Anexo de seguridad de Cloud Software Group Services

Versión 3.0

Vigente desde el 30 de septiembre de 2022

Contenido

Este Anexo de seguridad de servicios (el “Anexo”) de Cloud Software Group, Inc. (“Cloud Software Group”, “Nosotros”, “Nos” o “Nuestro”) describe los controles de seguridad implementados en relación con el rendimiento de los Cloud Services, los servicios de soporte técnico o los servicios de consultoría (los “Servicios”) prestados a los clientes (“Cliente”, “Usted” o “Su”) bajo la licencia pertinente de Cloud Services Group o el contrato de servicios y el pedido correspondiente de los Servicios (en conjunto, el “Contrato”). Los servicios de versión preliminar Beta o lab/tech (incluidos Cloud Labs) y Nuestros sistemas de TI internos que no participan en la prestación de Servicios se encuentran fuera del ámbito del presente Anexo.

Los términos en mayúscula inicial tienen una descripción de su significado en el Contrato o se definen en el presente documento. “Contenido del cliente” hace referencia a los datos a los que accedemos o recibimos o que Usted envía o carga para su almacenamiento o procesamiento a fin de que llevemos a cabo los Servicios. También incluye información técnica propietaria asociada con Su entorno, como las configuraciones de sistema o red y los controles que seleccione. “Registros” hace referencia a la información relacionada con el rendimiento, la estabilidad, el uso, la seguridad, el soporte, el hardware, el software, los servicios o los periféricos asociados al uso de Nuestros productos o Servicios.

1. Ámbito

Este Anexo describe los controles de seguridad administrativos, físicos y técnicos que empleamos para mantener la confidencialidad, la integridad y la disponibilidad de Nuestros Servicios. Estos controles se aplican a Nuestros sistemas y entornos operativos y de Servicios. Cloud Software Group emplea ISO/IEC 27002 como línea base para su programa de seguridad de los Servicios y ha obtenido certificaciones y evaluaciones del sector para Servicios específicos. Encontrará información adicional en la sección “Privacidad y conformidad” de Nuestro Centro de confianza.

Tenemos la intención de fortalecer y mejorar continuamente sus prácticas de seguridad, de modo que nos reservamos el derecho de modificar los controles que se describen en el presente documento. Las modificaciones no reducirán el nivel de seguridad durante el período relevante de los Servicios.

2. Programa de seguridad y marco de directivas

Cloud Software Group tiene un programa de seguridad y un marco de directivas establecido y aprobado por directores sénior y ejecutivos de que representan diversas áreas empresariales de toda la compañía.

2.1 Supervisión de riesgos de seguridad

El Comité de supervisión de riesgos de ciberseguridad (Cyber Risk Oversight Committee, CROC) rige las actividades de administración de riesgos de seguridad. El CROC consta de un equipo de administración y dirección que abarca todo el espectro de funciones. El equipo de dirección ejecutiva revisa a los miembros del comité todos los años para confirmar que se tratan adecuadamente todas las áreas empresariales y operativas.

El CROC se reúne al menos trimestralmente y proporciona instrucciones, información e indicaciones para identificar, evaluar y solucionar los riesgos de seguridad en las operaciones corporativas y en la infraestructura de prestación de servicios.

2.2 Administración de riesgos de seguridad

Cloud Software Group utiliza un programa de administración de riesgos de seguridad (Security Risk Management, SRM) que identifica las amenazas potenciales para Nuestros productos y servicios y para Nuestra infraestructura, clasifica la importancia de los riesgos asociados a esas amenazas, desarrolla estrategias de mitigación de riesgos y se asocia con Nuestros equipos de Productos e Ingeniería para implementar esas estrategias.

2.3 Seguridad de la información

Cloud Software Group ha designado un Director jefe de seguridad de la información (Chief Information Security Officer, CISO), que es responsable de la supervisión de la seguridad y las estrategias, la conformidad y la aplicación de las directivas. El Director de supervisión y respuesta de la seguridad dirige el proceso de respuesta de incidentes, incluidas la investigación, la contención y la reparación de los incidentes.

2.4 Seguridad física y medioambiental

El equipo de Seguridad de Cloud Software Group supervisa el acceso físico a Nuestras instalaciones.

3. Control de acceso

Requerimos el uso de medidas de control de acceso diseñadas para garantizar que se asignan y mantienen los privilegios adecuados para el acceso a los sistemas, los activos, los datos y las instalaciones de las empresas para protegerlas ante posibles daños, situaciones comprometidas o pérdidas. Seguimos el principio de mínimos privilegios, o seguridad basada en roles, que limita el acceso del usuario solo a lo necesario para realizar sus funciones o roles profesionales.

Los administradores diseñan roles que proporcionan la segregación adecuada de los deberes, distribuyendo tareas y privilegios entre varias personas para protegerse ante el fraude y los errores.

3.1 Nuevas solicitudes de cuentas, roles y acceso

Cloud Software Group requiere una solicitud formal para el acceso a los sistemas o los datos de la empresa. Cada solicitud de acceso requiere una aprobación mínima del administrador del usuario para confirmar el rol y el acceso del usuario. Los administradores de acceso confirman que se hayan obtenido las aprobaciones necesarias antes de conceder acceso a los sistemas o los datos. Se aplica el principio de mínimos privilegios.

3.2 Revisión de cuentas

Llevamos a cabo revisiones semestrales, como mínimo, de las cuentas de usuario y los permisos asignados de los sistemas clave. Los cambios requeridos como resultado de las revisiones están sujetos a un proceso de solicitud de acceso formal para confirmar que el usuario y el rol del usuario requieren acceso a los sistemas relevantes.

3.3 Eliminación de cuentas, roles y acceso

Requerimos que el acceso del usuario se inhabilite, se revoque o se elimine al poco tiempo de recibirse la notificación de cambio de rol de un usuario (si fuera necesario), el cese, la conclusión del compromiso o la salida de la empresa.

Se documentarán las solicitudes de eliminación del acceso y se llevará un seguimiento.

3.4 Credenciales

Cloud Software Group requiere la autenticación multifactor para el acceso remoto a Nuestros sistemas por parte de los empleados, y aplica las siguientes prácticas de gestión y administración de contraseñas:

- Las contraseñas rotan con regularidad, tal como especifican los requisitos del sistema que hemos establecido.

- Las contraseñas deben cumplir unos requisitos de longitud y complejidad, incluida una combinación de dígitos, caracteres especiales y letras en mayúsculas y minúsculas, un número mínimo de caracteres y la prohibición de usar palabras comunes o del diccionario.
- No se conceden ID de usuario desactivados o caducados a otras personas.
- Mantenemos procedimientos para desactivar las contraseñas que se han revelado inadvertidamente.
- Supervisamos los intentos repetidos de obtener acceso a los Servicios con una contraseña no válida y ejecuta acciones automatizadas para bloquear los intentos repetidos.

Cloud Software Group usa prácticas diseñadas para mantener la confidencialidad y la integridad de las contraseñas cuando se asignan, se distribuyen y se almacenan, como:

- Requerir que las contraseñas mantengan un algoritmo hash o estén cifradas durante todo su ciclo de vida.
- Prohibir que se compartan las contraseñas.

4. Desarrollo y mantenimiento de sistemas

Mantenemos un proceso de diseño pensando en la seguridad, que incluye estándares y procedimientos de controles de cambios creados para abordar los requisitos de seguridad de los sistemas de información, revisión y pruebas del código, y seguridad en el uso de los datos de prueba. El proceso está administrado y supervisado por un equipo de seguridad especializado que también es responsable de las revisiones de los diseños, el modelado de las amenazas, las revisiones y comprobaciones manuales del código, y las pruebas de penetración.

4.1 Principios del diseño seguro

Cloud Software Group ha adoptado una metodología formal del ciclo de vida del desarrollo de sistemas (Systems Development Life Cycle, SDLC) que rige el desarrollo, la adquisición, la implementación y el mantenimiento de sistemas de información computarizados y requisitos de tecnología relacionada.

Utilizamos un sistema basado en software para administrar las revisiones y aprobaciones de código abierto, que incluye la ejecución de exámenes y auditorías periódicos de sus productos de software. Tenemos directivas documentadas disponibles para todos los empleados sobre el uso del código abierto, así como formación para los desarrolladores y su administración en las prácticas recomendadas del código abierto.

4.2 Administración de cambios

Nuestro proceso de administración de cambios de la infraestructura y el software aborda los requisitos de seguridad y requiere que los cambios de software e infraestructura se autoricen, se documenten formalmente, se prueben (tal como sea necesario), se revisen y se aprueben antes de su implementación en el entorno de producción. Los cambios de infraestructura y software se administran y se siguen mediante sistemas de administración.

El proceso de administración de cambios se segrega adecuadamente y el acceso para migrar los cambios a producción queda restringido al personal autorizado. 5.

5. Administración de activos

5.1 Administración de activos físicos y virtuales

Cloud Software Group mantiene un inventario dinámico de los sistemas físicos y virtuales que administramos y utilizamos para llevar a cabo los Servicios ("Activos de servicio"). Los propietarios de sistemas son responsables de mantener y actualizar los Activos de servicio de un modo coherente con Nuestros estándares de seguridad.

Se han puesto en práctica unos procedimientos de eliminación formales para realizar la eliminación segura de los datos de Cloud Software Group y de los Clientes. Eliminamos los datos cuando ya no son necesarios según una clasificación mediante procesos de eliminación diseñados para impedir su reconstrucción o su lectura.

Nuestros activos de tecnología se sanean y se eliminan cuando ya no son necesarios en su área designada o asignada. Los activos de tecnología incluyen, sin limitación, dispositivos informáticos individuales, dispositivos informáticos multifunción, dispositivos de almacenamiento, dispositivos de imágenes y dispositivos de redes. La eliminación se coordina mediante Servicios de riesgo de seguridad globales y Seguridad de la información.

5.2 Administración de aplicaciones y sistemas

Los propietarios de aplicaciones y sistemas son responsables de revisar y clasificar los datos a los que acceden y almacenan, transmiten o eliminan. Entre otros controles, los empleados y contratistas deben hacer lo siguiente:

- Clasificar el Contenido del cliente entre las dos principales categorías de información confidencial de Citrix y aplicar las restricciones de acceso adecuadas.
- Restringir la impresión de Contenido del cliente y eliminar los materiales impresos en contenedores seguros.
- No almacenar información confidencial o corporativa en ningún equipo o dispositivo que no cumpla los requisitos de las directivas y estándares de seguridad de Citrix.
- Proteger los equipos informáticos y los datos mientras están desatendidos.

5.3 Retención de datos

El Cliente puede acceder al Contenido del cliente almacenado como parte de Nuestros Cloud Services durante un período de tiempo limitado tras la finalización de los Servicios. Este contenido (exceptuando las copias de seguridad) se eliminará después de que se haya enviado la confirmación al Cliente indicando que se llevará a cabo la eliminación. En la documentación específica de los servicios se incluye información adicional. El Contenido del cliente también se puede retener tras la finalización de los servicios si así se requiriese por motivos legales. Citrix cumplirá los requisitos de este Anexo hasta que dicho Contenido del cliente se haya eliminado permanentemente. 6.

6. Seguridad de recursos humanos

El mantenimiento de la seguridad del Contenido del cliente es uno de los requisitos básicos de todos los empleados y contratistas. Nuestro Código de conducta empresarial requiere que todos los empleados y contratistas cumplan Nuestras directivas y estándares de seguridad, y aborda específicamente la protección de la información confidencial, además de la información personal de los Clientes, socios, proveedores y empleados.

Todos los empleados y contratistas están sujetos a contratos de

confidencialidad que cubren la información del Cliente. La organización de Cloud Software Group también informa con regularidad a los empleados acerca de temas relacionados con la seguridad física y de la información para mantener una conciencia de seguridad sobre temas específicos.

6.1 Verificación de antecedentes

Actualmente, usamos proveedores de verificación de antecedentes para todas las nuevas contrataciones en todo el mundo y requerimos que también se use con el personal de los proveedores externos, excepto cuando esta práctica esté limitada por la legislación o las normativas sobre empleo locales.

6.2 Formación

Todos los empleados deberán recibir formación sobre protección de datos y sobre las directivas de la empresa diseñadas para proteger la seguridad de Nuestra Información confidencial, que incluye la Información confidencial de nuestros Clientes, socios, proveedores y empleados. La formación incluye las prácticas y los principios de privacidad que se aplican a la gestión por parte de los empleados de la información personal, como la necesidad de poner limitaciones en el uso, el acceso, el uso compartido y la conservación de información personal. Los miembros de la organización de ingeniería reciben una formación específica que consta del desarrollo, la arquitectura y la codificación seguros.

6.3 Aplicación

Todos los empleados deberán cumplir con Nuestras directivas y estándares de seguridad y privacidad. El incumplimiento estará sujeto a acciones disciplinarias, que podrían incluir la terminación del empleo. 7.

7. Seguridad de operaciones

7.1 Seguridad de redes y sistemas

Cloud Software Group tiene estándares documentados de fortalecimiento de redes y sistemas que garantizan que las redes y los sistemas se configuren con seguridad. Los procedimientos requeridos con estos estándares incluyen, entre otros:

- Cambiar o inhabilitar la configuración predeterminada y las cuentas
- Uso controlado del acceso administrativo
- Limitar las cuentas de servicio a solo la finalidad con la que se crearon
- Configurar los registros y las alertas adecuados para la auditoría

Requerimos la implementación de software antimalware en servidores y estaciones de trabajo, y examinamos la red en busca de software malintencionado.

Los controles de redes rigen el acceso al Contenido del cliente. Aquí se incluye, cuando corresponda: configurar una zona intermedia no de confianza entre Internet y la red interna que incluya un mecanismo de seguridad para restringir el acceso y el tráfico no autorizado; la segmentación de la red para impedir el acceso no autorizado del Contenido del cliente; y separar servidores de aplicaciones y de web de los servidores de bases de datos correspondientes en una estructura a base de niveles que restrinja el tráfico entre los niveles.

7.2 Registros

Recopilamos Registros para confirmar el correcto funcionamiento de nuestros

Servicios, para ayudar con la resolución de problemas de los sistemas y para proteger y asegurar nuestras redes y el Contenido del cliente. Los Registros pueden incluir el ID de acceso, la hora, la autorización concedida o denegada, datos diagnósticos como los archivos de bloqueos y rastreos, y otra información y actividades relevantes.

Recopilamos y utilizamos los Registros (i) para proporcionar, asegurar, administrar, medir y mejorar los Servicios, (ii) tal como lo solicite el Cliente o sus usuarios finales, (iii) para la facturación, la administración de cuentas, la creación de informes internos y la estrategia de productos, y/o (iv) para el cumplimiento de los acuerdos, las directivas, la legislación correspondiente o solicitudes gubernamentales. Aquí se podría incluir la supervisión del rendimiento, la estabilidad, el uso y la seguridad de los Servicios y los componentes relacionados. Los Registros pueden incluir el ID de acceso, la hora, la autorización concedida o denegada, datos diagnósticos como los archivos de bloqueos y rastreos, y otra información y actividades relevantes. Los clientes no pueden bloquear ni interferir con esta supervisión.

Para obtener más información sobre el Contenido del cliente y la gestión de Registros, consulte Nuestro Centro de confianza Cloud Assurance Data Protection & Security section, que contiene varias notas de producto sobre los registros de Citrix Cloud Services.

7.3 Administración de certificados, credenciales y secretos

Cloud Software Group mantiene directivas que cubren el ciclo de vida de certificados, credenciales y secretos para garantizar la protección, la disponibilidad y la confidencialidad. Es necesario documentar los custodios de los secretos y aceptar formalmente que aceptan las responsabilidades como personal de administración de secretos.

Las responsabilidades incluyen, entre otras:

- Los certificados deben ser emitidos por una autoridad de certificación aprobada.
- Las claves criptográficas no pueden almacenarse ni transmitirse como texto sin formato y deben utilizar protocolos criptográficos seguros y aprobados.
- Las credenciales y los secretos deben rotarse al menos una vez al año y almacenarse en una herramienta aprobada de administración de autenticación con privilegios.

7.4 Administración de vulnerabilidades

Supervisamos las aplicaciones y los sistemas en busca de vulnerabilidades con exploraciones automatizadas de vulnerabilidades y puertos de forma periódica.

Las vulnerabilidades identificadas deben corregirse en un plazo que depende de la valoración de la gravedad y las recomendaciones de los proveedores. En los casos donde no haya disponible una revisión, actualización o mitigación permanente, se utilizarán las contramedidas adecuadas para reducir el riesgo de explotación de la vulnerabilidad.

8. Cifrado

8.1 Protección de datos en tránsito

Cloud Software Group ha implementado protocolos de transmisión segura para la transmisión de la información en redes públicas que forman parte de los Servicios. Los Servicios están protegidos por cifrado y el acceso a través de Internet está protegido por conexiones TLS.

8.2 Protección de datos en reposo

Requerimos que todas las estaciones de trabajo utilizadas para proporcionar Servicios estén cifradas como mínimo con un cifrado de disco completo de 128 bits. El Contenido del cliente no puede almacenarse en ningún dispositivo portátil a menos que esté cifrado.

Algunos Cloud Services cifran ciertos elementos de datos de forma predeterminada y pueden proporcionar otras funciones de cifrado para que los clientes las implementen. Consulte la documentación de Cloud Services aplicable para obtener información adicional.

9. Seguridad física

9.1 Instalaciones

Mantenemos los siguientes controles diseñados para impedir el acceso no autorizado a cualquier instalación:

- El acceso a las instalaciones está limitado a personas autorizadas.
- Los visitantes deberán registrarse en un registro digital de visitantes y estarán acompañados o vigilados en todo momento.
- Los empleados, los contratistas y los invitados deberán llevar distintivos de identificación que estarán visibles en todo momento mientras estén en las instalaciones.
- El personal de Seguridad gestiona y controla el acceso fuera del horario de trabajo en las instalaciones.
- Deberá haber guardias de seguridad, sistemas de detección de intrusos o cámaras CCTV que supervisen los puntos de entrada de los edificios, los muelles de carga y de envíos, y las áreas de acceso público (los mecanismos para supervisar el acceso pueden variar de unas instalaciones a otras, en función de cada una de las instalaciones y sus ubicaciones).

Además, las instalaciones de Cloud Software Group proporcionan:

- Sistemas o dispositivos de extinción de incendios y detección de incendios
- Sistemas o dispositivos de control del clima (temperatura, humedad, etc.)
- Válvulas maestras accesibles de cierre o aislamiento del agua
- Salidas de emergencia y rutas de evacuación

Los armarios de datos de las oficinas están protegidos mediante acceso con distintivo.

9.2 Centros de datos

Además de los controles de las instalaciones descritos arriba, en las instalaciones que posee y administra Cloud Software Group, implementamos controles adicionales en los centros de datos que utilizamos para proporcionar los Servicios.

Usamos sistemas diseñados para proteger contra la pérdida de datos debida a fallos del suministro eléctrico o interferencias en la línea, incluida una infraestructura de servicios globales y redundantes configurada con sitios de recuperación ante desastres. Los centros de datos y los proveedores de servicios de Internet (ISP) se evalúan para optimizar el rendimiento en relación con el ancho de banda, la latencia y el aislamiento en la recuperación ante desastres.

Los centros de datos están situados en instalaciones independientes de los ISP y proporcionan seguridad física, fuentes de energía redundantes, redundancia de infraestructuras y acuerdos de tiempo de actividad de los

proveedores clave.

Cuando usamos centros de datos externos o servicios de nube para la prestación de los Servicios, contratamos a proveedores que cumplen o superan los requisitos de seguridad físicos y medioambientales de Nuestras instalaciones.

10. Continuidad empresarial y recuperación ante desastres

10.1 Continuidad empresarial

Cloud Software Group planifica estratégicamente la continuación de las operaciones empresariales durante situaciones adversas o problemáticas, y diseña sistemas para mantener los servicios operativos mientras ocurran dichos eventos.

Llevamos a cabo un análisis de las repercusiones empresariales (Business Impact Analysis, BIA) a nivel de departamentos al menos cada dos años, con una revisión anual cada año. El BIA se usa para crear un Plan de continuidad empresarial (Business Continuity Plan,BCP), que identifica y documenta para cada departamento sus requisitos de recursos, parámetros y métodos de recuperación, necesidades de reubicación y mecanismos de seguridad requeridos en todo el proceso para evitar errores o divergencias. Los directores sénior de cada departamento revisan y aprueban el BCP cada año, o cuando se producen cambios organizativos considerables.

Tenemos planes de emergencia y contingencia para todas Nuestras instalaciones. En el caso de que no haya instalaciones disponibles, los empleados tienen la opción de trabajar de forma remota en otras instalaciones de Cloud Software Group o en la ubicación que elijan. En los BCP se documentan estrategias de recuperación adicional cuando corresponda.

10.2 Recuperación ante desastres

Nos esforzamos en minimizar el impacto que puedan tener las interrupciones del servicio u operativas mediante la implementación de procesos y controles diseñados para garantizar la recuperación y restauración estable y ordenada de Nuestros datos y sistemas empresariales. Cloud Software Group implementa redundancia en todos los sistemas, datos e infraestructuras fundamentales para sus misiones. El Plan de recuperación ante desastres (Disaster Recovery Plan, DRP) usa la evaluación realizada en el BIA mencionado arriba para identificar y documentar los parámetros de tiempo de recuperación, los métodos, las prioridades y los mecanismos de seguridad requeridos en todo el proceso para evitar errores o divergencias.

El plan esboza la estructura general y el enfoque para restaurar sistemas y datos críticos, incluidos, entre otros:

- Roles y responsabilidades de personas o equipos
- Información de contacto del personal esencial o terceros
- Planes y requisitos de formación para el personal esencial
- Objetivos de recuperación, prioridades de restauración y métricas de éxito
- Esquema de recuperación y restauración completa

Los directores sénior revisan y aprueban el DRP cada año, o cuando se producen cambios organizativos considerables. 11.

11. Respuesta ante los incidentes

Cloud Software Group mantiene un Plan de respuesta ante los incidentes de ciberseguridad que detalla los procesos para detectar, notificar, identificar, analizar y responder a Incidentes de seguridad que afecten a Nuestras redes y sistemas administrados o al Contenido del cliente. La formación sobre la respuesta ante los incidentes de seguridad y las pruebas se llevan a cabo al menos una vez al año.

Por “Incidente de seguridad” se entiende el acceso no autorizado al Contenido del cliente que resulta en la pérdida de confidencialidad, integridad o disponibilidad. Si determinamos que el Contenido del cliente bajo Nuestro control ha estado sujeto a un Incidente de seguridad, Usted recibirá una notificación en el período de tiempo que exija la legislación. Nuestro aviso describirá, cuando se sepa, la naturaleza del incidente, el período de tiempo y el impacto potencial para Usted.

Mantenemos un registro de cada Incidente de seguridad.

12. Administración de proveedores

Cloud Software Group podría usar subcontratistas y agentes para llevar a cabo los Servicios. Los subcontratistas y agentes tendrán derecho a acceder al Contenido del cliente solo cuando sea necesario para realizar los Servicios y estarán sujetos por contratos por escrito que requieren que proporcionen al menos el nivel de protección de datos que se requiere de Nosotros en este Anexo, cuando corresponda. Seremos responsable en todo momento del cumplimiento por parte de sus subcontratistas y agentes de los términos del Contrato, cuando corresponda. Encontrará una lista de los subprocesadores de Cloud Software Group que tienen acceso al Contenido del cliente en Nuestro Centro de confianza.

12.1 Incorporación

Nuestro Programa de administración de riesgos de terceros proporciona un enfoque sistemático a la administración de riesgos de seguridad que supone el uso de proveedores externos. Trabajamos para identificar, analizar y mitigar los riesgos de seguridad antes de participar en la contratación de dichos terceros.

Cloud Software Group firma contratos con los proveedores para documentar las medidas y obligaciones de seguridad relevantes coherentes con las que se especifican en el presente Anexo.

12.2 Evaluación continua

Llevamos a cabo evaluaciones de seguridad periódicas diseñadas para garantizar que las medidas de seguridad se mantienen durante toda la relación con el proveedor. Los cambios en los servicios proporcionados o los cambios en contratos existentes requieren una evaluación de los riesgos de seguridad para confirmar que los cambios no presentan un riesgo adicional o indebido.

12.3 Cancelación de los servicios

Nos esforzamos por notificar a la organización de contratación de la empresa con al menos 90 días de antelación antes de finalizar la relación con un proveedor o antes de que caduque el contrato con un proveedor (a menos que sea necesaria una rescisión más rápida). La organización de contratación de la empresa coordina la terminación de las relaciones existentes para confirmar que Nuestros datos y activos corporativos estén seguros y gestionados adecuadamente.

13. Cumplimiento

13.1 Tratamiento de datos personales

Los datos personales son información relacionada con una persona identificada o identificable. Usted determina los datos personales que incluye en el Contenido de cliente. Al ejecutar los Servicios, Nosotros actuamos como procesador de datos y Usted continúa siendo la persona con el control de los datos personales en el Contenido del cliente. Actuaremos bajo Sus instrucciones en relación con el procesamiento de dichos datos personales, tal como se especifique en el Contrato.

En el Apéndice de procesamiento de datos de Cloud Software Group se proporciona información adicional en relación con el tratamiento de los datos personales sujetos al Reglamento General de Protección de Datos, incluidos los mecanismos empleados para la transferencia internacional de dichos datos.

13.2 Ubicación de los servicios

Los Clientes de Cloud Services mantienen el control sobre la elección de la ubicación geográfica de su entorno de Cloud Services. En ningún momento durante la suscripción de los Cloud Services correspondientes podremos cambiar la ubicación geográfica del entorno elegida por Usted sin su consentimiento. Tenga en cuenta que ciertas ubicaciones geográficas pueden no estar disponibles en algunos Cloud Services, y como parte de la prestación general del Servicio, el Contenido del cliente se puede transferir a Estados Unidos u otros países en los que operen Citrix y sus proveedores de servicios, cuando sea necesario para proporcionar los Servicios.

13.3 Revelación del Contenido del cliente

Podríamos revelar el Contenido del cliente cuando lo requiera la ley, como en el caso de la respuesta a una citación, una orden judicial o administrativa, u otro instrumento vinculante (cada uno de ellos, una “Demanda”). Excepto cuando lo prohíba la ley, le notificaremos lo antes posible a Usted en el caso de una Demanda y le proporcionaremos una asistencia razonablemente necesaria para que Usted responda a la Demanda de forma oportuna.

13.4 Requisitos de seguridad y reglamentarios del Cliente

Los Servicios están diseñados para prestarse en un entorno de TI de Cliente más grande, de modo que los Clientes mantienen la responsabilidad total de todos los aspectos de seguridad no gestionados expresamente por Citrix, incluidos, sin limitación, la integración técnica con los Servicios, controles y administración de acceso de usuarios, y todas las aplicaciones y redes que los Clientes pueden usar junto con los Servicios.

Usted es responsable de determinar si el uso que hace de los Servicios, incluido el acceso concedido a Nosotros a cualquier Contenido del cliente como parte de los Servicios, está sujeto a requisitos de seguridad y reglamentarios más allá de los especificados en el Contrato, incluido este Anexo. Por tanto, los Clientes deben garantizar que no envían ni almacenan Contenido del cliente que esté regido por leyes que imponen controles específicos no incluidos en este Anexo. Aquí se podrían incluir los reglamentos de tráfico de armas internacionales (International Traffic in Arms Regulations, ITAR) de EE. UU. o normativas similares de cualquier país que restrinjan la importación o la exportación de artículos o servicios de defensa, información sanitaria protegida (Protected Health Information, PHI), información de tarjetas de pago (Payment Card Information, PCI), o datos de distribución controlada bajo normativas

gubernamentales, a menos que se especifique en el Contrato con la Descripción del Servicio correspondiente, y las partes hayan firmado contratos adicionales (como un contrato de asociado empresarial HIPAA) por adelantado, si lo requerimos para procesar dichos datos.

14. Auditorías e investigaciones del Cliente

Cloud Software Group responderá, como máximo una vez al año, a solicitudes de auditoría en forma de respuestas a las evaluaciones de riesgos del Cliente. Los Clientes también pueden acceder a Nuestro Paquete de diligencia debida en cualquier momento para obtener un paquete y cuestionario de seguridad actualizado. Nuestro Paquete de diligencia debida se creó para las consultas de seguridad de los clientes y proporciona información sobre seguridad de fácil acceso, incluido un breve cuestionario de recopilación de información estandarizada (Standardized Information Gathering, SIG) para Nuestros servicios de nube. El Paquete de diligencia debida se puede descargar en Nuestro Centro de confianza en Sección Protección y seguridad de datos de garantías de nube.

15. Contactos

Función	Contacto
Asistencia al cliente	https://www.citrix.com/contact/technical-support.html
Notificar un Incidente de seguridad	secure@citrix.com
Sospecha de vulnerabilidades en Nuestros Servicios	https://www.citrix.com/about/trust-center/ (Haga clic en el botón "Informar de un problema de seguridad".

Ventas de empresa
Norteamérica | 800-424-8749
Otros países | +1 408-790-8000

Ubicaciones
Sede central corporativa | 851 Cypress Creek Road Fort Lauderdale, FL 33309, Estados Unidos
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, Estados Unidos