil de Tratamiento de Datos). Las herramientas de compra de Microsoft validan el estado Verde de cumplimiento de la SSPA (de cada proveedor dentro de su alcance) y las aprobaciones de los requisitos antes de autorizar la interacción.

Perfil de Tratamiento de Datos de SSPA

Los proveedores de Microsoft tienen control sobre su Perfil de Tratamiento de Datos de SSPA. Las aprobaciones seleccionadas en el Perfil de Tratamiento de Datos ayudan a la SSPA a evaluar el nivel de riesgo de su(s) interacción(es) con Microsoft. Los requisitos de cumplimiento de la SSPA difieren según el Perfil de Tratamiento de Datos y las aprobaciones relacionadas con él, lo que permite a los proveedores determinar para qué interacciones desean postularse. Es importante prestar especial atención a las selecciones y tener en cuenta la actividad de cumplimiento que se deberá completar para obtener la aprobación.

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 por el proveedor.

Los proveedores podrán actualizar su Perfil de Tratamiento de Datos en cualquier momento en caso de no haber tareas abiertas. Si se realiza algún cambio, se emitirá la actividad de cumplimiento correspondiente (tareas), la cual deberá completarse antes de que las nuevas aprobaciones se reflejen en el Perfil de Tratamiento de Datos. Las aprobaciones existentes y completadas continuarán vigentes hasta que se completen los nuevos requisitos emitidos. Si las tareas nuevas no se completan dentro del periodo 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.

También hay combinaciones que podrían incrementar o reducir los requisitos de cumplimiento. Estas combinaciones se detallan en la tabla a continuación 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 que la situación del proveedor se adapta a este marco solicitando una revisión al equipo de SSPA.

Tabla del Perfil de Tratamiento de Datos de SSPA

#	Perfil	Requisitos	Opciones de garantía independiente
1	**Alcance**: Personal y 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 o SÍ **Alojamiento de sitios web:** N/A o SÍ **Atención médica:** N/A o SÍ	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:** 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	
3	**Alcance:** Confidenciales **Ubicación del tratamiento de los datos:** En el Proveedor **Función del tratamiento:** N/A	Autocertificación de cumplimiento de los DPR **y**	Opciones de garantía independiente: 1. Completar una evaluación

	Clase de datos: 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	Garantía de cumplimiento independiente	independiente según los DPR **o** 2. Enviar la certificación ISO 27001
4	**Alcance**: Personal y confidencial **Ubicación del tratamiento de los datos**: En el Proveedor **Función del tratamiento**: Encargado **Clase de datos**: 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 **y** Garantía de cumplimiento independiente	Opciones de garantía independiente: 1. Completar una evaluación independiente según los DPR **o** 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 y confidencial **Ubicación del tratamiento de los datos**: En el Proveedor **Función del tratamiento**: Encargado **Clase de datos**: 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	
6	**Alcance**: Personal y 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 **SaaS**: N/A **Uso de Subcontratistas**: N/A o SÍ **Alojamiento de sitios web**: N/A **Atención médica**: N/A o SÍ	Autocertificación de cumplimiento de los DPR	

7	**Alcance:** Personal y 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 una evaluación independiente según los DPR **o** 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
8	**Alcance:** Personal y 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 una evaluación independiente según los DPR **o** 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 entidades cubiertas o proveedores de servicios de salud en los Estados Unidos)
	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

	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 una certificación ISO 27001 con cobertura funcional del/de los servicio(s) prestado(s).
	Cualquiera de los perfiles anteriores y **Sistemas de Inteligencia Artificial (IA)**	Autocertificación de cumplimiento de los DPR, incluyendo la rama de IA **y** Garantía de cumplimiento independiente	Opciones de garantía independiente: 1. Completar una evaluación independiente según los DPR, incluyendo la rama de IA **o** 2. Evaluación independiente según los artículos A-I, K de los DPR y la certificación ISO 27001 3. Evaluación independiente según el artículo K de los DPR y la certificación ISO 27001 e ISO 27001, **o** 4. Enviar las certificaciones ISO 27701, ISO 27001 e ISO 42001* (*ISO 42001 se requiere para la prestación de servicios que impliquen sistemas de IA de uso sensible)

Alcance

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 y confidencial

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

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. Tenga en cuenta que estos son solo algunos ejemplos y no una lista exhaustiva.

Nota: Todo propietario de un negocio de Microsoft puede solicitar su eliminación 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 vencimiento; **o** código de seguridad/acceso o contraseña/credenciales que permitan el acceso a una cuenta
Información seudonimizada de usuario final (EUPI, por sus siglas en inglés) (identificadores creados por Microsoft para identificar a los usuarios de sus productos y servicios) • Identificador global único (GUID, por sus siglas en inglés) • ID de usuario de Passport o Identificador único (PUID, por sus siglas en inglés) • Información identificable de usuario final cifrada (EUII) • ID de sesión

• ID de dispositivo • Datos de diagnósticos • Datos de ingreso • Datos de clientes relacionados con casos de asistencia al cliente
Datos de clientes
Documentos, fotos, videos, música, etc.
Ingreso de opiniones y/o calificaciones sobre productos o servicios
Respuestas a encuestas
Historial de navegación, intereses y favoritos
Expresiones escritas, manuscritas y orales (voz/audio y/o chat/bot)
Datos sobre credenciales (contraseñas, sugerencias de contraseñas, nombres de usuario, datos biométricos utilizados para identificación)
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 gráfico 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
Uso sensible (sistemas de IA)
Impacto de las consecuencias sobre la situación jurídica o las oportunidades de vida, incluyendo: • Sistemas de puntuación y evaluación de riesgos del sistema de justicia penal • Sistema de admisión a la educación superior • Sistemas de solicitud y puntuación de créditos

Riesgo de lesiones físicas o psicológicas, incluyendo: • Sistemas de diagnóstico o tratamiento médico • Sistemas de salud mental y bienestar • Sistemas de control de equipos y mantenimiento predictivo
Amenaza a los derechos humanos, incluyendo: • Sistemas de medios de comunicación sintéticos que podrían generar desinformación o propaganda política para influir en las elecciones • Sistema de alerta basado en expresiones religiosas, políticas o sociales • Puntuación de créditos social

Datos confidenciales de Microsoft

Los ejemplos incluyen, entre otros:

Altamente confidencial
Información concerniente o relacionada con el desarrollo, prueba o fabricación de productos Microsoft o sus componentes *Todo software, servicio en línea o hardware de Microsoft 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 las normas de la SEC

Confidencial
Claves de licencias de productos Microsoft en nombre de Microsoft para distribución a través de cualquier medio
Información concerniente o relacionada con el desarrollo o prueba de aplicaciones de líneas de negocios internas (LOB) 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, tales como dispositivos (guías de proceso o procedimiento, datos de configuración, etc.)

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

Ubicación del tratamiento de los datos

En Microsoft o el Cliente

Seleccione esta aprobación si la Actividad del proveedor involucra 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 de un cliente de Microsoft.

No seleccione esta opción en las siguientes circunstancias:

- El proveedor administra un centro en el extranjero designado por Microsoft (OF, por sus siglas 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, se debe seleccionar “Encargado” en lugar de “Responsable del tratamiento”.

Encargado

Esta es la función de tratamiento de datos más común cuando el proveedor realiza 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 una Adenda de protección de datos y una evaluación independiente (véase más adelante). Aquellos proveedores que integren la lista de Subencargados publicada por Microsoft también deberán presentar una verificación de cumplimiento independiente.

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 relacionadas con el procesamiento de tarjetas de pago.

Requisito de certificación PCI

La "Norma de seguridad de datos para la industria de las 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, un organismo autónomo de la industria. El objetivo de los requisitos PCI DSS es identificar las vulnerabilidades de la tecnología y de 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 PCI.

Dependiendo del volumen de transacciones procesadas, el proveedor deberá contar con un Evaluador de seguridad calificado para que certifique el cumplimiento, o responder el 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.

Software como Servicio (SaaS, por sus siglas en inglés)

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 para también incluir la Plataforma como Servicio (PaaS, por sus siglas en inglés) y la Infraestructura como Servicio (IaaS, por sus siglas en inglés). (Para conocer más acerca de 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 use". Este método de entrega de software y licencias brinda acceso en línea a través de una suscripción en lugar de tener que comprarlo e instalarlo en cada computadora individual.

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.

Es posible que los proveedores que cumplan con la definición de SaaS incluida en el Perfil de Tratamiento de Datos tengan que presentar una certificación ISO 27001 válida, si el "Contrato de servicios en la nube" de Microsoft así lo estipula Le pedimos no enviar una certificación del centro de datos. Únicamente se acepta la certificación ISO 27001 correspondiente a los servicios de software especificados en el contrato celebrado con Microsoft.

Uso de Subcontratistas

Seleccione esta aprobación si el proveedor utiliza Subcontratistas para la realización de las Actividades. 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.

Esto también incluye a los trabajadores independientes o *freelancers* (consulte las definiciones en los DPR).

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 se realizará el tratamiento de dichos datos personales por parte de cada Subcontratista.

Alojamiento de sitios web

Seleccione esta opción de perfil si el proveedor aloja sitios web, ofrece portales de sitios web, servicios en línea y/o aplicaciones móviles en nombre de Microsoft.

El servicio de alojamiento de sitios web es un servicio en línea que crea y/o mantiene sitios web en nombre 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.

Atención médica

Seleccione esta opción de perfil si el proveedor está obligado a tratar datos de información médica protegida.

Por "**Información Médica Protegida**" o "**PHI**" (por sus siglas en inglés), se entiende los Datos Personales de Microsoft protegidos por la Ley de Portabilidad y Responsabilidad de la Información Médica de los Estados Unidos (*United States Health Information Portability and Accountability Act*, o HIPAA).

Sistemas de inteligencia artificial (IA)

Seleccione esta opción de perfil si el proveedor prestará servicios a Microsoft relacionados con sistemas de IA, incluyendo el uso de herramientas, sistemas o plataformas con tecnología de IA para entrenar y crear sistemas inteligentes con el fin de crear contenidos totalmente nuevos, tales como imágenes, sonidos, videos, perspectivas, análisis y/o texto.

La aprobación de los sistemas de IA como parte de la SSPA incluirá documentación sobre el Tratamiento de Datos Personales y/o Confidenciales de Microsoft, el impacto para las personas, las organizaciones y la sociedad, y la aceptación de las certificaciones adecuadas de los proveedores. Para poder proceder con la compra, el proveedor deberá completar la rama de IA responsable incluida en los Requisitos de Protección de Datos para los proveedores de Microsoft, junto con los contratos firmados y/o las revisiones internas de Microsoft que se requieran. Todos los proveedores de sistemas de IA estarán obligados a presentar opciones de garantía independiente. Se puede presentar la ISO 42001 para validar el cumplimiento del artículo K de los DPR y es **obligatoria** para cualquier caso delicado de IA. En el caso de los proveedores que obtengan una evaluación independiente de conformidad con el artículo K de los DPR, la evaluación independiente debe ser realizada por alguno de los evaluadores avalados (consulte la lista aquí).

Esta aprobación solo se concederá si la SSPA acepta la evaluación independiente.

Resumen del proceso de la SSPA

¿Qué es la SSPA?

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, nos esforzamos a diario para merecer y mantener la confianza de nuestros clientes.

Las buenas prácticas de seguridad y privacidad son cruciales 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 realizan el tratamiento de datos de Microsoft en nombre nuestro.

Los términos clave de la SSPA se definen en los DPR. Para mayor información sobre el programa, consulte nuestras Preguntas frecuentes (FAQ) o comuníquese con nuestro equipo global al correo electrónico SSPAHelp@microsoft.com.

Los DPR son un requisito anual. Las actividades de cumplimiento determinan 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) y las aprobaciones de los requisitos antes de autorizar la interacción.

Diagrama del proceso de la SSPA – Inscripción de nuevo proveedor

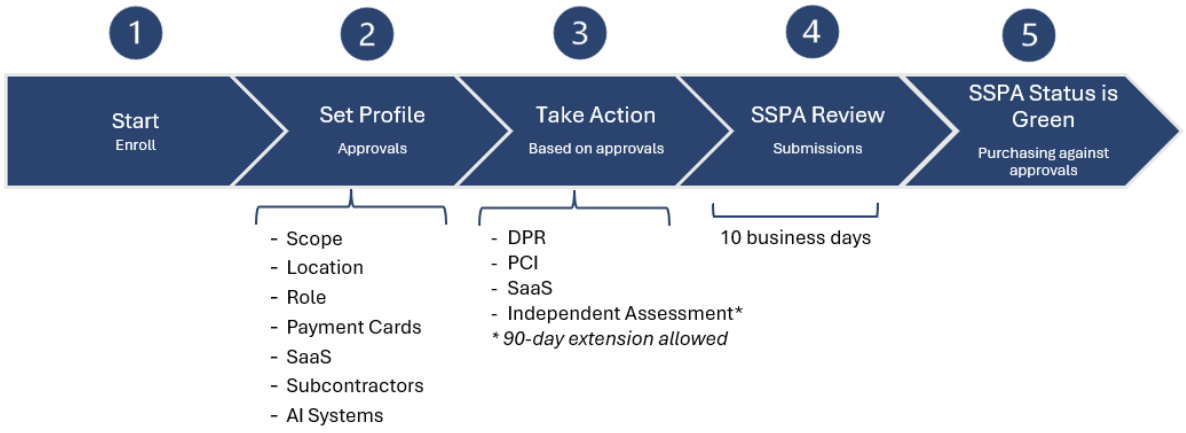
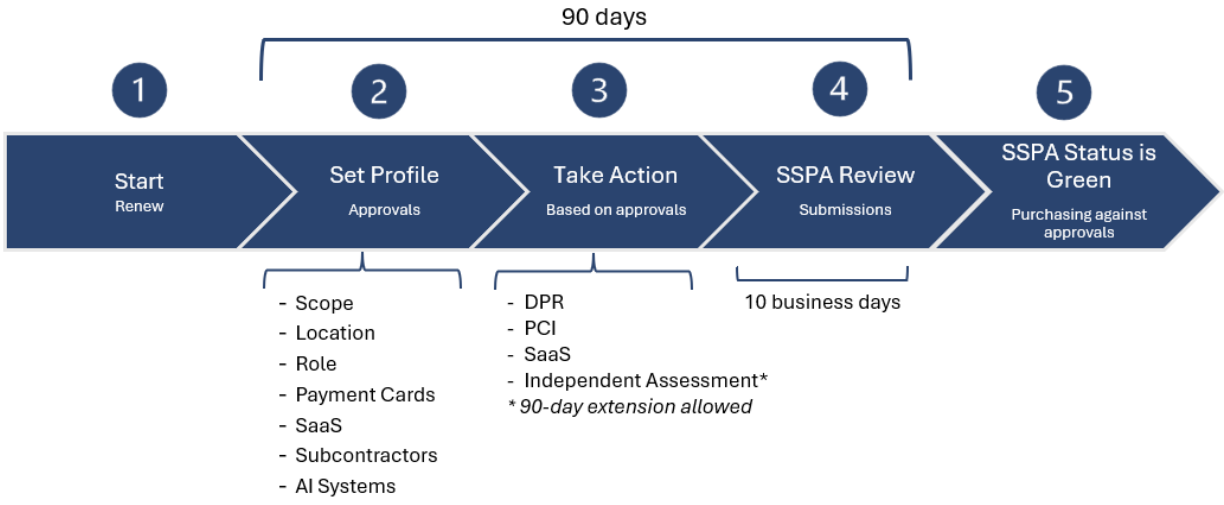


Diagrama del proceso de la SSPA – Renovación anual de proveedor



Requisitos de garantía

Las aprobaciones seleccionadas en el Perfil de Tratamiento de Datos ayudan a la SSPA a evaluar el nivel de riesgo de su(s) interacción(es) con Microsoft. Los requisitos de cumplimiento de la SSPA difieren según el Perfil de Tratamiento de Datos y las aprobaciones relacionadas con él.

Autocertificación de cumplimiento de los DPR

Todos los proveedores inscritos en el programa SSPA deben completar una autocertificación de cumplimiento de los DPR en un plazo de 90 días a partir de la recepción de la solicitud. Esta solicitud se proporcionará 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 nuevas compras comprendidas dentro del alcance de la SSPA no podrán procesarse hasta que 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 la 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 del programa SSPA podrá solicitar la aclaración sobre una o varias elecciones. 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 obtenida de expertos en el tema para responder a cada requisito con solvencia. Asimismo, al escribir su nombre en el formulario de SSPA certifican que han leído y entendido los DPR. Para que se pueda considerar que se ha cumplido con lo establecido en el artículo J de los DPR, es necesario tener un contacto de seguridad independiente al cual se le podría pedir ayuda en caso de que ocurra algún incidente de seguridad que involucre a su empresa. 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 para cada requisito aplicable.
3. Firmar y enviar la certificación en el portal de Cumplimiento de Proveedores de Microsoft.

Importante: El equipo del programa SSPA podrá solicitar pruebas colaborativas del cumplimiento de un determinado Requisito de Protección de Datos para respaldar las certificaciones de cumplimiento. Asimismo, los proveedores podrían ser seleccionados para aportar pruebas fuera del ciclo de cumplimiento anual, tal y como se describe en los Requisitos de Protección de Datos para los proveedores de Microsoft. Esto solo se aplicará a las empresas que no reciban la tarea de evaluación independiente.

Requisito de evaluación independiente

Consulte los "Requisitos por aprobaciones" que se encuentran en la Tabla del Perfil de Tratamiento de Datos de SSPA 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 de, 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 (Carta de Certificación) 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, el cual se adjunta al PDF "Evaluadores avalados", disponible aquí.**

La **Tabla del Perfil de Tratamiento de Datos de SSPA** incluye alternativas de certificación aceptables 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), ISO 27001 (seguridad), e ISO 42001 para los sistemas de IA (artículo K de los DPR) se pueden tomar como punto de referencia, ya que consideran en forma minuciosa los DPR.

En los casos en los que el proveedor sea una entidad amparada por HIPAA o un proveedor de servicios de salud en los Estados Unidos, 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, el equipo del programa SSPA puede solicitar una evaluación independiente sin considerar el Perfil de Tratamiento de Datos. Algunos ejemplos son: una solicitud de privacidad o seguridad de la división; una validación de la subsanación de incidentes de datos; una revisión fuera del ciclo por parte del equipo del programa SSPA; o un requerimiento de ejecución automatizada de los derechos del interesado.

Guía para cumplir con este requisito:

1. La interacción debe realizarla 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*, oIFAC) o al Instituto Estadounidense de Contadores Públicos Certificados (*American Institute of Certified Public Accountants*, oAICPA); o ser un auditor ISO certificado calificado para ISO 27001, ISO 27701 e ISO 42001 cuando corresponda; 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 Professionals*, oIAPP) o la Asociación para la Auditoría y el Control de Sistemas Informáticos (*Information Systems Audit and Control Association*, oISACA).
3. El evaluador debe utilizar los DPR vigentes que incluyan las pruebas que deben presentarse como respaldo para cada requisito. **Los proveedores deberán proporcionarle al evaluador las respuestas de certificación de los DPR más recientemente aprobadas.**
4. El alcance de la interacción se limita a toda actividad pertinente de tratamiento de datos que se lleve a cabo según 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.**

5. La carta enviada al programa SSPA no debe incluir ninguna declaración que implique que el proveedor no puede cumplir con los Requisitos de Protección de Datos descritos. Estas cuestiones deberán corregirse antes de enviar la carta.

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

Perfiles que requieren una garantía independiente adicional:

Software como Servicio (SaaS, por sus siglas en inglés)

Es posible que los proveedores que cumplan con la definición de SaaS incluida en el Perfil de Tratamiento de Datos tengan que presentar una certificación ISO 27001 válida, si el "Contrato de servicios en la nube" de Microsoft así lo estipula Le pedimos no enviar una certificación del centro de datos. Únicamente se acepta la certificación ISO 27001 correspondiente a los servicios de software especificados en el contrato celebrado con Microsoft.

Los revisores del programa SSPA validarán que la información enviada cumpla la obligación contractual.

Sistemas de IA

Si la prestación del servicio incluye Uso Delicado, será necesaria una certificación ISO 42001. La ISO 42001 también puede presentarse para cumplir con el artículo K de la tarea de evaluación independiente.

Incidentes de datos

Si un proveedor tiene conocimiento de algún incidente en relación con la privacidad o seguridad de los datos, deberá informarlo a Microsoft según se detalla y define en los DPR.

Cualquier incidente de datos deberá reportarse a través del sitio SupplierWeb o por correo electrónico a SupplR@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 (OC), si corresponde o está disponible
- Resumen del incidente de datos