La traducción que figura a continuación se ofrece únicamente a título informativo. En caso de discrepancia, incoherencia o conflicto entre esta traducción y la versión inglesa (en particular debido a retrasos en la traducción), prevalecerá la versión inglesa.

POLÍTICA DE SEGURIDAD DEL PROVEEDOR

Última actualización 28 de enero de 2022

1. ÁMBITO DE APLICACIÓN; DEFINICIONES.

1.1 Política de seguridad. El Proveedor cumplirá en todos los aspectos los requisitos de seguridad de la información de Amazon expuestos en esta política (la "**Política de seguridad**"). La presente Política de seguridad se aplica a la actuación del Proveedor en virtud del Acuerdo y a todo acceso, recopilación, uso, almacenamiento, transmisión, revelación, destrucción o borrado de Información de Amazon por parte del Proveedor e incidentes de seguridad relacionados con esta. La presente Política de seguridad no limita ninguna de las demás obligaciones del Proveedor, incluidas aquellas en virtud de cualquier otro acuerdo con Amazon o cualquier otra ley que se aplique al Proveedor, la actuación del Proveedor de conformidad con cualquier otro acuerdo con Amazon, la Información de Amazon o el Fin permitido. Si esta Política de seguridad entra en conflicto con cualquier acuerdo de confidencialidad entre las partes, o cualquier otro acuerdo aplicable a las partes, el Proveedor notificará de inmediato a Amazon el conflicto y cumplirá con los requisitos que sean más protectores de la Información de Amazon, a menos que se declare expresamente que los requisitos menos protectores anulan los requisitos más protectores (que pueden ser señalados por Amazon). Amazon puede cambiar esta Política de seguridad según proceda a su entera discreción, a condición de que si dichos cambios no son comercialmente razonables, Amazon se reunirá, a petición, con el Proveedor y acordará las tarifas adicionales apropiadas.

1.2 Definiciones.

1.2.1 "**Agregar**" significa combinar o almacenar Información de Amazon con cualquier dato o información del Proveedor o de cualquier tercero.

1.2.2 "**Acuerdo**" significa cualquier acuerdo que haga referencia a esta Política de seguridad.

1.2.3 "**Amazon**" significa Amazon.com, Inc. y sus empresas afiliadas.

1.2.4 "**Anonimizar**" significa utilizar, recopilar, almacenar, transmitir o transformar cualquier dato o información (incluida la Información de Amazon) de una manera o forma que no identifique, permita la identificación de Amazon ni de ningún usuario, identificador de dispositivo, fuente, producto, servicio, contexto o marca, y no sea atribuible de otro modo a estos.

1.2.5 "**Información de Amazon**" significa, individual y colectivamente: a) toda la Información confidencial de Amazon (según se defina en un acuerdo de confidencialidad o cualquier otro acuerdo entre las partes); b) todos los demás datos, registros, archivos, contenido o información, en cualquier forma o formato, adquiridos, accedidos, recogidos, recibidos, almacenados o mantenidos por el Proveedor o sus empresas afiliadas, desde o en nombre de Amazon, o de otro modo en relación con esta Política de seguridad o los servicios, o el cumplimiento o ejercicio de los derechos de las partes en virtud del Acuerdo o en relación con él; y c) información derivada de a) o b), incluso si se anonimiza.

1.2.6 "Proveedor" significa cada Proveedor, Vendedor o Contratista definido en un Acuerdo y cualquier otro proveedor supeditado a un Acuerdo.

1.3 Fin permitido. El Proveedor puede acceder, recopilar, utilizar, almacenar y transmitir únicamente la Información de Amazon expresamente autorizada en virtud del Acuerdo y únicamente con el fin de proporcionar los productos o servicios en virtud del Acuerdo, de conformidad con las licencias (si las hubiera) otorgadas por esta Política de seguridad (el "**Fin permitido**"). Salvo que se autorice expresamente en virtud del Acuerdo, el Proveedor no accederá, recopilará, usará, almacenará ni transmitirá ninguna Información de Amazon y no agregará

Información de Amazon, aunque sea anonimizada. Salvo con el previo consentimiento expreso por escrito de Amazon, el Proveedor no a) transferirá, alquilará, intercambiará, comerciará, venderá, prestará o arrendará, ni distribuirá ni pondrá a disposición de ningún tercero, ninguna Información de Amazon; o b) agregará a la Información de Amazon cualquier otra información o datos, aunque sean anonimizados.

2. POLÍTICA DE SEGURIDAD DE AMAZON.

2.1 Requisitos de seguridad básicos. El Proveedor deberá, de conformidad con las mejores normas actuales del sector y otros requisitos especificados por Amazon en función de la clasificación y confidencialidad de la Información de Amazon, mantener salvaguardas físicas, administrativas y técnicas y otras medidas de seguridad para a) mantener la seguridad y confidencialidad de la Información de Amazon accedida, recogida, utilizada, almacenada o transmitida por el Proveedor; y b) proteger esa información de amenazas o peligros conocidos o razonablemente previstos a su seguridad e integridad, pérdida accidental, modificación y revelación y todas las demás formas ilegítimas de tratamiento. Sin limitación, el Proveedor cumplirá con los siguientes requisitos para cualquier sistema que el Proveedor utilice para tratar Información de Amazon o que tenga acceso a Información de Amazon ("**Sistemas de información de Amazon**"):

2.1.1 Seguridad de la red. El Proveedor protegerá cualquier Sistema de información de Amazon mediante la restricción del acceso no autorizado a la red, especialmente desde Internet externo. El Proveedor instalará y mantendrá una solución de seguridad de red eficaz, como un cortafuegos, para proteger la Información de Amazon en todo momento.

2.1.2 Actualizaciones Según se describe en la publicación especial ("SP") del Instituto Nacional de Normas y Tecnología (National Institute of Standards and Technology, "NIST") 800-40, revisión 3, el Proveedor mantendrá actualizados los Sistemas de información de Amazon con las últimas mejoras, actualizaciones, correcciones de errores y nuevas versiones y con cualquier otra modificación necesaria para garantizar la seguridad de la Información de Amazon.

2.1.3 Antimalware. El Proveedor utilizará en todo momento software antimalware o un control de seguridad equivalente para mitigar el riesgo de daño y propagación de malware. Si se utiliza, el Proveedor mantendrá actualizado el software antimalware.

2.1.4 Cifrado. El Proveedor cifrará los datos en reposo y los datos enviados a través de redes abiertas de acuerdo con las mejores prácticas del sector.

2.1.5 Pruebas. El Proveedor probará con frecuencia sus sistemas y procesos de seguridad para garantizar que cumplen los requisitos de esta Política de seguridad o la última política de seguridad acordada por el Proveedor y Amazon. En la medida en que haya cambios en la Política de seguridad de conformidad con el apartado 1.1, dichos cambios no entrarán en vigor a efectos de este apartado hasta que se acuerde entre el Proveedor y Amazon (basta con un correo electrónico).

2.1.6 Controles de acceso. El Proveedor protegerá la Información de Amazon, lo que incluye el cumplimiento de los siguientes requisitos:

2.1.6.1 El Proveedor asignará un ID único a cada persona con acceso informático a la Información de Amazon o a los Sistemas de información de Amazon.

2.1.6.2 El Proveedor restringirá el acceso a la Información de Amazon solo a aquellas personas con "necesidad de saber" para un Fin permitido.

2.1.6.3 El Proveedor revisará periódicamente (al menos una vez cada 90 días) la lista de personas y servicios con acceso a la Información de Amazon, y eliminará las cuentas que ya no requieran acceso a los Sistemas de información de Amazon. .

2.1.6.4 El Proveedor no utilizará los valores predeterminados proporcionados por el fabricante para las contraseñas del sistema y otros parámetros de seguridad en ningún Sistema de información de Amazon. El Proveedor exigirá y garantizará el uso de "contraseñas seguras" impuestas por el sistema de acuerdo con las mejores prácticas descritas en NIST SP 800-63B en todos los Sistemas de información de Amazon. El Proveedor exigirá que todas las contraseñas y credenciales de acceso se mantengan confidenciales y no se compartan entre el personal.

2.1.6.5 El Proveedor mantendrá e impondrá el "bloqueo de cuentas" al desactivar las cuentas con acceso a la Información de Amazon o a los Sistemas de información de Amazon cuando una cuenta supere más de diez (10) intentos de contraseña incorrectos consecutivos.

2.1.6.6 Salvo cuando Amazon lo autorice expresamente por escrito, el Proveedor separará física o lógicamente la Información de Amazon en todo momento (incluido en el almacenamiento, tratamiento o transmisión) de la información del Proveedor y de cualquier información de terceros.

2.1.6.7 Si Amazon solicita controles de acceso físico adicionales por escrito, el Proveedor aplicará y utilizará dichas medidas de control de acceso físico seguro.

2.1.6.8 El Proveedor proporcionará a Amazon, a petición razonable de Amazon, a) datos de registro sobre todo uso (autorizado y no autorizado) de las cuentas o credenciales de Amazon proporcionadas al Proveedor para una actividad autorizada (p. ej., credenciales de cuenta de redes sociales); y b) datos de registro detallados sobre cualquier suplantación, o intento de suplantación, de personal de Amazon o personal del Proveedor que tenga acceso a la Información de Amazon.

2.1.6.9 El Proveedor revisará con frecuencia los registros de acceso para detectar signos de comportamiento malicioso o acceso no autorizado.

2.1.7 Política del Proveedor. El Proveedor mantendrá e impondrá una política de seguridad de la información y la red para empleados, subcontratistas, agentes y proveedores que cumpla con las normas expuestas en esta Política de seguridad, incluidos métodos para detectar y registrar infracciones de la política. Cuando Amazon lo solicite, el Proveedor proporcionará a Amazon información sobre infracciones de la política de seguridad de la red e información del Proveedor si el Proveedor o Amazon tienen una sospecha razonable de que puede constituir un Incidente de seguridad (definido más adelante).

2.1.8 Subcontratación. El Proveedor no subcontratará ni delegará ninguna de sus obligaciones en virtud de esta Política de seguridad a ningún subcontratista o delegado (colectivamente, "**Subcontratistas**") sin el previo consentimiento por escrito de Amazon. Sin perjuicio de la existencia o las condiciones de cualquier subcontrato o delegación, el Proveedor seguirá siendo responsable del pleno cumplimiento de sus obligaciones en virtud de esta Política de seguridad. Las condiciones de esta Política de seguridad serán vinculantes para los Subcontratistas y el personal del Proveedor. El Proveedor a) se asegurará de que sus Subcontratistas y personal cumplan con esta Política de seguridad; y b) será responsable de todos los actos, omisiones, negligencia y conducta indebida de los Subcontratistas y personal del Proveedor.

2.1.9 Acceso remoto. El Proveedor se asegurará de que cualquier acceso a los Sistemas de información de Amazon requiera autenticación multifactorial (p. ej., requiere al menos dos factores independientes para identificar a los usuarios).

2.1.10 Acceso "masivo". Para los fines de este apartado, acceso "masivo" significa acceder a datos mediante una consulta a la base de datos, generación de informes o cualquier otra transferencia masiva de datos. Salvo cuando Amazon lo autorice expresamente por escrito, el Proveedor no accederá ni permitirá el acceso "masivo" a la Información de Amazon si esta se encuentra en una base de datos controlada por el Proveedor o Amazon o almacenada de cualquier otra manera, incluido el almacenamiento en archivos basados en archivos (p. ej., archivos planos), etc. Concretamente, este apartado prohíbe todo acceso a la Información de Amazon salvo para acceder a registros individuales según sea necesario para el Fin permitido. El Proveedor conservará los datos de registro detallados sobre los intentos de acceso "masivo" a la Información de Amazon conseguida o no y proporcionará informes de estos registros como parte de las obligaciones del Proveedor en virtud del apartado 2.5 (Revisión de seguridad). Si Amazon proporciona al Proveedor autorización por escrito para el acceso "masivo" a la Información de Amazon, el Proveedor a) limitará dicho acceso solo a determinados empleados con una "necesidad de saber"; y b) utilizará herramientas que limiten el acceso y requieran autorización explícita y registro de todos los accesos.

2.1.11 Personal del Proveedor. Amazon puede condicionar el acceso del personal del Proveedor a la Información de Amazon con acuerdos de confidencialidad individuales, cuya forma especificará Amazon y que el Proveedor deberá firmar y entregar a Amazon. El personal del Proveedor ejecutará el acuerdo de confidencialidad individual si Amazon así lo requiere. El Proveedor obtendrá y entregará a Amazon acuerdos de confidencialidad individuales firmados por el personal del Proveedor que vaya a tener acceso a la Información de Amazon (antes de otorgar acceso o proporcionar información al personal del

Proveedor). El Proveedor también mantendrá una lista de todo el personal del Proveedor que haya accedido o recibido la Información de Amazon en los Sistemas de información de Amazon y proporcionará inmediatamente dicha lista a Amazon previa solicitud. Si un integrante del personal del Proveedor a) ya no necesita acceso a la Información de Amazon; o b) ya no cumple los requisitos como personal del Proveedor (p. ej., la persona deja el empleo del Proveedor), el Proveedor cancelará inmediatamente (en un plazo máximo de 24 horas) el acceso a la Información de Amazon y los Sistemas de información de Amazon. Si dicho personal está autorizado a acceder a la Información de Amazon en los Sistemas de información de Amazon, el Proveedor también lo notificará a Amazon en un plazo de 24 horas.

2.2 Acceso a la extranet de Amazon y portales de proveedores. Amazon puede conceder al Proveedor acceso a la Información de Amazon a través de portales web u otros sitios web o servicios de extranet no públicos en el sitio web o sistema de Amazon o de un tercero (cada uno, una "**Extranet**") para el Fin permitido. Si Amazon permite al Proveedor acceder a cualquier Información de Amazon a través de una Extranet, el Proveedor debe cumplir con los requisitos siguientes:

2.2.1 Fin permitido. El Proveedor y el personal del Proveedor accederán a la Extranet y accederán, recopilarán, utilizarán, verán, recuperarán, descargarán o almacenarán Información de Amazon de la Extranet únicamente para el Fin permitido.

2.2.2 Cuentas. El Proveedor se asegurará de que el personal del Proveedor utilice únicamente la cuenta o cuentas de Extranet designada(s) por Amazon para cada persona y requerirá que el personal del Proveedor mantenga la confidencialidad de sus credenciales de acceso.

2.2.3 Sistemas. El Proveedor accederá a la Extranet únicamente a través de sistemas informáticos o de tratamiento, o aplicaciones que ejecuten sistemas operativos gestionados por el Proveedor y que incluyan: a) cortafuegos de red del sistema de acuerdo con el apartado 2.1.1 (Seguridad de la red); b) gestión centralizada de parches de conformidad con el apartado 2.1.2 (Actualizaciones); c) software antimalware del sistema operativo adecuado de acuerdo con el apartado 2.1.3 (Antimalware); y d) cifrado de disco completo para dispositivos portátiles.

2.2.4 Restricciones. Salvo si Amazon lo aprueba previamente por escrito, el Proveedor no descargará, replicará ni almacenará permanentemente ninguna Información de Amazon desde ninguna Extranet en ningún medio, incluidos equipos, dispositivos o servidores.

2.2.5 Cancelación de cuenta. El Proveedor cancelará la cuenta, y notificará a Amazon no más tarde de 24 horas después, sobre cualquier integrante del personal del Proveedor que esté autorizado a acceder a cualquier Extranet: a) que ya no necesite acceso a la Información de Amazon; o b) que ya no se califique como personal del Proveedor (p. ej., el personal deja el empleo del Proveedor).

2.2.6 Sistemas de terceros.

2.2.6.1 El Proveedor notificará previamente a Amazon y obtendrá su aprobación previa por escrito antes de utilizar cualquier sistema de terceros que almacene o pueda tener acceso de otro modo a la Información de Amazon, a menos que a) los datos estén cifrados de acuerdo con esta Política de seguridad; y b) el sistema de terceros no tenga acceso a la clave de descifrado o a las versiones de "texto plano" sin cifrar de los datos. Amazon se reserva el derecho de exigir una revisión de seguridad de Amazon, de acuerdo con el apartado 2.5 (Revisión de seguridad), del sistema de terceros antes de dar su aprobación.

2.2.6.2 Si el Proveedor utiliza sistemas de terceros que almacenan Información de Amazon sin cifrar o puede acceder de otro modo a Información de Amazon sin cifrar, el Proveedor revisará la seguridad de los sistemas de terceros y sus controles de seguridad y proporcionará a Amazon informes periódicos sobre los controles de seguridad del sistema de terceros en el formato solicitado por Amazon (p. ej., SAS 70 o el informe más reciente, u otro informe reconocido por la normativa del sector aprobado por Amazon).

2.3 Conservación y destrucción de datos.

2.3.1 Conservación. El Proveedor conservará la Información de Amazon únicamente con el Fin permitido y durante el tiempo que sea necesario para Fin permitido.

2.3.2 Devolución o borrado. A petición de Amazon, el Proveedor devolverá inmediatamente (pero en un plazo no superior a 72 horas) a Amazon y borrará de forma permanente y segura toda la Información de Amazon de acuerdo con la notificación de Amazon que requiera devolución o borrado. El Proveedor también borrará de forma permanente y segura todas las copias activas (en línea o accesibles en red) de la Información de Amazon en un plazo de 30 días tras la finalización anticipada del Fin permitido o la rescisión o vencimiento de esta Política de seguridad. Si así lo solicita Amazon, el Proveedor certificará por escrito que toda la Información de Amazon ha sido destruida. En aras de la claridad, este apartado no se aplicará a las copias de archivo de conformidad con el apartado 2.3.3

2.3.3 Copias de archivo. Si el Proveedor está obligado por ley a conservar copias de archivo de la Información de Amazon a efectos fiscales o normativos similares, esta Información de Amazon archivada debe almacenarse de una de las maneras siguientes:

2.3.3.1 como copia de seguridad "fría" o fuera de línea (es decir, no disponible para uso inmediato o interactivo) almacenada en una instalación físicamente segura; o

2.3.3.2 cifrada, donde el sistema que aloja o almacena el archivo o archivos cifrado(s) no tiene acceso a una copia de la(s) clave(s) utilizada(s) para el cifrado.

2.3.4 Recuperación. Si el Proveedor vuelve a una copia de seguridad con el fin de recuperación de desastre ("recuperación"), el Proveedor tendrá y mantendrá un proceso que garantice que toda la Información de Amazon que deba borrarse de conformidad con el Acuerdo o esta Política de seguridad o cualquier otro acuerdo con Amazon se volverá a borrar o sobrescribir desde los datos recuperados de conformidad con este apartado 2.3 en un plazo de 24 horas tras la recuperación. Si el Proveedor pone en marcha una recuperación para cualquier fin, no se podrá recuperar Información de Amazon a ningún sistema o red de terceros sin la previa aprobación por escrito de Amazon. Amazon se reserva el derecho a exigir una revisión de seguridad de Amazon, de acuerdo con el apartado 2.5 (Revisión de seguridad), del sistema o red de terceros antes de permitir la recuperación de cualquier Información de Amazon a cualquier sistema o red de terceros.

2.3.5 Normas de saneamiento de datos. Toda la Información de Amazon borrada por el Proveedor se borrará de acuerdo con las Recomendaciones de saneamiento mínimo, contenidas en NIST SP 800-88, revisión 1, Directrices para el saneamiento de medios, de 18 de diciembre de 2014 (disponible en http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf), Apéndice A, para purgar el tipo de dispositivo pertinente. En ausencia de una orientación relevante en NIST SP 800-88, Apéndice A, el dispositivo que contenga Información de Amazon se destruirá de una de las maneras siguientes: a) mediante la desmagnetización de medios magnéticos en un campo de flujo electromagnético de 10.000+ Gauss; b) mediante el triturado o desintegración mecánica que genere partículas de menos de 2x2 mm; o c) a través de otras normas que Amazon pueda requerir en función de la clasificación y confidencialidad de la Información de Amazon.

2.4 Destrucción forense. Antes de eliminar (de cualquier manera) todo hardware, software o cualquier otro medio que contenga, o haya contenido en algún momento, Información de Amazon, el Proveedor llevará a cabo una destrucción forense completa del hardware, software u otros medios que impida la recuperación de la Información de Amazon de cualquier forma. El Proveedor llevará a cabo la destrucción forense de acuerdo con las Recomendaciones de saneamiento mínimo, contenidas en NIST SP 800-88, Apéndice A, para destruir el tipo de dispositivo pertinente.

2.4.1 El Proveedor no venderá, revenderá, donará, renovará ni transferirá de otro modo (incluida toda venta o transferencia de dicho hardware, software u otros medios, cualquier disposición con respecto a cualquier liquidación del negocio del Proveedor, o cualquier otra) ningún hardware, software u otros medios que contengan Información de Amazon que no haya sido destruida de forma forense por el Proveedor según requiere este apartado 2.4.

2.5 Revisión de seguridad.

2.5.1 Amazon se reserva el derecho a solicitar periódicamente al Proveedor que participe en una evaluación de riesgos de Amazon.

2.5.2 Certificación. A petición por escrito de Amazon, el Proveedor certificará por escrito a Amazon que la información proporcionada como parte de la evaluación de riesgos cumple con esta última Política de

seguridad acordada por última vez por el Proveedor y Amazon. En la medida en que haya cambios en la Política de seguridad de conformidad con el apartado 1.1, dichos cambios no entrarán en vigor a efectos de este apartado hasta que se acuerde entre el Proveedor y Amazon (basta con un correo electrónico).

2.5.3 Otras revisiones. Amazon se reserva el derecho a revisar periódicamente la seguridad de los Sistemas de información de Amazon, pero no más de una vez al año, a menos que a) se haya identificado una deficiencia importante anterior dentro del año natural; o b) Amazon esté obligada por un organismo gubernamental u otro organismo regulador a dicha revisión. El Proveedor cooperará y proporcionará a Amazon toda la información requerida en un plazo razonable, pero no más de 20 días naturales desde la fecha de la solicitud de Amazon.

2.5.4 Reparación. Si alguna revisión de seguridad identifica alguna deficiencia, el Proveedor tomará, a cargo exclusivo del Proveedor, todas las medidas razonables necesarias para remediar esas deficiencias dentro de un plazo acordado.

2.6 Incidentes de seguridad.

2.6.1 El Proveedor informará a Amazon tan pronto como sea posible, pero no más tarde de 24 horas después de que el Proveedor tenga conocimiento o sospecha de cualquier acceso, recopilación, adquisición, uso, transmisión, revelación, corrupción o pérdida no autorizados de Información de Amazon o de violación de cualquier Sistema de información de Amazon (un "**Incidente de seguridad**"). El Proveedor remediará cada Incidente de seguridad de forma oportuna y proporcionará a Amazon detalles escritos sobre la investigación interna del Proveedor con respecto a cada Incidente de seguridad. Cuando la legislación vigente lo permita, el Proveedor acepta no notificar a ninguna autoridad reguladora o cliente en nombre de Amazon, a menos que Amazon solicite específicamente por escrito que el Proveedor lo haga, y Amazon se reserva el derecho de revisar y aprobar la forma y el contenido de cualquier notificación antes de que se facilite a cualquier parte. El Proveedor cooperará y colaborará con Amazon para formular y ejecutar un plan para rectificar todos los Incidentes de seguridad confirmados.

2.6.2 En la medida en que lo permita la legislación vigente, en caso de que el Proveedor reciba un requerimiento u orden de un organismo gubernamental (como una citación, orden judicial u orden de registro) que pida datos que incluyan cualquier Información de Amazon, el Proveedor proporcionará aviso suficiente a Amazon para permitir que Amazon solicite una orden de protección u otro recurso apropiado.

2.7 Disposiciones generales Amazon tiene la entera discreción de tomar todas las decisiones aplicables en virtud de esta Política de seguridad. Cualquier relación de ejemplos después de "incluido" o "p. ej." es ilustrativa y no exhaustiva. Todas las referencias a normas para los requisitos de seguridad en virtud de esta Política de seguridad se refieren a las normas especificadas y sus respectivas versiones posteriores o versiones equivalentes, en la medida en que se actualicen, a menos que Amazon especifique lo contrario.