NOTA: Esta traducción se ha generado de forma automática y se ofrece únicamente para la comodidad de los usuarios. Esta traducción generada automáticamente no ofrece la misma calidad que la traducción humana y puede contener errores. Esta traducción se proporciona "TAL CUAL" y sin ninguna garantía en cuanto a la exactitud, la exhaustividad o la fiabilidad de la misma. Si existiera alguna incoherencia entre la versión en lengua inglesa de este documento y cualquier versión traducida, prevalecerá la versión en lengua inglesa.

ANEXO DE PROCESAMIENTO DE DATOS

Fecha De Revisión: 20 de enero de 2022

Si este Anexo de procesamiento de datos ("**Anexo**") se incorpora expresamente como referencia en un Acuerdo ("**Acuerdo principal**") entre Sophos Limited, una empresa registrada en Inglaterra y Gales con el número 2096520, con su domicilio social en The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, Reino Unido ("**Proveedor**") y un cliente del Proveedor ("**Cliente**"), este Anexo forma parte del Acuerdo Principal y es efectivo entre el Proveedor y el Cliente.

1. PREÁMBULO

1.1 Las partes han firmado el Acuerdo Principal en relación con la provisión por parte del Proveedor al Cliente de determinados productos y/o servicios (colectivamente, "**Productos**").

1.2 Si el Acuerdo principal es un Acuerdo de MSP de forma similar al Acuerdo de MSP ubicado en https://www.sophos.com/es-es/legal/sophos-msp-partner-terms-and-conditions.aspx ("**MSP Acuerdo**"), el Cliente es un proveedor de servicios gestionados ("**MSP**"). Si el Acuerdo Principal es un Acuerdo OEM bajo el cual el Cliente está autorizado a distribuir, sublicenciar o poner a disposición de los Productos Proveedores de terceros en combinación con los productos del Cliente como parte de una unidad empaquetada ("**Acuerdo OEM**"), el Cliente es un fabricante de equipos originales ("**OEM**"). De lo contrario, el cliente es un usuario final ("**Usuario final**").

1.3 La provisión de los Productos puede incluir la recolección, procesamiento y uso de los Datos del Controlador por parte del Proveedor para el Cliente. El presente Addendum establece las obligaciones de las partes con respecto a dicho procesamiento de datos y complementa los términos y condiciones del Acuerdo Principal.

1.4 El Acuerdo Principal, este Anexo y los documentos a los que se hace referencia expresamente en el Acuerdo Principal y este Anexo constituirán el Acuerdo completo entre las partes en relación con los datos personales recopilados, procesados y utilizados por el Proveedor en nombre del Cliente en relación con el Acuerdo Principal, y reemplazará todos los acuerdos, arreglos y entendimientos anteriores entre las partes con respecto a ese tema.

2. DEFINICIONES

2.1 En este Anexo, los siguientes términos tendrán los siguientes significados:

Por «**Leyes aplicables de protección de datos**» se entenderá i) el Reglamento 2016/679 de la UE del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos (Reglamento general de protección de datos o «**GDPR**»); (ii) la Directiva sobre privacidad electrónica (Directiva 2002/58/CE de la UE); y (iii) toda la legislación nacional aplicable sobre protección de datos, incluida la legislación que se haya establecido en virtud de (i) o (ii); en cada caso que pueda modificarse o sustituirse de vez en cuando.

"**Beneficiario**" tiene el significado que se le da en el MSP Acuerdo.

"**Controlador**" significa: (a) el Cliente, si el Cliente es un Usuario Final; (b) el Beneficiario, si el Cliente es un MSP; o (c) el Cliente Final, si el Cliente es un OEM.

"**Datos del controlador**" hace referencia a todos y cada uno de los datos personales para los que el controlador es el controlador según las leyes de protección de datos aplicables.

"**Cliente final**" tiene el significado que se le da en el Acuerdo del OEM.

Por «**Europa**» (y «**Europa**») se entenderá i) los Estados miembros del Espacio Económico Europeo ("**EEE**"), y ii) con efecto inmediato a partir de la fecha en que la legislación de la Unión Europea ya no se aplica al Reino Unido, el Reino Unido.

Por "cláusulas contractuales estándar de la UE" o "CCE de la UE" se entiende las cláusulas contractuales estándar para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo aprobado por la decisión de aplicación de la Comisión Europea (UE) 2021/914 de 4 de junio de 2021;

"Cláusulas de controlador a procesador de la UE" se refiere a las cláusulas del Módulo Dos a las CCE de la UE;

"Cláusulas de procesador a procesador de la UE" se refiere a las cláusulas del Módulo Tres a los PCC de la UE.

" **Productos alojados**" se refiere a los productos enumerados en **el Anexo 3**.

"**Incumplimiento de datos personales**" se refiere a un incumplimiento de la seguridad (distinto de los causados por el Cliente o sus usuarios) que lleve a la destrucción, pérdida, alteración, divulgación o acceso accidentales o ilegales a, Datos del controlador procesados por el Proveedor en virtud de este Anexo.

"**Addendum del Reino Unido**" significa el addendum a los SCCs de la UE que figura en el Anexo cuando sea aplicable.

2.2 En este Anexo, los términos en minúsculas «**controlador**», «**procesador**», «**asunto de los datos**», «**datos personales**» y «**procesamiento**» (y sus derivados) tendrán los significados que se indican en la Ley de protección de datos aplicable.

3. ALCANCE

3.1 El objeto y la duración del tratamiento de los Datos del Controlador por parte del Proveedor, incluida la naturaleza y el propósito del procesamiento, los tipos de Datos del Controlador que se van a procesar y las categorías de sujetos de los datos, serán los descritos en: (i) este Apéndice; (ii) el Acuerdo Principal; (iii) cualquier instrucción en **el Anexo 1**; Y (v) las instrucciones del Cliente emitidas de conformidad con la Cláusula 4.

3.2 El Cliente es responsable de garantizar (i) que el Controlador tenga una base legal para el procesamiento de los Datos del Controlador que será realizado por el Proveedor en su nombre, Y (ii) que el Contralor ha obtenido todos los consentimientos necesarios de sujetos de datos que puedan ser necesarios para el procesamiento de los Datos del Controlador por parte del Cliente y el Proveedor (incluidos, pero sin limitación, en relación con categorías especiales de datos); Y (iii) que de otro modo cumple y garantizará que sus instrucciones al Proveedor para el procesamiento de los Datos del Controlador cumplan en todos los aspectos las leyes de protección de datos aplicables.

3.3 El resto de las disposiciones de este Anexo describen las obligaciones respectivas de las partes en relación con los Datos del Controlador para los que: (i) el cliente es el controlador y el proveedor es el procesador, si el cliente es un usuario final; o (ii) el cliente es el procesador de un controlador de terceros y el proveedor es el subprocesador, si el cliente es un MSP o OEM.

4. INSTRUCCIONES PARA EL CLIENTE

4.1 El Proveedor procesará los Datos del Controlador de acuerdo con las instrucciones de procesamiento documentadas del Cliente, según se establece exclusivamente en la Cláusula 3.1 , excepto:

(a) Cuando se acuerde lo contrario por escrito entre el Proveedor y el Cliente; o.

(b) Cuando lo exija la ley a la que está sujeto el Proveedor (en cuyo caso, el Proveedor informará al Cliente de ese requisito legal antes de su procesamiento, a menos que dicha ley prohíba el suministro de dicha información).

4.2 Si el Proveedor se da cuenta de que las instrucciones de procesamiento del Cliente infringen las leyes de protección de datos aplicables (sin imponer ninguna obligación al Proveedor de supervisar activamente el cumplimiento del Cliente), notificará inmediatamente al Cliente lo mismo y suspenderá el procesamiento de los Datos del Controlador.

5. OBLIGACIONES DEL PROVEEDOR

5.1 Todo el personal del Proveedor que procese los Datos del Controlador deberá estar debidamente formado con respecto a sus obligaciones de protección de datos, seguridad y confidencialidad, y estará sujeto a obligaciones escritas de mantener la confidencialidad.

5.2 El Proveedor, a su propio costo, implementará las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo y proteger los Datos del Controlador contra una Incumplimiento de Datos Personales. Tales medidas tendrán en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines de la tramitación, así como el riesgo de que varyan las probabilidades y la severidad de los derechos y libertades de las personas físicas, a fin de garantizar un nivel de seguridad adecuado al riesgo. En particular, las medidas adoptadas por el Proveedor incluirán las descritas en el **Anexo 2** del presente Anexo. El Proveedor puede cambiar o modificar las medidas técnicas y organizativas descritas en el **Anexo 2** sin el consentimiento previo por escrito del Cliente, siempre que el Proveedor mantenga al menos un nivel de protección equivalente. A petición del Cliente, el Proveedor proporcionará una descripción actualizada de las medidas técnicas y organizativas en el formulario que se presenta en el **Anexo 2**.

5.3 El Proveedor seguirá los requisitos especificados en la Cláusula 7 para contratar a cualquier subprocesador para procesar los Datos del Controlador.

5.4 El Proveedor seguirá los requisitos especificados en la Cláusula 8 para ayudar al Cliente a responder a consultas de terceros, incluidas las solicitudes de los sujetos de datos para ejercer sus derechos conforme a las leyes de protección de datos aplicables.

5.5 Al confirmar la aparición de cualquier violación de los datos personales, el Proveedor informará al Cliente sin demora indebida y proporcionará toda la información y cooperación oportunas que el Cliente pueda requerir razonablemente para el Cliente (y, si el Cliente es un MSP o OEM, su Controlador) Cumplir sus obligaciones de notificación de infracciones de datos en virtud de (y de acuerdo con los plazos exigidos por) la Ley de protección de datos aplicable. Además, el Proveedor tomará todas las medidas y acciones necesarias para remediar o mitigar los efectos de la Incumplimiento de los Datos

Personales y mantendrá informado al Cliente de todos los desarrollos relacionados con la Incumplimiento de los Datos Personales.

5.6 El Proveedor proporcionará al Cliente (o, si el Cliente es un MSP o OEM, su Controlador) toda la asistencia razonable y oportuna que el Cliente (o, según corresponda, el Controlador) pueda requerir para llevar a cabo una evaluación de impacto en la protección de datos y, si es necesario, consulte con su autoridad de protección de datos pertinente. Dicha asistencia se proporcionará a expensas del Cliente.

5.7 El Proveedor eliminará los Datos del Controlador del Controlador en un plazo razonable tras la terminación o expiración del presente Anexo, en cada caso si y en la medida en que lo permita la legislación europea aplicable.

5.8 El Proveedor seguirá los requisitos especificados en la Cláusula 6 para proporcionar al Cliente (y, si el Cliente es un MSP o OEM, su Controlador) la información necesaria para demostrar el cumplimiento por parte del Proveedor de las obligaciones establecidas en este Anexo.

6. DERECHOS DE AUDITORÍA DEL CLIENTE

6.1 El Cliente reconoce que el Proveedor es auditado regularmente de conformidad con las normas SSAE 18 SOC 2 por auditores independientes de terceros. Previa solicitud, el Proveedor deberá proporcionar al Cliente una copia de su informe de auditoría del SOC 2, que estará sujeta a las disposiciones de confidencialidad del Acuerdo Principal como información confidencial del Proveedor. El Cliente reconoce y acepta que el auditor externo que haya creado dicho informe ("**Autor**") no acepta ninguna responsabilidad o responsabilidad con el Cliente o con los auditores del Cliente a menos que y hasta que el Cliente entresida un Acuerdo de deber de cuidado separado con el Autor. El Proveedor también responderá a cualquier pregunta de auditoría por escrito que le envíe el Cliente, siempre que el Cliente no ejerza este derecho más de una vez al año.

7. SUB

7.1 El Cliente da su consentimiento a los subprocesadores existentes del Proveedor en la fecha de este Anexo, que se enumeran en https://www.sophos.com/en-us/legal ("**Lista de subprocesadores**"). El Proveedor no subcontratará el procesamiento de los Datos del Controlador a ningún subprocesador adicional de terceros (cada uno un "**Nuevo Subprocesador**") sin notificación previa al Cliente. El Proveedor notificará con antelación la adición de cualquier Nuevo Subprocesador (incluidos los detalles generales del procesamiento que realiza o realizará), que podrá notificarse mediante la publicación de los detalles de dicha adición en la Lista de Subprocesadores. Si el Cliente no se opone por escrito a la designación de un nuevo subprocesador por parte del Proveedor (por motivos razonables relacionados con la protección de los Datos del Controlador) en un plazo de 30 días desde que el Proveedor agregue dicho nuevo subprocesador a la Lista de subprocesadores, El Cliente acepta que se considerará que ha dado su consentimiento a ese Nuevo Subprocesador. Si el Cliente presenta dicha objeción por escrito al Proveedor, el Proveedor notificará por escrito al Cliente en un plazo de 30 días que: (i) el Proveedor no utilizará el Nuevo Subprocesador para procesar los Datos del Controlador; o (ii) el Proveedor no puede o no está dispuesto a hacerlo. Si se da la notificación que figura en el apartado ii), el Cliente podrá, en un plazo de 30 días a partir de dicha notificación, Elegir rescindir este Anexo y el Acuerdo Principal en cuanto al procesamiento afectado previa notificación por escrito al Proveedor y al Proveedor sólo para los clientes ubicados dentro del Área Económica Europea y Reino Unido, autorizar un reembolso prorrateado o crédito de cualquier tarifa prepagada por el período restante después de la terminación. Sin embargo, si no se proporciona dicho aviso de terminación dentro de ese plazo, se considerará que el Cliente ha dado su consentimiento al Nuevo Subprocesador. El Proveedor impondrá las condiciones de protección de datos a los Nuevos Subprocesadores para proteger los Datos del Controlador con el mismo estándar

que se establece en este Anexo y el Proveedor seguirá siendo totalmente responsable de cualquier incumplimiento de este Anexo causado por dicho subprocesador.

8. INVESTIGACIONES DE TERCEROS

8.1 El Proveedor proporcionará toda la asistencia razonable y oportuna al Cliente (o, si el Cliente es un MSP o OEM, el Controlador), a expensas del Cliente, para permitir al Cliente responder a: i) cualquier solicitud de datos sujetos a ejercer cualquiera de sus derechos en virtud de la Ley de protección de datos aplicable (incluidos sus derechos de acceso, corrección, objeción, borrado y portabilidad de datos, según corresponda); Y (ii) cualquier otra correspondencia, consulta o queja recibida de un sujeto de datos, regulador u otro tercero en relación con el procesamiento de los Datos del Controlador. Si dicha solicitud, correspondencia, consulta o queja se hace directamente al Proveedor, el Proveedor informará inmediatamente al Cliente proporcionando todos los detalles de la misma.

9. TRANSFERENCIAS INTERNACIONALES DE DATOS

9.1 Algunos productos permiten al cliente elegir si alojar los datos del controlador de dichos productos en centros de datos que puedan estar ubicados en (i) el Espacio Económico Europeo, (ii) el Reino Unido o (iii) los Estados Unidos de América ("**Central Storage Location**"). Esta selección se realiza en el punto de instalación, creación de cuenta o primer uso del Producto correspondiente. Una vez seleccionada, la ubicación de almacenamiento central no se puede modificar en una fecha posterior.

9.2 El Cliente reconoce y acepta que, independientemente de la ubicación de almacenamiento central seleccionada (si procede), los Datos del Controlador se pueden exportar a otras jurisdicciones (dentro y/o fuera del Reino Unido y del Espacio Económico Europeo): (i) al equipo global de técnicos e ingenieros de Sophos para malware, amenazas a la seguridad y análisis de falsos positivos, así como para fines de investigación y desarrollo, (ii) para proporcionar asistencia técnica y al cliente, gestión de cuentas, facturación y otras funciones auxiliares, y (iii) como se describe expresamente en la documentación a la que se hace referencia en la Cláusula 3.1.

9.3 El Proveedor no transferirá los Datos del Controlador (ni permitirá que los Datos del Controlador sean procesados en o desde) Un país fuera de Europa, a menos que la transferencia sea a un país que se considere adecuado según las leyes de protección de datos aplicables o el Proveedor tome las medidas necesarias para garantizar que la transferencia cumple las leyes de protección de datos aplicables, incluidas, por ejemplo, pero sin limitación, Mediante el uso de los SCC de la UE (modificados de vez en cuando).

9.4 La restricción de transferencia descrita en la cláusula 9.3 se aplicará también a las transferencias de datos de controlador del Espacio Económico Europeo al Reino Unido cuando el Reino Unido deje de estar sujeto a la legislación de la Unión Europea.

9.5 Si se aplica la cláusula 9.3 porque el Proveedor o una filial del Proveedor procesará los Datos del Controlador en un país fuera del Reino Unido o del EEE, entonces en tal caso (y sólo en la medida en que se trate de cualquier transferencia de Datos del Controlador, No se dispone de ninguna otra medida reconocida por las leyes de protección de datos aplicables para permitir dichas transferencias (como, sin limitación, Transferir a un destinatario de un país que se considere que proporciona la protección adecuada para los datos personales conforme a las leyes de protección de datos aplicables o transferir a un destinatario que haya logrado la autorización de normas corporativas vinculantes de conformidad con las leyes de protección de datos aplicables)) para cualquier transferencia de datos del controlador, las partes acuerdan que:

a) para las transferencias desde el EEE, se aplicarán las cláusulas del Controlador de la UE al Procesador y dichas cláusulas de la UE se incorporan por la presente adición como referencia;

(b) Para las transferencias desde el Reino Unido, se aplicarán las cláusulas de Controlador a Procesador de la UE (y dichas cláusulas de controlador a procesador de la UE se incorporan por la presente como referencia en este Apéndice) siempre que dichas cláusulas de controlador a procesador de la UE estén sujetas al Apéndice del Reino Unido.

9.6 si se aplica la cláusula 9.3 porque el Proveedor o una filial del Proveedor procesarán los Datos del Controlador en un país fuera del Reino Unido o del EEE en ese caso (y sólo en la medida en que se trate de cualquier transferencia de Datos del Controlador, No se dispone de ninguna otra medida reconocida por las leyes de protección de datos aplicables para permitir dichas transferencias (como, sin limitación, Transferir a un destinatario de un país que se considere que proporciona la protección adecuada para los datos personales conforme a las leyes de protección de datos aplicables o transferir a un destinatario que haya logrado la autorización de normas corporativas vinculantes de acuerdo con las leyes de protección de datos aplicables) cuando (Como se contempla en la Cláusula 3.3(ii))) El Cliente es el procesador de un controlador de terceros y el Proveedor es el subprocesador, las partes acuerdan que:

(a) para las transferencias desde el EEE, se aplicarán las cláusulas de la UE de Procesador a Procesador y dichas cláusulas de la UE se incorporan por la presente adición como referencia;

(b) Para las transferencias desde el Reino Unido, se aplicarán las cláusulas de Procesador a Procesador de la UE (y dichas cláusulas de Procesador a Procesador de la UE se incorporan por la presente como referencia en este Apéndice) siempre que dichas cláusulas de Procesador a Procesador de la UE estén sujetas al Apéndice del Reino Unido.

9.7 El apéndice de las SCC de la UE se completará como se indica en el Anexo 4.

9.8 Para cada módulo de las SCCs de la UE, si procede:

(a) No se aplicará la cláusula de acoplamiento opcional de la Cláusula 7;

(b) Se aplicará la opción 2 de la cláusula 9. El importador de datos notificará al exportador de datos con 30 días de antelación cualquier cambio previsto (mediante adición o sustitución) de la lista de subprocesadores.

(c) En la Cláusula 11, el lenguaje facultativo no se aplicará;

(d) A efectos de las cláusulas 13 a):

- Cuando el exportador de datos esté establecido en un Estado miembro de la UE: La autoridad supervisora responsable de garantizar el cumplimiento por el exportador de datos del Reglamento (UE) 2016/679 en lo que respecta a la transferencia de datos será la autoridad supervisora competente en la que esté establecido el exportador de datos y actuará como autoridad supervisora competente.

(e) A los efectos de la Cláusula 17, las SCC de la UE se regirán por la legislación del Estado miembro de la UE en el que esté establecido el exportador de datos;

(f) A los efectos de la cláusula 18(b), las controversias se resolverán ante los tribunales del Estado miembro de la UE en el que esté establecido el exportador de datos.

10. DURACIÓN

10.1 El presente Anexo comienza con la ejecución por ambas partes del Acuerdo Principal (o la fecha en que el Acuerdo Principal entra en vigor, si es posterior) y continúa hasta la fecha anterior de: (i) la expiración del derecho del Cliente a utilizar y recibir los Productos, tal como se indica en el Acuerdo Principal o en cualquier derecho de licencia asociado; y (ii) la terminación del Acuerdo Principal.

11. OTRAS REGULACIONES

11.1 Las modificaciones y enmiendas a este Apéndice requieren el formulario escrito. Esto también se aplica a los cambios y modificaciones de esta Cláusula 11.1.

11.2 En ningún caso la responsabilidad del Proveedor con respecto al Cliente en relación con cualquier problema que surja de, o en relación con, este Anexo excederá las limitaciones de responsabilidad del Proveedor establecidas en el Acuerdo Principal. Las limitaciones de responsabilidad del Proveedor, tal como se establecen en el Acuerdo Principal, se aplicarán en conjunto tanto en el Anexo Principal como en este Anexo, de forma que se aplique una única limitación del régimen de responsabilidad tanto en el Acuerdo Principal como en este Anexo.

11.3 Este Anexo se regirá e interpretará de acuerdo con las leyes de Inglaterra y Gales, sin tener en cuenta los principios de conflicto de leyes. En la medida en que lo permita la ley aplicable, los tribunales de Inglaterra tendrán jurisdicción exclusiva para determinar cualquier disputa o reclamación que pueda surgir de, bajo o en relación con este Apéndice.

11.4 En caso de conflicto con los términos de este Anexo sobre procesamiento de datos y con los términos de cualquier SCC suscrito por las partes, prevalecerán los términos de las SCC de la UE aplicables.

Anexo 1
Instrucciones de procesamiento de datos

En este Anexo 1 se describe el procesamiento que el Proveedor realizará en nombre del Cliente.

A) Objeto, naturaleza y finalidad de las operaciones de transformación
Los datos del controlador estarán sujetos a las siguientes actividades básicas de procesamiento (especifíquense):

1. Suministro de los Productos comprados por el Cliente bajo y de conformidad con el Acuerdo Principal
2. Proporcionar servicios de gestión de cuentas y asistencia técnica al cliente

El Proveedor proporciona Productos diseñados para detectar, prevenir y gestionar, o ayudar al Proveedor a detectar, prevenir y gestionar amenazas de seguridad dentro o contra sistemas, redes, dispositivos, archivos y otros datos disponibles por el Cliente. El contenido de cualquier información contenida en estos sistemas, redes, dispositivos, archivos y otros datos está determinado exclusivamente por el Cliente y no por el Proveedor.

(B) Duración de las operaciones de procesamiento:
Los datos del controlador se procesarán durante la siguiente duración (especifique):

La duración especificada en el Acuerdo principal (o para el término del Acuerdo principal, si no se especifica lo contrario).

(C) Temas de datos
Los datos del controlador se refieren a las siguientes categorías de sujetos de datos (especifique):

Los sujetos de datos incluyen a las personas sobre las que se proporcionan datos al Proveedor a través de los Productos por parte (o bajo la dirección de) el Cliente o los usuarios finales del Cliente.

(D) Tipos de datos personales
Los datos del controlador se refieren a las siguientes categorías de datos (especifique):

Datos relativos a las personas proporcionadas al Proveedor a través de los Productos, por (o bajo la dirección del) Cliente o por los usuarios finales del Cliente, como la información de contacto

E) Categorías especiales de datos (si procede)
Los datos del controlador se refieren a las siguientes categorías especiales de datos (especifíquense):

A menos que se especifique lo contrario, los Productos del Proveedor no están diseñados para procesar categorías especiales de datos.

Anexo 2
Medidas técnicas y organizativas

Algunas de estas medidas sólo pueden ser pertinentes o aplicables a los productos alojados.

A) Control de acceso físico.

- Sophos tiene una política de control de acceso físico;
- Todo el personal lleva identificación / insignias de acceso;
- Las entradas a las instalaciones están protegidas por insignias o llaves de acceso;
- Las instalaciones se dividen en (i) áreas de acceso público (como áreas de recepción), (ii) áreas de acceso general del personal, y (iii) áreas de acceso restringido a las que sólo puede acceder el personal con una necesidad empresarial expresa;
- Las insignias de acceso y las teclas controlan el acceso a las áreas restringidas dentro de cada instalación de acuerdo con los niveles de acceso autorizados de una persona;
- Los niveles de acceso de las personas son aprobados por los funcionarios superiores y se verifican trimestralmente;
- El personal de recepción y/o de seguridad está presente en las entradas a sitios más grandes;
- Las instalaciones están protegidas por alarmas;
- Los visitantes están pre-registrados y los registros de visitantes se mantienen.

B) Control de acceso al sistema.

- Sophos tiene una política de control de acceso lógica;
- La red está protegida por firewalls en cada conexión a Internet;
- La red interna está segmentada por firewalls basados en la sensibilidad de las aplicaciones;
- LOS IDENTIFICADORES y otros controles de detección y bloqueo de amenazas se ejecutan en todos los firewalls;
- El filtrado del tráfico de red se basa en reglas que aplican el principio de “acceso mínimo”;
- Los derechos de acceso sólo se conceden al personal autorizado en la medida y duración necesarias para desempeñar sus funciones y se revisan trimestralmente;
- El acceso a todos los sistemas y aplicaciones se controla mediante un procedimiento de inicio de sesión seguro;
- Los individuos tienen ID de usuario y contraseñas únicos para su propio uso;
- Las contraseñas se prueban de forma fuerte y los cambios se aplican a contraseñas débiles;
- Las pantallas y las sesiones se bloquean automáticamente después de un período de inactividad;
- Los productos de protección contra malware de Sophos se instalan de serie;
- Se realizan análisis periódicos de vulnerabilidades en sistemas y direcciones IP;
- Los sistemas se aplican en un ciclo regular con un sistema de priorización para realizar un seguimiento rápido de los parches urgentes.

C) Control de acceso a datos.

- Sophos tiene una política de control de acceso lógica;
- Los derechos de acceso sólo se conceden al personal autorizado en la medida y duración necesarias para desempeñar sus funciones y se revisan trimestralmente;
- El acceso a todos los sistemas y aplicaciones se controla mediante un procedimiento de inicio de sesión seguro;
- Los individuos tienen ID de usuario y contraseñas únicos para su propio uso;

- Las contraseñas se prueban de forma fuerte y los cambios se aplican a contraseñas débiles;
- Las pantallas y las sesiones se bloquean automáticamente después de un período de inactividad;
- Los ordenadores portátiles se cifran mediante los productos de cifrado de Sophos;
- Los remitentes deben considerar el cifrado de archivos antes de enviar cualquier correo electrónico externo.

D) Control de entrada.

- El acceso a todos los sistemas y aplicaciones se controla mediante un procedimiento de inicio de sesión seguro;
- Los individuos tienen ID de usuario y contraseñas únicos para su propio uso;
- Los productos Sophos Central utilizan el cifrado de capa de transferencia para proteger los datos en tránsito;
- La comunicación entre el software cliente y el sistema Sophos de fondo se realiza a través de HTTPS para proteger los datos en tránsito, estableciendo la comunicación de confianza a través de certificados y validación del servidor.

E) Control de Subcontratistas.

- Los subcontratistas con acceso a los datos llevan a cabo un procedimiento de investigación de seguridad de TI antes de la incorporación y según se requiera a partir de entonces;
- Los contratos contienen una obligación de confidencialidad y protección de datos adecuada basada en las obligaciones del subcontratista.

F) Control de disponibilidad.

- Sophos protege sus instalaciones frente a incendios, inundaciones y otros peligros medioambientales;
- Los generadores de reserva están disponibles para mantener las fuentes de alimentación en caso de cortes de energía;
- Los centros de datos y las salas de servidores utilizan controles y supervisión del clima;
- El sistema Sophos Central tiene un equilibrio de carga y conmutación por error entre tres sitios, cada uno de los cuales ejecuta dos instancias del software, cualquiera de las cuales es capaz de proporcionar el servicio completo.

G) Control de segregación.

- Sophos mantiene y aplica un proceso de control de calidad para la implantación de nuevos productos de cliente;
- Los entornos de prueba y producción son independientes;
- El nuevo software, los sistemas y los desarrollos se prueban antes de su lanzamiento al entorno de producción.

H) Control organizacional.

- Sophos cuenta con un equipo de seguridad de TI dedicado;
- El equipo de gestión de riesgos y cumplimiento de normativas gestiona los informes y controles de riesgos internos, que incluyen la elaboración de informes sobre los riesgos clave para la gestión;
- Un proceso de respuesta a incidentes identifica y soluciona los riesgos y vulnerabilidades de forma oportuna;

- Cada nuevo empleado lleva a cabo la protección de datos y la formación en seguridad de TI;
- El departamento de seguridad de TI lleva a cabo campañas trimestrales de concienciación sobre la seguridad.

Anexo 3
Productos alojados

- Sophos Central
- Sophos Cloud Optix
- Central Device Encryption
- Central Endpoint Protection
- Central Endpoint Intercept X
- Central Endpoint Intercept X Advanced
- Central Mobile Advanced
- Central Mobile Standard
- Central Phish Threat
- Central Intercept X Advanced for Server
- Central Server Protection
- Central Mobile Security
- Central Web Gateway Advanced
- Central Web Gateway Standard
- Central Email Standard
- Central Email Advanced
- Central Wireless Standard
- Cualquier otro producto de Sophos que se administre y opere a través de Sophos Central

Anexo 4

Datos de referencia para LAS CLÁUSULAS CONTRACTUALES ESTÁNDAR de la UE

APÉNDICE 1 DE LAS CLÁUSULAS CONTRACTUALES ESTÁNDAR DE LA UE

A: LISTA DE PARTES

Exportador(s) de datos: [*Identidad y datos de contacto del exportador o exportadores de datos, incluida cualquier persona de contacto responsable de la protección de datos]*

Nombre del cliente: tal como se proporciona al proveedor bajo el Acuerdo principal

Dirección: Como se proporciona al proveedor en el correo electrónico de contacto de Acuerdo principal:

Nombre/puesto de la persona de contacto: Tal como se proporciona al Proveedor en virtud del Acuerdo principal

Actividades relacionadas con los datos transferidos en virtud de estas cláusulas: Como se describe en la Cláusula 3 supra

Función (controlador/procesador): Controlador

Importador(s) de datos: [*Identidad y datos de contacto del importador o importadores de datos y, en su caso, de su responsable de protección de datos y/o representante en la Unión Europea]*

Nombre: Sophos Limited (para y en nombre de sus filiales de la UE y Suiza)

Dirección: The Pentagon, Abingdon Science Park Abingdon, OX14 3YP, Reino Unido

Número de registro: 2096520

Nombre, cargo y datos de contacto de la persona de contacto: dataprotection@sophos.com

Actividades relacionadas con los datos transferidos en virtud de estas cláusulas: Como se describe en la Cláusula 3 supra.

Función (controlador/procesador): Procesador

B. DESCRIPCIÓN DE LA TRANSFERENCIA

Categorías de sujetos de datos cuyos datos personales se transfieren:

Como se describe en la sección C, prueba 1 anterior

Categorías de datos personales transferidos:

Como se describe en la sección D, prueba 1 anterior.

Transferencia de datos sensibles (si procede) y aplicación de restricciones o salvaguardias que tengan plenamente en cuenta la naturaleza de los datos y los riesgos implicados, como, por ejemplo, la limitación estricta del propósito, las restricciones de acceso (incluido el acceso sólo para el personal que haya seguido una formación especializada), manteniendo un registro del acceso a los datos, restricciones para transferencias posteriores o medidas de seguridad adicionales:

Como se describe en la sección E, prueba 1 anterior.

La frecuencia de la transferencia (por ejemplo, si los datos se transfieren de forma continua o en una sola vez).

Continuo

Naturaleza de la transformación

Como se describe en la sección A, prueba 1 anterior.

Finalidad(es) de la transferencia de datos y su posterior procesamiento

Como se describe en la sección A, prueba 1 anterior.

El período durante el cual se conservarán los datos personales o, si no es posible, los criterios utilizados para determinar dicho período

Por la duración del período de contratación.

Para las transferencias a (sub-) procesadores, especifique también el tema, naturaleza y duración del procesamiento

Como se describe en la Cláusula 3 supra.

AUTORIDAD SUPERVISORA COMPETENTE

VÉASE LA CLÁUSULA 9.8 SUPRA

ANEXO II – MEDIDAS TÉCNICAS Y ORGANIZATIVAS, INCLUIDAS LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA ASETERSE LA SEGURIDAD DE LOS DATOS[1]

Las medidas se exponen en la prueba 2 supra.

ANEXO III – LISTA DE SUBPROCESADORES[2]

No se requiere como cláusula 9(a), no se ha seleccionado la opción 1.

[1] El anexo II deberá cumplimentarse para todos los módulos excepto PARA EL MÓDULO CUATRO.
[2] El anexo III se aplica únicamente al MÓDULO DOS (controlador de transferencia al procesador) y AL MÓDULO TRES (procesador de transferencia al procesador), donde se ha seleccionado la cláusula 9(a), opción 1).