*Última revisión: 1 de marzo de 2018*

# Anexo de seguridad de servicios de Citrix

Este Anexo de seguridad de servicios de Citrix (el Anexo) describe los controles de seguridad técnicos y organizativos empleados en relación con los servicios de Citrix Cloud, los servicios de asistencia técnica o los servicios de consultoría con un contrato de servicios, una suscripción o una licencia de Citrix. Este Anexo está incorporado como referencia en dichos contratos de servicios (los "Contratos"). Este Anexo no se aplica a los servicios Beta, Technology Preview o Labs, incluido Citrix Cloud Labs.
Los términos con inicial en mayúscula tienen el significado especificado en el Contrato o definido en el presente documento, incluido el Artículo 7, Definiciones, más abajo.

## Artículo 1. Controles de seguridad de Citrix

Este Artículo describe los controles físicos, lógicos y administrativos que Citrix emplea para proteger los Servicios y las obligaciones de seguridad asociadas del Cliente. Citrix cumple con el estándar ISO/IEC 27002 como base de referencia para el programa de seguridad de los Servicios.

Los controles especificados en el Artículo 1.A se aplican a todos los Servicios. Los controles adicionales especificados en la Sección 1.B se aplican a todos los servicios de Citrix Cloud disponibles generalmente (en conjunto, "Cloud Services").

Citrix se reserva el derecho de modificar los controles especificados en el Artículo 1 siempre que los controles empleados durante un período de servicio por el cual el Cliente haya realizado pagos protejan el Contenido del cliente al menos en la misma medida que los especificados en este Artículo 1 en la fecha de entrada en vigor de dicho período.

### 1.A. Controles de seguridad empresarial: todos los servicios

| Área | Controles |
|---|---|
| Administración del programa de seguridad | **Propiedad de seguridad**. Citrix ha designado a uno o varios Security Officers responsables de coordinar y supervisar los controles de seguridad de los Servicios.<br><br>**Roles de seguridad y responsabilidades**. El personal de Citrix con acceso al Contenido del cliente está sujeto a obligaciones de confidencialidad.<br><br>**Directivas de seguridad del servicio.** Citrix mantiene un completo marco de seguridad global (GSF, por sus siglas en inglés), que proporciona los principios globales de seguridad establecidos y aprobados por la administración ejecutiva de Citrix. Las directivas proporcionan |

| Área | Controles |
| --- | --- |
| | requisitos de seguridad de manera clara y concisa. Los estándares definen el proceso o la metodología para cumplir los requisitos de las directivas. El programa de seguridad del GSF está sometido a revisiones y evaluaciones regulares. Citrix mantiene un resumen del programa del GSF que proporcionará a los clientes cuando lo soliciten.<br><br>**Gestión de riesgos de productos.** Citrix realiza evaluaciones de las áreas clave de los riesgos asociados a los Servicios, incluidos (exclusivamente a modo de ejemplo cuando sean aplicables) las evaluaciones del riesgo de privacidad, las revisiones del código abierto y los análisis de control de exportaciones. |
| Administración de activos | **Inventario de activos**. Citrix mantiene un inventario del equipamiento administrado por Citrix que se utiliza para prestar los Servicios ("Activos"). Los propietarios de los sistemas identificados son responsables de mantener y actualizar el inventario cuando sea necesario.<br><br>**Gestión de activos y de datos**<br><br>Citrix identifica y clasifica el Contenido del cliente para garantizar que el acceso se restrinja adecuadamente.<br><br>Citrix impone restricciones en relación con la impresión del Contenido del cliente y la eliminación de materiales impresos que incluyen Contenido del cliente.<br><br>El personal de Citrix debe obtener la autorización pertinente antes de almacenar Contenido del cliente en dispositivos portátiles, acceder remotamente a dicho contenido o tratarlo fuera de las instalaciones administradas por Citrix o por sus proveedores de servicios. |
| Administración de accesos | **Directiva de acceso.** Citrix mantiene un registro de los privilegios de seguridad de las personas que tienen acceso al Contenido del cliente y sigue el principio de privilegio mínimo.<br><br>**Autorización de accesos**<br><br>Citrix mantiene y actualiza un registro del personal autorizado a acceder a los sistemas de Citrix que alojan Contenido del cliente.<br><br>La administración revisa y aprueba cada nuevo acceso a los sistemas antes de que se conceda.<br><br>Citrix lleva a cabo revisiones regulares de las cuentas de usuario y de los permisos asignados para los sistemas clave.<br><br>Citrix identifica el personal que puede conceder, modificar o cancelar el acceso autorizado a los datos y a las instalaciones.<br><br>En caso de que haya varias personas con acceso a sistemas que alojan Contenido del cliente, Citrix garantiza que estas personas dispondrán de sus propios identificadores e inicios de sesión. |

| Área | Controles |
| --- | --- |
| | **Privilegio mínimo**<br><br>Citrix limita el acceso al Contenido del cliente solo a las personas que requieren dicho acceso para llevar a cabo su función laboral.<br><br>**Integridad y confidencialidad**<br><br>Citrix requiere que los usuarios protejan los equipos y los datos cuando estén desatendidos.<br><br>Citrix requiere que las contraseñas sean ininteligibles durante todo el ciclo de vida.<br><br>**Autenticación**<br><br>Citrix usa prácticas estándar del sector para identificar y autenticar a los usuarios que acceden a los sistemas de información.<br><br>Cuando los mecanismos de autenticación se basan en contraseñas, Citrix sigue las prácticas estándar del sector para la gestión y la administración de contraseñas, que incluyen lo siguiente:<br><br>Las contraseñas se renuevan con regularidad, tal como establecen los requisitos del sistema y los estándares de Citrix.<br><br>Las contraseñas deben cumplir los requisitos de longitud y complejidad, que incluyen una longitud mínima de 8 caracteres.<br><br>El personal tiene prohibido compartir las contraseñas.<br><br>No se puede conceder identificadores desactivados o caducados a otras personas.<br><br>Citrix dispone de procedimientos para desactivar contraseñas dañadas o que se han revelado inadvertidamente.<br><br>Citrix supervisa los intentos repetidos de obtener acceso a los Servicios con una contraseña no válida.<br><br>Citrix implementa prácticas diseñadas para preservar la confidencialidad y la integridad de las contraseñas durante su asignación, distribución y almacenamiento. |
| Prevención de pérdidas | **Software malintencionado**. Citrix usa software antivirus y otros controles para evitar que el software malintencionado obtenga acceso no autorizado al Contenido del cliente, incluido el software malintencionado que procede de redes públicas.<br><br>**Eliminación de multimedia.** Citrix elimina los elementos multimedia cuando ya no son necesarios según su clasificación y mediante procesos seguros de eliminación. |

| Área | Controles |
| --- | --- |
| Seguridad física y del entorno (control de acceso, control de disponibilidad) | **Acceso físico a instalaciones de Citrix**. Citrix limita el acceso a las instalaciones solo a las personas autorizadas. Todos los empleados, los contratistas y los invitados deben llevar insignias de identificación visibles mientras se encuentren en las instalaciones. Citrix supervisa los puntos de entrada a las instalaciones mediante varios métodos, como guardias de seguridad, detección de intrusos y cámaras de televigilancia.<br><br>**Protección contra interrupciones**. Citrix usa sistemas para protegerse frente a la pérdida de datos debida a fallos del suministro eléctrico o interferencias en la línea, incluidos los siguientes: infraestructura de servicios global y redundante configurada con sitios de recuperación ante desastres; evaluación de centros de datos y proveedores de servicios de Internet (ISP) para optimizar el rendimiento en relación con el aislamiento de la recuperación ante desastres, la latencia y el ancho de banda; ubicación de los centros de datos en instalaciones seguras que sean neutrales en cuanto a los proveedores ISP y que proporcionen seguridad física, alimentación redundante y redundancia de la infraestructura; y contratos de tiempo de actividad de los proveedores clave.<br><br>**Centros de datos alojados.** Cuando Citrix usa centros de datos externos para el aprovisionamiento de los Servicios, Citrix requiere que el proveedor de servicios cumpla o supere los requisitos de seguridad físicos y del entorno de las instalaciones administradas por Citrix. Los requisitos mínimos de seguridad incluyen, entre otros:<br>• Restricciones de acceso físico y medidas de protección (autenticación, registros, supervisión, etc.)<br>• Separación adecuada de los entornos<br>• Mecanismos de prevención, detección y extinción de incendios<br>• Sistemas de control del clima (temperatura, humedad, etc.)<br><br>**Informática en la nube.** Cuando Citrix usa XaaS [Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS), Software como servicio (SaaS)] para el aprovisionamiento de los Servicios, Citrix realiza contratos con proveedores de XaaS con un nivel materialmente similar de control de acceso físico a sus centros de datos alojados. |
| Seguridad de aplicaciones y desarrollo | **Desarrollo y mantenimiento de sistemas.** Citrix implementa un proceso Secure by Design (Diseño seguro) que incluye procedimientos de control de cambios y estándares diseñados para abordar los requisitos de seguridad de los sistemas de información, la revisión y las pruebas de códigos, y la seguridad relativa al uso de los datos de prueba. Este proceso está administrado y supervisado por un equipo de ingeniería de seguridad especializado, que también es responsable de la revisión de diseños, el modelado de amenazas, las inspecciones |

| Área | Controles |
| --- | --- |
| | y revisiones manuales de códigos, y los exámenes de penetración.<br><br>**Administración de código abierto**. Citrix usa un sistema basado en software para administrar las revisiones y aprobaciones de código abierto. Además, Citrix lleva a cabo exámenes y auditorías periódicas de sus productos de software para confirmar la conformidad del código abierto.<br><br>**Administración de cambios.** Citrix implementa procedimientos de control de cambios que abordan los requisitos de seguridad de los sistemas de información, las pruebas, la aceptación de las pruebas y la seguridad relativa al uso de los datos de prueba. La administración y el seguimiento de los cambios del software y de la configuración se realizan a través de sistemas de tiquets estándar. |
| Operaciones seguras | **Diseño de red**. Citrix implementa mecanismos diseñados para aplicar estándares y directivas de administración de acceso en todos los Servicios, incluidos los controles de red sobre el acceso al Contenido del cliente. Los mecanismos son los siguientes, según 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; y separar servidores web y de aplicaciones de los servidores de bases de datos correspondientes en una estructura basada en niveles que restrinja el tráfico entre los niveles. |
| Administración de incidentes | **Respuesta ante incidentes**. Citrix mantiene un programa de respuesta ante incidentes diseñado para contener, analizar, remediar y comunicar los incidentes de seguridad que afectan a las redes o los sistemas administrados por Citrix o al Contenido del cliente.<br><br>**Notificación de incidentes**. Si Citrix determina que el Contenido del cliente bajo su control ha sufrido un Incidente de seguridad, se notificará al Cliente en el plazo de tiempo establecido por la legislación aplicable.<br><br>**Registro de incidentes**. Citrix mantiene un registro de los Incidentes de seguridad conocidos con una descripción del incidente, el período de tiempo, las consecuencias del incidente, el nombre del informador, a quién se notificó el incidente y el procedimiento para la recuperación de los datos y los Servicios, cuando corresponda. |
| Administración de proveedores | **Incorporación**. Citrix lleva a cabo evaluaciones de seguridad de los proveedores de servicios que tendrán acceso al Contenido del cliente o a los componentes de los Servicios que tratan el Contenido del cliente.<br><br>Citrix requiere que los proveedores de servicios conectados a los Servicios cumplan con el nivel de seguridad de esta Sección aplicable a los servicios que proporcionan. Los proveedores de servicios que accedan al Contenido del Cliente de acuerdo con la legislación de la Unión Europea deberán certificar que cumplen con los programas Escudo de privacidad de la Unión |

| Área | Controles |
|---|---|
| | Europea - EE. UU. y de la Unión Europea - Suiza, o bien formalizar las Cláusulas contractuales tipo.<br><br>**Mantenimiento continuo.** Se llevará a cabo una evaluación periódica de los proveedores de servicios, en función de la confidencialidad y el riesgo asociados a sus servicios.<br><br>**Cese.** Al finalizar la relación con un proveedor, el proveedor de servicios deberá devolver todo el Contenido del cliente que tenga en su posesión o certificar que todo el Contenido del cliente se ha destruido de modo seguro. |
| Continuidad de negocio y recuperación ante desastres | **Continuidad de negocio.** Citrix mantiene planes de emergencia y de contingencia para las instalaciones en las que se encuentran los sistemas de información de Citrix que tratan el Contenido del cliente.<br><br>**Recuperación ante desastres.** El almacenamiento redundante de Citrix y sus procedimientos para la recuperación de datos están diseñados para intentar reconstruir el Contenido del cliente con su estado original o el de la última replicación. |
| Obligaciones de seguridad del Cliente | El Cliente es responsable de administrar los aspectos de seguridad que no se contemplen expresamente como parte de los Servicios. Esto incluye, entre otras, las siguientes acciones:<br>• Limitar el acceso de Citrix solo a la parte del Contenido del cliente que sea necesaria para que el Cliente reciba los Servicios.<br>• Proteger los componentes de redes y servicios frente a posibles interferencias, lo que incluye supervisar y proteger sus redes y el equipamiento informático.<br>• Descargar el Contenido del cliente cuando sea necesario, tanto durante el período de los Servicios como en su finalización.<br>• Citrix cifra de manera predeterminada los datos en tránsito u ofrece a los clientes medios para cifrar dichos datos. Se proporciona más información en la documentación de los productos de los Servicios. El Cliente es responsable de garantizar que los datos se protejan adecuadamente mientras se transfieren. |

**1.B. Controles de seguridad de los servicios de nube adicionales**

| Área | Controles |
|---|---|
| Protección de la información<br><br>(control de disponibilidad, control de transmisión, | **Procedimientos de conmutación por error**. Citrix implementa mecanismos diseñados para abordar la pérdida de la disponibilidad del Contenido del cliente, incluido el almacenamiento de copias de dicho contenido en una ubicación diferente a aquella en la que se encuentra el |

| Área | Controles |
| --- | --- |
| eliminación de datos) | equipamiento informático principal que trata el Contenido del cliente.<br><br>**Datos más allá de los límites**. Citrix cifra el Contenido del cliente que se transmite por las redes públicas que forman parte de un Servicio (o permite que el Cliente lo cifre).<br><br>**Retención.** Citrix puede retener el Contenido del cliente después del período del Servicio y archivarlo para que el Cliente pueda acceder a él cuando sea obligatorio para fines legales. Citrix cumplirá con los requisitos de este Anexo hasta que el Contenido del cliente se haya eliminado permanentemente. Sujeto a la sección Devolución, que se encuentra a continuación, Citrix no tiene obligación de retener el Contenido del cliente después de la finalización del Servicio.<br><br>**Devolución.** Sujeto a la disponibilidad y a la Descripción aplicable de los Servicios, el Cliente dispone de treinta (30) días para descargar el Contenido del cliente tras la fecha de caducidad.<br><br>**Eliminación de datos**. Citrix eliminará de manera segura el Contenido del cliente cuando ya no sea necesario para finalidades legítimas. |
| Operaciones seguras | **Registro de eventos**. En determinados Servicios, Citrix recopila Registros. Los Registros pueden incluir el id. de acceso, la hora, la autorización concedida o denegada, datos de diagnóstico (como los archivos de seguimiento o de bloqueos) y otra actividad relevante.<br><br>Los Registros se usan (**i**) para proporcionar, proteger, administrar, medir y mejorar los Servicios y los análisis asociados, (**ii**) tal como indiquen o especifiquen el Cliente y sus Usuarios, o (**iii**) para la conformidad con las directivas de Citrix, la legislación vigente, las normas o los requisitos gubernamentales. Esto podría incluir la supervisión del rendimiento, la estabilidad, el uso y la seguridad de los Servicios y los componentes relacionados. El Cliente no debe bloquear este proceso de supervisión ni interferir en él.<br><br>Citrix puede complementar los Registros con la información recopilada de terceros para los fines especificados anteriormente.<br><br>Los Registros se podrían utilizar para fines no especificados en este Anexo solo en forma agregada. |
| Continuidad de negocio y recuperación ante desastres | **Copias de seguridad.** Excepto cuando se especifique de otro modo en la Descripción de los servicios respectiva, los Servicios deberán mantenerse en clústeres de tipo activo-activo y de alta disponibilidad que abarquen varios sitios físicos. En el caso de los sistemas que no se mantengan en una configuración activa-activa, se realizarán copias de seguridad de acuerdo con los objetivos del nivel de servicio específicos del Servicio. |

**Artículo 2.** **Tratamiento de los datos personales**

Los datos personales son la información sobre una persona identificada o que se pueda identificar. El Cliente determina los datos personales que se incluyen en el Contenido del cliente. Al prestar los Servicios, Citrix actúa como encargado del tratamiento de los datos y el Cliente sigue siendo el responsable del tratamiento de todos los datos personales incluidos en el Contenido del cliente. Citrix actuará según las instrucciones del Cliente en relación con el tratamiento de dichos datos personales, tal como se especifica en el Contrato.

En el Anexo I, Términos del Reglamento general de protección de datos, se proporciona más información en relación con el tratamiento de datos personales conforme al Reglamento general de protección de datos, incluidos los mecanismos empleados para la transferencia internacional de dichos datos.

**Artículo 3.** **Ubicación de los Servicios**

El Contenido del cliente se puede transferir, almacenar o tratar en Estados Unidos o en otros países donde operan Citrix y sus proveedores de servicios. Los requisitos de este Anexo siguen siendo de aplicación independientemente de la ubicación donde Citrix almacene o trate el Contenido del cliente.

Las partes pueden negociar de buena fe en relación con cualquier acuerdo de tratamiento de datos o de transferencia de datos adicional que sea necesario para facilitar la transferencia internacional de datos de forma legítima en conexión con el aprovisionamiento de los Servicios por parte de Citrix.

**Artículo 4.** **Divulgación del Contenido del cliente**

El Cliente da su consentimiento a la divulgación del Contenido del cliente por parte de Citrix tal como se establece en esta sección.
Citrix puede recurrir a subcontratistas y agentes para llevar a cabo los Servicios. Todos los subcontratistas y agentes tendrán derecho a acceder al Contenido del cliente solo cuando sea necesario para llevar a cabo los Servicios y quedarán obligados mediante contratos por escrito a proporcionar como mínimo el mismo nivel de protección de datos exigido a Citrix en virtud de este Anexo, según corresponda. Citrix seguirá siendo responsable en todo momento de la conformidad de sus subcontratistas y agentes con los términos del Contrato, cuando corresponda.

Citrix también puede divulgar el Contenido del cliente: (a) a entidades afiliadas, por motivos consistentes con el Contrato; (b) en conexión con cualquier fusión, adquisición, venta, bancarrota o cualquier otro tipo de reorganización anticipada o real de su negocio, total o parcialmente, sujeto a la obligación de proteger el Contenido del cliente de acuerdo con los términos del Contrato; (c) por motivos legales, incluidos la aplicación de sus derechos, la detección y prevención del fraude, la protección frente a daños a los derechos o la propiedad de Citrix, los Clientes, los Usuarios o el público; y (c) tal como lo requiera la legislación, ya sea como respuesta a una citación, una orden judicial o administrativa, o cualquier otro instrumento vinculante (cada uno de ellos, una “Demanda”). Excepto en los casos en los que quede prohibido por ley, Citrix comunicará al Cliente cualquier Demanda lo antes posible y le proporcionará la asistencia razonablemente necesaria para que responda a la Demanda de manera oportuna.

**Artículo 5. Obligaciones del Cliente**

**1. Disposiciones generales**. El Cliente puede usar los Servicios y acceder a ellos estrictamente conforme a lo permitido en el Contrato. El Cliente cumplirá con todas las leyes aplicables en relación con su uso de los Servicios.

**2. Permisos.** El Cliente es responsable de obtener todos los permisos necesarios para que Citrix lleve a cabo los Servicios, lo cual incluye proporcionar avisos y obtener los consentimientos o las licencias necesarias para que Citrix pueda acceder al Contenido del cliente y tratarlo tal como establece este Anexo.

**3. Referencias normativas.** El Cliente es responsable de determinar si el Contenido del cliente está sujeto a requisitos normativos o de seguridad adicionales más allá de los especificados en el Contrato, incluido este Anexo. El Cliente no enviará a los Servicios ni almacenará en ellos ningún Contenido del Cliente regulado por el Reglamento de EE. UU. de tráfico internacional de armas (ITAR) o por regulaciones similares de otros países que restrinjan la importación o exportación de artículos o servicios de defensa. Además, el Cliente no proporcionará ni almacenará ningún Contenido del cliente sujeto a los requisitos normativos adicionales, como la información médica confidencial (PHI, por sus siglas en inglés), la información de tarjetas de pagos (PCI, por sus siglas en inglés) o los datos de distribución controlada bajo normativas gubernamentales, a menos que se especifique en la Orden del Cliente y la Descripción del Servicio y que las partes hayan firmado contratos adicionales (como un Contrato de socio comercial (BAA, por sus siglas en inglés)) por adelantado, tal como requiera Citrix para tratar dichos datos. Los Clientes del servicio ShareFile pueden ponerse en contacto con Citrix en privacy@sharefile.com para solicitar un BAA.

**4. Entorno de seguridad del Cliente.** Los Servicios están diseñados para que se proporcionen solo en un entorno de seguridad del Cliente más grande. El Cliente garantizará las funciones de seguridad adecuadas para todos los componentes que no estén administrados expresamente por Citrix, incluidos, entre otros, los controles de acceso, firewalls, aplicaciones y redes utilizados de forma conjunta con los Servicios. Vea la Sección 1.A., Obligaciones de seguridad del Cliente, más arriba.

**5. Notificación de seguridad**. El Cliente es responsable de comunicar a Citrix lo antes posible los incidentes de seguridad relacionados con los Servicios o el Contenido del cliente, tal como se especifica más adelante en el Artículo VI, Contactos de Citrix.

**6. Conformidad de los Usuarios**. El Cliente es responsable de la conformidad de sus Usuarios con los términos de la Orden y del Contrato.

**Artículo 6. Contactos de Citrix**

| FUNCIÓN | CONTACTO |
|---|---|
| Asistencia al cliente | https://www.citrix.com/contact/technical-support.html |
| Notificar un incidente | secure@citrix.com |
| Sospechas de vulnerabilidades en productos de Citrix | secure@citrix.com |

**Artículo 7. Definiciones**

Los términos con mayúscula inicial en el Anexo tendrán el significado que se especifique en el Contrato o más abajo. En caso de conflicto entre los términos restantes del Contrato y cualquiera de las siguientes definiciones, las definiciones siguientes se aplicarán en este Anexo.

**Contenido del cliente** hace referencia a los datos cargados en la cuenta del Cliente para su almacenamiento o los datos del entorno informático del Cliente a los que Citrix puede acceder para prestar los Servicios.

**Registro** hace referencia a un registro de eventos relacionados con los Servicios, incluidos los registros que miden el rendimiento, la estabilidad, el uso, la seguridad y la asistencia.

**Incidente de seguridad** hace referencia al acceso no autorizado al Contenido del cliente que provoca la pérdida de confidencialidad, integridad o disponibilidad.