La traducción a continuación se proporciona únicamente con fines informativos. En caso de discrepancias, incoherencias o conflictos entre esta traducción y la última versión en inglés actualizada (incluso debido a retrasos en la traducción), prevalecerá la versión en inglés.

POLÍTICA DE SEGURIDAD PARA PROVEEDORES DE AMAZON

Última actualización: 11 de septiembre de 2024

1. **ALCANCE.** El Proveedor cumplirá con estos requisitos de seguridad (la "Política de Seguridad"). Esta Política de Seguridad no limita ninguna de las otras obligaciones contractuales o legales del Proveedor. En la medida en que exista un conflicto entre esta Política de Seguridad y otros acuerdos entre el Proveedor y Amazon, el Proveedor cumplirá con los requisitos más restrictivos que protejan mejor la Información de Amazon.

2. **ACTUALIZACIONES**

2.1 Amazon podrá realizar actualizaciones comercialmente razonables a esta Política de Seguridad de vez en cuando, que entrarán en vigencia 30 días después de la fecha de la "Última actualización" de esta Política de Seguridad. El Proveedor acepta quedar sujeto a la Política de Seguridad actualizada una vez que las actualizaciones entren en vigencia.

2.2 Si el Proveedor desea recibir un aviso previo de estas actualizaciones antes de que entren en vigencia, podrá suscribirse para recibir avisos de actualización a través del formulario de suscripción provisto en esta página web de la Política de Seguridad. El Proveedor se asegurará de que toda la información de contacto del Proveedor proporcionada para la suscripción al aviso de actualización esté actualizada y sea precisa en todo momento. Se considerará que el Proveedor ha recibido cualquier aviso de actualización cuando se envíe por correo electrónico, independientemente de si el Proveedor recibe o no la notificación de actualización.

3. **PROPÓSITO PERMITIDO.**

3.1 **Autorización expresa**. El Proveedor solo podrá tratar 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 (en adelante, "Propósito Permitido").

3.2 **Retención de datos**. El Proveedor conservará la Información de Amazon solo para los fines del Propósito Permitido y durante el tiempo que sea necesario para dicho propósito.

3.3 **Limitaciones expresas.** El Proveedor no podrá, de ninguna otra manera, realizar lo siguiente: (a) tratar ninguna Información de Amazon, incluso si está Anonimizada; (b) transferir, alquilar, intercambiar, comerciar, vender, prestar, arrendar o, de otra manera, distribuir o poner a disposición de terceros, ninguna Información de Amazon, incluso si está Anonimizada; o (c) desarrollar, entrenar o mejorar cualquier modelo de inteligencia artificial (IA) o aprendizaje automático (Machine Learning, ML) utilizando Información de Amazon, incluso si está Anonimizada.

4. **REQUISITOS MÍNIMOS DE SEGURIDAD**. El Proveedor mantendrá protecciones físicas, administrativas y técnicas consistentes con las mejores prácticas de la industria (incluidas las normas 27001 y 27002 de la Organización Internacional de Normalización (International Organization for Standardization, ISO), el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST), u otros
estándares similares). Las protecciones mantenidas por el Proveedor incluirán los requisitos mínimos descritos a continuación en las Secciones 4.1 a 4.18.

4.1 **Programa escrito de seguridad de la información**. El Proveedor tendrá un programa escrito de seguridad de la información que: (a) incluirá políticas, procedimientos y estándares adecuados que cumplen con los requisitos establecidos en esta Política de Seguridad; (b) designará un punto de contacto de seguridad que es responsable de comunicar y gestionar los problemas de seguridad (incluidos los Incidentes de Seguridad); (c) se revisará al menos una vez al año y se actualizará según sea necesario; y (d) se aplicará al personal. El Proveedor supervisará y hará cumplir su programa de seguridad de la información y abordará los incumplimientos.

La traducción a continuación se proporciona únicamente con fines informativos. En caso de discrepancias, incoherencias o conflictos entre esta traducción y la última versión en inglés actualizada (incluso debido a retrasos en la traducción), prevalecerá la versión en inglés.

4.2 **Administración de parches.** El proveedor mantendrá los Sistemas de Información Cubiertos actualizados con las últimas actualizaciones, correcciones de errores y nuevas versiones. El Proveedor implementará mitigaciones para los activos a los que no se puedan aplicar parches.

4.3 **Registro.** El Proveedor recopilará, gestionará y conservará registros de auditoría, eventos y seguridad, incluidos: (a) los datos de registro sobre todo uso (autorizado y no autorizado) de las cuentas o credenciales de Amazon proporcionadas al Proveedor para un Propósito Permitido, y (b) los datos de registro sobre cualquier suplantación o intento de hacerse pasar por el personal de Amazon o Personal que tenga acceso a la Información de Amazon o a los Sistemas de Información Cubiertos. Dichos registros contendrán datos suficientes para identificar cada evento registrado: (i) el personal o la cuenta que inicia el evento, (ii) la hora del evento y (iii) el sistema, los datos u otro recurso afectado. El Proveedor analizará de manera regular dichos registros para ayudar a detectar e investigar las actividades no autorizadas y recuperarse de ellas.

4.4 **Defensas contra malware.** El Proveedor (a) implementará software anti-malware o un control de seguridad equivalente en todos los Sistemas de Información Cubiertos; (b) mantendrá las actualizaciones, firmas y configuraciones del software anti-malware o control de seguridad equivalente; y (c) configurará sistemas para detectar, prevenir y remediar la instalación, propagación y ejecución de código malicioso o no autorizado.

4.5 **Programa de gestión de riesgos.** El Proveedor tendrá un programa escrito de gestión de riesgos de seguridad de la información, que definirá los procesos para el análisis de riesgos, el tratamiento de riesgos, la aceptación de riesgos y las excepciones.

4.6 **Capacitación de concientización sobre seguridad**. El Proveedor proporcionará capacitación sobre seguridad de la información y privacidad de los datos al Personal al momento de la contratación y al menos una vez al año a partir de entonces. El Proveedor también se asegurará de que el Personal esté informado de manera oportuna sobre las actualizaciones de las políticas de seguridad y privacidad de los datos del Proveedor.

4.7 **Inventario de datos.** El Proveedor documentará y mantendrá información sobre (a) qué Información de Amazon está tratando y (b) cómo y dónde se tratará esa Información de Amazon (p. ej., en un diagrama de arquitectura actualizado). El Proveedor proporcionará esta información a Amazon, si Amazon lo solicita.

4.8 **Pruebas de seguridad.**

4.8.1 El Proveedor realizará pruebas anuales para garantizar que cumpla con los requisitos de esta Política de Seguridad.

4.8.2 El Proveedor realizará pruebas de penetración de sus defensas de seguridad al menos una vez al año. Las pruebas de penetración incluirán lo siguiente: (a) pruebas dentro y fuera de la red del Proveedor, (b) ingeniería social (p. ej., simulaciones de ciberestafa) y (c) pruebas de seguridad para redes inalámbricas. El Proveedor abordará las vulnerabilidades identificadas como parte de su programa de gestión de vulnerabilidades. El Proveedor proporcionará a Amazon los resultados de dichas pruebas de penetración y corrección de vulnerabilidades, si Amazon lo solicita.

4.9 **Seguridad de la red**. El Proveedor protegerá los Sistemas de Información Cubiertos y restringirá el acceso no autorizado a la red, especialmente desde las redes externas. El Proveedor mantendrá y configurará cortafuegos u otros controles de seguridad equivalentes para proteger los sistemas del acceso no autorizado y revisará los conjuntos de reglas de cortafuegos al menos una vez al año para garantizar que existan casos comerciales válidos y documentados para todas las reglas.

4.10 **Entorno adecuado**. El Proveedor solo tratará la Información de Amazon en un entorno adecuado para su propósito y no tratará la Información de Amazon en un entorno de prueba, a menos que lo permita el Acuerdo.

La traducción a continuación se proporciona únicamente con fines informativos. En caso de discrepancias, incoherencias o conflictos entre esta traducción y la última versión en inglés actualizada (incluso debido a retrasos en la traducción), prevalecerá la versión en inglés.

4.11 **Cifrado.** El Proveedor cifrará toda la Información de Amazon en reposo y en tránsito a través de redes externas de acuerdo con las mejores prácticas de la industria. Si la información de Amazon se transmite en redes internas del Proveedor, se transmitirá a través de un protocolo cifrado que cumpla con las mejores prácticas de la industria. El Proveedor gestionará y protegerá las claves de cifrado de acuerdo con las mejores prácticas de la industria.

4.12 **Uso controlado de privilegios administrativos**. El Proveedor gestionará las funciones administrativas de acuerdo con el Marco de Ciberseguridad del NIST o la norma ISO 27002. El Proveedor, como mínimo, separará las cuentas administrativas de las cuentas estándares y restringirá las cuentas administrativas solo a aquellas capacidades necesarias para realizar funciones administrativas. El Proveedor registrará todas las acciones de la cuenta administrativa de manera atribuible a un usuario individual. Las capacidades administrativas proporcionadas a una cuenta estándar se basarán en el privilegio mínimo y se registrarán de una manera atribuible a un usuario individual.

4.13 **Control de acceso.**

4.13.1 **Identificaciones únicas.** El Proveedor asignará identificaciones individuales y únicas al Personal con acceso a la Información de Amazon o a los Sistemas de Información Cubiertos, incluidas las cuentas con acceso administrativo.

4.13.2 "**Necesidad de saber" solamente.** El Proveedor restringirá el acceso a la Información de Amazon y a los Sistemas de Información Cubiertos solo al Personal que tenga una "necesidad de saber" para un Propósito Permitido.

4.13.3 **Revisión del acceso del usuario.** El Proveedor revisará, al menos una vez cada 90 días, la lista de Personal y servicios con acceso a la Información de Amazon y a los Sistemas de Información Cubiertos, y eliminará el acceso de las cuentas que ya no lo requieran.

4.13.4 **Inicio de sesión único (Single Sign-On, SSO**). Cualquier servicio del Proveedor que requiera autenticación del personal de Amazon deberá integrarse con un proveedor de identidad de Amazon (p. ej., Amazon Federate) para proporcionar dicha autenticación. Dichos servicios no deberán usar las credenciales proporcionadas o administradas por el Proveedor para la autenticación.

4.14 **Gestión de contraseñas.**

4.14.1 **Contraseñas fuertes.** El Proveedor no utilizará los valores predeterminados suministrados por el fabricante para las contraseñas del sistema y otros parámetros de seguridad en ningún Sistema de Información Cubierto. El Proveedor exigirá y garantizará el uso de "contraseñas fuertes" aplicadas por el sistema de acuerdo con las mejores prácticas descritas en el NIST SP 800-63B en todos los Sistemas de Información Cubiertos. El Proveedor requerirá que todas las contraseñas y credenciales de acceso se mantengan confidenciales y no se compartan entre el Personal.

4.14.2 **Bloqueo.** El Proveedor mantendrá y aplicará el "bloqueo de cuenta" y desactivará las cuentas con acceso a la Información de Amazon o a los Sistemas de Información Cubiertos cuando una cuenta exceda no más de diez (10) intentos consecutivos de acceso con contraseña incorrecta.

4.15 **Acceso remoto; autenticación multifactor.** El Proveedor implementará la autenticación multifactor (es decir, requerirá al menos dos factores para autenticar a un usuario) para el acceso remoto a cualquier red, sistema, aplicación u otro activo del Proveedor.

4.16 **Acceso "en masa".** Para los fines de esta sección, el acceso "en masa" significa acceder a los datos mediante consultas a bases de datos, generación de informes o cualquier otra transferencia masiva de datos.

La traducción a continuación se proporciona únicamente con fines informativos. En caso de discrepancias, incoherencias o conflictos entre esta traducción y la última versión en inglés actualizada (incluso debido a retrasos en la traducción), prevalecerá la versión en inglés.

4.16.1 El Proveedor no accederá ni permitirá el acceso a la Información de Amazon “en masa”, ya sea que la Información de Amazon esté en una base de datos controlada por Amazon o el Proveedor, o esté almacenada mediante cualquier otro método, incluido el almacenamiento en archivos (por ejemplo, archivos planos), excepto que se establezca expresamente en el Acuerdo o que Amazon establezca expresamente lo contrario por escrito.

4.16.2 Cuando Amazon autorice el acceso “en masa”, el Proveedor: (a) limitará dicho acceso solo al Personal especificado con una “necesidad de saber” y (b) requerirá autorización explícita y registro de dicho acceso de acuerdo con los requisitos de la Sección 4.3. El Proveedor proporcionará a Amazon todos los registros sobre el acceso “en masa” a los que se hace referencia en esta sección, si Amazon lo solicita de conformidad con las revisiones de seguridad de la Sección 10 o los Incidentes de Seguridad de la Sección 11.

4.17 Separación de datos. El Proveedor separará física o lógicamente la Información de Amazon de la información del Proveedor y de cualquier tercero en todo momento. Si la separación no es posible, el Proveedor se asegurará de que la Información de Amazon se distinga de otra información para fines de registro, eliminación y respuesta a incidentes.

4.18 **Seguridad del Personal del Proveedor.**

4.18.1 El Proveedor tomará todas las precauciones razonables para garantizar que el Personal al que se le otorgue acceso a la Información de Amazon mantenga su confidencialidad y la utilice solo para un Propósito Permitido. Estas precauciones deberán incluir la imposición de requisitos de confidencialidad a través de un acuerdo de confidencialidad o una política del Proveedor.

4.18.2 Para cualquier Personal que (a) ya no necesite acceso a la Información de Amazon o (b) ya no sea elegible como Personal del Proveedor, el Proveedor terminará el acceso a la Información de Amazon y a los Sistemas de Información Cubiertos en el transcurso de 24 horas. Si algún integrante del Personal conserva el acceso a la Información de Amazon o a los Sistemas de Información Cubiertos más de 24 horas después de que (a) o (b) ocurran, el Proveedor notificará a Amazon sobre este acceso continuo en el transcurso de 24 horas de que el Proveedor tome conocimiento de ello y enviará un correo electrónico a security@amazon.com.

5. **REQUISITOS DE SEGURIDAD DE LOS PAGOS**. Si el Proveedor tiene acceso a los datos del titular de la tarjeta de pago o trata esos datos en un futuro, deberá cumplir con la última versión del Estándar de Seguridad de los Datos de la Industria de Tarjetas de Pago (Payment Card Industry Data Security Standard, PCI DSS).

6. **SUBCONTRATISTAS.**

6.1 El Proveedor no subcontratará ni delegará ninguna de sus obligaciones en virtud de esta Política de Seguridad a ningún tercero (en conjunto, “Subcontratistas”) sin el consentimiento previo por escrito de Amazon. Sin perjuicio de la existencia o los términos de cualquier subcontrato o delegación, el Proveedor seguirá siendo responsable del cumplimiento total de sus obligaciones en virtud de esta Política de Seguridad. Los términos y condiciones de esta Política de Seguridad serán vinculantes para los Subcontratistas del Proveedor y el Personal de los Subcontratistas.

6.2 Si el Proveedor utiliza Sistemas de Información Cubiertos del Subcontratista, el Proveedor realizará una revisión de seguridad de los Sistemas de Información Cubiertos del Subcontratista y sus controles de seguridad y, si Amazon lo solicita, proporcionará a Amazon informes periódicos sobre los controles de seguridad de los Sistemas de Información Cubiertos del Subcontratista en el formato que Amazon solicite (p. ej., Declaración de Normas para Trabajos de Atestificación N.º 16 [Statement on Standards for Attestation Engagements, SSAE 16]).

7. ACCESO A LOS SISTEMAS DE INFORMACIÓN ADMINISTRADOS POR AMAZON. Amazon podrá otorgar al Proveedor el derecho de tratar la Información de Amazon a través de portales web u otros sitios web o extranets no públicas (cada uno, un “Sistema de Información Administrado por Amazon”) solo para el Propósito Permitido. Si

La traducción a continuación se proporciona únicamente con fines informativos. En caso de discrepancias, incoherencias o conflictos entre esta traducción y la última versión en inglés actualizada (incluso debido a retrasos en la traducción), prevalecerá la versión en inglés.

Amazon permite que el Proveedor trate cualquier Información de Amazon mediante el uso de un Sistema de Información Administrado por Amazon, el Proveedor y su personal deberán cumplir con los siguientes requisitos:

7.1 **Cuentas.** El Proveedor se asegurará de que el Personal del Proveedor utilice solo la cuenta (o cuentas) del Sistema de Información Administrado por Amazon que Amazon designó para cada persona y requerirá que el Personal del Proveedor mantenga sus credenciales de acceso confidenciales y no las comparta.

7.2 **Sistemas**. El Proveedor y su Personal utilizarán los Sistemas de Información Administrados por Amazon solo a través de sistemas o aplicaciones informáticos o de tratamiento (a) que ejecuten sistemas operativos administrados por el Proveedor y que utilicen cifrado de disco completo, y (b) que cumplan con los requisitos de las Secciones 4.2 (Administración de parches), 4.4 (Defensas contra malware) y 4.9 (Seguridad de la red).

7.3 **Restricciones.** El Proveedor y el Personal no descargarán, copiarán ni almacenarán de forma permanente ninguna Información de Amazon de ningún Sistema de Información Administrado por Amazon en ningún medio, a menos que Amazon lo apruebe previamente por escrito.

7.4 **Terminación de la cuenta**. Para cualquier integrante del Personal que (a) ya no necesite acceso al Sistema de Información Administrado por Amazon o (b) ya no sea elegible como Personal del Proveedor (por ejemplo, el individuo deja el empleo del Proveedor), el Proveedor terminará inmediatamente (en el transcurso de un máximo de 24 horas) el acceso de dicho Personal al Sistema de Información Administrado por Amazon o notificará a Amazon para eliminar dicho acceso.

8. **DOMINIOS O URLS DE AMAZON.** Cualquier dominio o URL que el Proveedor proporcione para el uso exclusivo de Amazon no deberá ser emitido por el Proveedor a ningún tercero, ni reutilizado por este, durante al menos 5 años después de la rescisión del Acuerdo.

9. DEVOLUCIÓN Y ELIMINACIÓN DE LOS DATOS; DESTRUCCIÓN DE MEDIOS CONFORME A LAS NORMAS VIGENTES.

9.1 **Devolución y eliminación de datos**. Si Amazon lo solicita, el proveedor devolverá rápidamente toda la Información de Amazon (pero en un plazo no mayor a 72 horas) a Amazon y la eliminará de forma permanente y segura, de acuerdo con el aviso de Amazon que requiera la devolución y/o eliminación. El Proveedor también eliminará de forma permanente y segura todas las instancias en vivo (en línea o accesibles a la red) de la Información de Amazon en el transcurso de los 30 días posteriores a la finalización del Propósito Permitido o la rescisión o el vencimiento del Acuerdo, lo que ocurra primero. Si Amazon lo solicita, el Proveedor certificará por escrito que toda la Información de Amazon se ha eliminado. Para mayor claridad, esta sección no se aplicará a las copias de archivo de conformidad con la Sección 9.3.

9.2 **Desinfección de datos**. Toda la Información de Amazon eliminada por el Proveedor se eliminará de acuerdo con las Recomendaciones Mínimas de Desinfección incluidas en el NIST SP 800-88 Revisión 1, Pautas para la Desinfección de Medios (18 de diciembre de 2014, Apéndice A) para limpiar el tipo de dispositivo relevante. En ausencia de orientación en la norma NIST SP 800-88 para el tipo de dispositivo relevante, el Proveedor destruirá el dispositivo que contiene la Información de Amazon de una de las siguientes maneras: mediante (a) la limpieza según se define en la norma del NIST SP 800-88, (b) la destrucción según se define en la norma del NIST SP 800-88, o (c) a través de otros estándares que Amazon pueda requerir en función de la clasificación y sensibilidad de la Información de Amazon.

9.3 **Copias de archivo.** Si la ley exige que el Proveedor conserve copias de archivo de la Información de Amazon, el Proveedor no utilizará la Información de Amazon archivada para ningún otro propósito y seguirá estando vinculado por todas sus obligaciones en virtud de esta Política de Seguridad. Toda información archivada de Amazon deberá cifrarse y almacenarse cuando el Sistema de Información Cubierto que aloja o almacena la Información de Amazon cifrada no tenga acceso a una copia de la clave (o claves) utilizada para el

La traducción a continuación se proporciona únicamente con fines informativos. En caso de discrepancias, incoherencias o conflictos entre esta traducción y la última versión en inglés actualizada (incluso debido a retrasos en la traducción), prevalecerá la versión en inglés.

cifrado. Cualquier copia de seguridad fuera de línea o “en frío” (es decir, no disponible para uso inmediato o interactivo) deberá almacenarse en una instalación físicamente segura.

9.4 **Destrucción de medios conforme a las normas vigentes**. Antes de desechar cualquier hardware, software o cualquier otro medio que contenga, o haya contenido en cualquier momento, Información de Amazon, el Proveedor realizará una destrucción completa conforme a las normas vigentes del hardware, software u otros medios de acuerdo con la norma del NIST SP 800-88, Apéndice A. Este requisito de destrucción no se aplicará a los medios de almacenamiento a los que el Proveedor no tenga acceso o control físico. En tales casos, el Proveedor se asegurará de que la Información de Amazon se elimine de manera segura cuando ya no sea necesaria; para hacerlo, seguirá las mejores prácticas de la industria.

> 9.4.1 A menos que el Proveedor reciba el consentimiento expreso por escrito y por adelantado de Amazon, el Proveedor no venderá, revenderá, donará, restaurará ni transferirá de otro modo ningún hardware, software u otro medio que en algún momento haya contenido Información de Amazon a menos que se haya
> destruido de manera forense de acuerdo con esta Sección.

10. **REVISIONES DE SEGURIDAD**. Si Amazon lo solicita, el Proveedor hará lo siguiente: (a) completará una evaluación de riesgos de Amazon, (b) proporcionará evidencia solicitada por Amazon para validar el cumplimiento del Proveedor con esta Política de Seguridad, (c) permitirá que Amazon o un tercero designado en su nombre realice una revisión del cumplimiento del Proveedor con esta Política de Seguridad, y/o (d) proporcionará a Amazon todos los registros a los que se hace referencia en la Sección 4.3 en el formato del Marco de Esquema de Ciberseguridad Abierto (Open Cybersecurity Schema Framework, OCSF). Si el Proveedor requiere que cualquier evidencia se revise en persona o en una inspección en el sitio en lugar de proporcionar dicha evidencia para la revisión remota de Amazon, el Proveedor asumirá el costo del viaje y otros gastos relacionados con dicha inspección en el sitio. Si alguna evaluación o revisión identifica algún hallazgo, el Proveedor, a su exclusivo costo y cargo, tomará rápidamente todas las medidas razonables necesarias para remediar dichos hallazgos a satisfacción razonable de Amazon y dentro de un plazo acordado.

11. **INCIDENTES DE SEGURIDAD.**

11.1 **Aviso de Incidente de Seguridad.** El Proveedor notificará a Amazon lo antes posible, pero a más tardar 24 horas después de que el Proveedor sepa o crea razonablemente que ha habido acceso, recopilación, adquisición, uso, transmisión, divulgación, corrupción o pérdida no autorizados de la Información de Amazon o de un Sistema de Información Cubierto (un “Incidente de Seguridad”). El Proveedor enviará notificaciones de Incidente de Seguridad a security@amazon.com.

11.2 **Plan de respuesta a incidentes.** El Proveedor mantendrá un plan de respuesta a incidentes por escrito y proporcionará una copia de este a Amazon cuando lo solicite. El Proveedor remediará cada Incidente de Seguridad de manera oportuna; para hacerlo, seguirá el plan de respuesta a incidentes escrito del Proveedor y las mejores prácticas de la industria. El Proveedor revisará, probará y (si es necesario) actualizará el plan al menos una vez al año.

11.3 **Cooperación con Amazon.** El Proveedor (a) ayudará a Amazon en la investigación del Incidente de Seguridad; (b) facilitará entrevistas con el Personal y otras personas involucradas en el Incidente de Seguridad o respuesta; (c) mantendrá detalles escritos de la investigación y respuesta del Incidente de Seguridad del Proveedor; y (d) pondrá a disposición de Amazon todos los registros, archivos, informes de datos, informes forenses, informes de investigación y otros materiales relevantes solicitados por Amazon.

11.4 **Notificaciones de terceros.** A menos que la ley exija lo contrario, el Proveedor obtendrá el consentimiento previo por escrito de Amazon antes de realizar lo siguiente: (a) notificar a cualquier tercero (incluida cualquier autoridad reguladora o cliente) sobre cualquier Incidente de Seguridad; o (b) identificar a Amazon en cualquier

notificación o declaración pública con respecto a cualquier Incidente de Seguridad. A menos que la ley exija lo contrario, Amazon tendrá derecho a determinar si se debe proporcionar un aviso de un Incidente de Seguridad a un tercero y la forma, el tiempo y el contenido de dicho aviso.

12. **AVISO DE PROCESO LEGAL.** Excepto cuando lo prohíba la ley, si se busca Información de Amazon en respuesta a un proceso legal u otra ley aplicable, el Proveedor proporcionará un aviso suficiente a Amazon para permitir que Amazon busque una orden de protección u otro recurso apropiado.

13. **DEFINICIONES.**

13.1 "**Acuerdo**" significa cualquier acuerdo que haga referencia a esta Política de Seguridad.

13.2 "**Amazon**" significa Amazon.com, Inc. y sus afiliadas.

13.3 "**Información de Amazon**" significa: (a) toda la Información Confidencial de Amazon (según se define en cualquier otro acuerdo entre las partes); (b) todos los datos, registros, archivos, contenido o información, en cualquier forma, adquirida, accedida, recopilada, recibida, almacenada o mantenida por el Proveedor o sus filiales, de Amazon o en su nombre, o de otro modo en relación con el Acuerdo; e (c) información derivada de (a) o (b), incluso si se Anonimiza.

13.4 "**Anonimizar**" significa Tratar cualquier dato o información (incluida la Información de Amazon) de una manera o forma que no identifique a Amazon o permita su identificación o no le sea atribuible de otro modo, o a cualquier usuario, identificador de dispositivo, fuente, producto, servicio, contexto o marca de estos.

13.5 "**Sistema de Información Cubierto**" significa cualquier sistema que el Proveedor utilice para tratar la Información de Amazon.

13.6 "**Personal**" se refiere a los empleados, agentes, Subcontratistas y otros usuarios autorizados del Proveedor o del Subcontratista de sus sistemas y recursos de red.

13.7 "**Tratar**" significa realizar cualquier operación con datos, como acceso, uso, recopilación, recepción, almacenamiento, alteración, transmisión, difusión o puesta a disposición, eliminación o destrucción.

13.8 "**Proveedor**" significa cada proveedor, vendedor o contratista definido en un Acuerdo y cualquier otro proveedor sujeto a un Acuerdo.