AUTODESK

Documento técnico de seguridad de Autodesk® Fusion 360

Octubre de 2022

Contenido

1. Introducción

Autodesk® Fusion 360™ es la primera herramienta CAD, CAM y CAE 3D de su clase. Permite conectar el proceso de desarrollo de productos en una única plataforma basada en la nube compatible con Mac y PC. Las herramientas de Fusion 360 facilitan y agilizan la exploración de ideas de diseño con un conjunto de herramientas seguras e integradas que van del concepto a la fabricación y que se extienden para incluir navegadores web y dispositivos móviles.

1.1 Objetivo y alcance del documento

Este documento tiene por objeto explicar las operaciones de Autodesk, el proceso de desarrollo de software y las medidas de seguridad que se aplican en el entorno. En este documento, Autodesk Fusion 360 hace referencia tanto al software cliente de Fusion 360 como al software de acceso al navegador de Fusion 360.

El marco de seguridad de Autodesk se basa en las normas del sector para proteger la confidencialidad, la integridad y la disponibilidad de la información de los clientes.

Fusion 360 se ha diseñado para ofrecer alta disponibilidad y escalabilidad, lo que proporciona a nuestros clientes un servicio en la nube rápido y flexible. El proveedor de alojamiento en la nube de Autodesk es Amazon Web Services (AWS), líder en infraestructuras en la nube. Autodesk utiliza el modelo de responsabilidad compartida del proveedor de alojamiento de AWS, que incluye una infraestructura compuesta por el hardware, el software, las redes y las instalaciones que ejecutan los servicios en la nube de AWS. (Para obtener más información, consulte: https://aws.amazon.com/es/compliance/shared-responsibility-model/).

2. Seguridad de Autodesk

La estructura de seguridad de Autodesk se basa en las normas del sector para garantizar la coherencia de las prácticas de seguridad, lo que nos permite construir de forma segura, ejecutar de forma segura y mantener la seguridad.

- **Construir de forma segura**: la integración de la seguridad en nuestros productos desde cero es una parte fundamental de la garantía de la inversión de nuestros clientes en

productos y servicios de Autodesk. Integramos la seguridad en todas las fases del desarrollo de software.

- **Ejecutar de forma segura**: incorporamos la seguridad directamente en nuestra infraestructura. Nuestro enfoque integral incluye la implementación de herramientas de protección de puntos finales, requisitos estandarizados de parches y endurecimiento, controles de administración de identidad y acceso y actividades de seguridad ofensivas.
- **Mantener la seguridad**: la seguridad de Autodesk se centra en tres objetivos principales que protegen la confidencialidad, la integridad y la disponibilidad de la información:
    - Confidencialidad: la información solo está disponible para personas autorizadas.
    - Integridad: la información es completa y exacta.
    - Disponibilidad: los datos están disponibles y accesibles para los clientes.

El director de seguridad (CSO) es responsable del desarrollo, la implementación y la gestión de la estrategia y el programa de seguridad y garantiza que las políticas y normas de seguridad se apliquen en todos los productos y entornos de Autodesk. El CSO y el equipo de seguridad tienen el apoyo de los directivos y del Consejo de Administración de Autodesk.

3. Ingeniería de Fusion 360

El equipo de ingeniería de Fusion 360 se encarga de diseñar, implementar y probar el software cliente y la aplicación de servicios en la nube de Fusion 360.

El diseño, la codificación, las pruebas y el mantenimiento de Fusion 360 se basan en un proceso ágil de desarrollo de software. Durante las fases de diseño, se elaboran documentos de diseño detallados que los arquitectos revisan para evaluar la funcionalidad y la escalabilidad del diseño. Durante las fases de implantación, los ingenieros de software y los arquitectos llevan a cabo revisiones de código entre pares para detectar posibles desviaciones de las prácticas de desarrollo de aplicaciones de Fusion 360. Todo el código que se produce durante el proceso incluye pruebas de unidades funcionales, y no se completa ninguna experiencia de usuario hasta que el personal de control de calidad verifica la aceptación y los criterios de definición del estado Listo. Las pruebas de rendimiento de Fusion 360 también se integran en

el ciclo de vida de desarrollo. El equipo de Fusion 360 efectúa pruebas de carga en todas las fases de desarrollo para identificar los cambios que afectan negativamente al rendimiento lo antes posible en el proceso.

3.1 Formación de empleados

Todos los empleados de Autodesk deben afirmar la importancia de la seguridad de la información como parte de la orientación a la contratación de nuevo personal. Los empleados deben leer, comprender y realizar un curso de formación sobre el Código de Conducta de la empresa. El código exige que todos los empleados desarrollen su actividad de forma legal, ética, íntegra y respetuosa entre sí y con los usuarios, socios y competidores de la empresa.

Los empleados de Autodesk deben seguir las directrices de la empresa en materia de confidencialidad, ética empresarial, uso adecuado y normas profesionales. Los nuevos empleados deben firmar un acuerdo de confidencialidad. La orientación de los nuevos empleados hace hincapié en la confidencialidad y privacidad de los datos de los clientes.

Para implementar las prácticas recomendadas de seguridad, Autodesk ha introducido un Programa anual de certificación de seguridad de software (SSCP) para todos los usuarios de las funciones de ingeniería e infraestructura en la nube.

4. Seguridad de productos de Fusion 360

Autodesk Fusion 360 tiene funciones de seguridad integradas que abarcan desde la comunicación con los servicios en la nube hasta las funciones de colaboración y seguridad de nivel de producto que pueden controlar los usuarios.

4.1 Seguridad de las comunicaciones

Toda comunicación entre Autodesk Fusion 360 y los servicios en la nube requiere conexiones HTTPS seguras.

4.2 Cifrado

La comunicación entre Fusion 360 y los servicios backend y dentro de los servicios backend se produce a través de un canal cifrado.

4.3 Autenticación

Se requieren credenciales formadas por un ID de Autodesk, un ID de usuario y una contraseña para acceder a Autodesk Fusion 360. Las credenciales se aseguran durante la transmisión de red y se almacenan solo como hash salado.

Fusion 360 ofrece a los usuarios finales la opción de utilizar la autenticación multifactor al iniciar sesión. Los usuarios que opten por activar esta función pueden utilizar su dispositivo personal seguro autorizado (por ejemplo, el teléfono móvil) para recibir un código que se utilizará junto con su contraseña.

4.4 Seguridad de datos

Todos los diseños de Fusion 360 se guardan en la nube en un almacenamiento cifrado. La solución de almacenamiento utiliza el Estándar de cifrado avanzado de 256 bits (AES-256) para cifrar los datos.

En el ámbito local, los diseños almacenados en caché se basan en los permisos de nivel de usuario del sistema operativo para el control de acceso.

4.5 Versiones de diseño

Para cada diseño, Autodesk Fusion 360 mantiene un historial de versiones. El control de versiones protege la integridad de los datos, ya que permite a los usuarios regresar a versiones anteriores y proporciona una lista auditable que contiene información sobre cada modificación de archivo.

4.6 Seguridad de colaboración basada en grupos y centros

Los proyectos proporcionan una base sencilla para conceder o limitar el acceso a los diseños de Autodesk Fusion 360 a un conjunto de colaboradores. El propietario o el moderador del proyecto aprueba las invitaciones a los proyectos, lo que garantiza un control estricto sobre los miembros que conceden acceso a nuevos usuarios.

Las empresas pueden optar por los centros del equipo, que les permiten ejercer sus derechos de propiedad y tomar el control de acceso a todos los proyectos creados por los miembros. La configuración de privacidad de los proyectos, como los proyectos abiertos, cerrados y secretos, permite una colaboración controlada. Con los centros del equipo, los miembros pueden restringir el acceso a los colaboradores invitados al proyecto. Los centros del equipo también

permiten a los administradores de clientes desactivar cuentas de empleados antiguos y transferir la propiedad del proyecto a otros miembros del equipo.

4.7 Uso compartido público

Con el uso compartido público, los usuarios pueden colaborar con participantes externos que no tengan derechos de uso de Autodesk ID o Fusion 360. Los usuarios de Fusion 360 crean un vínculo que proporciona acceso de solo lectura al diseño. Los usuarios también tienen la opción de activar las funciones de descarga y exportación. En cualquier momento, el usuario puede revocar el uso compartido público que ofrece este vínculo.

5. Infraestructura en la nube

El equipo de infraestructura en la nube es responsable de definir y ejecutar procedimientos para la administración de versiones de aplicaciones, actualizaciones de hardware y del sistema operativo, supervisión del estado del sistema y otras actividades necesarias para mantener Autodesk Fusion 360.

5.1 Alta disponibilidad

Autodesk Fusion 360 se ha diseñado para lograr un alto nivel de disponibilidad mediante el uso de sistemas redundantes en su infraestructura de soporte y la distribución de la carga en una flota de instancias escalable.

5.2 Replicación y redundancia de datos

La replicación de datos de clientes se realiza entre las zonas de disponibilidad (AZ) de Amazon Web Services (AWS). La replicación limita la posibilidad de pérdida de datos o de un retraso en la reanudación del servicio si se requiere conmutación por error a un centro de datos de copia de seguridad.

5.3 Redundancia de sistemas de alimentación

Los centros de datos de AWS contienen sistemas de energía eléctrica redundantes para mantener las operaciones las 24 horas del día, los siete días de la semana. Las fuentes de alimentación ininterrumpida (UPS) proporcionan automáticamente respaldo a los sistemas eléctricos primarios en caso de avería. Los generadores de cada centro de datos proporcionan energía de respaldo a largo plazo en caso de que se produzca un apagón.

5.4 Redundancia de conectividad a Internet

Se utiliza un sistema redundante de varios proveedores para mantener la conectividad a Internet en cada uno de los centros de datos.

El software cliente de Autodesk Fusion 360 también tiene un modo sin conexión que permite a los usuarios seguir accediendo y trabajando en copias locales de su diseño cuando no están conectados a Internet.

5.5 Seguridad de la infraestructura física

La aplicación Autodesk Fusion 360 se ejecuta en centros de datos seguros de AWS que están protegidos contra el acceso físico no autorizado y los peligros medioambientales por una serie de controles de seguridad. A continuación se resumen algunos controles físicos y medioambientales. Aquí encontrará una descripción general completa de los procesos de seguridad de AWS.

5.6 Control de acceso a las instalaciones

Los centros de datos de AWS están protegidos las 24 horas del día, los siete días de la semana por personal de seguridad física profesional. El perímetro de cada centro de datos, así como las salas que contienen equipos informáticos y de soporte, se protegen mediante videovigilancia. La videovigilancia se conserva en medios digitales que permiten ver la actividad reciente bajo demanda. Las entradas a los centros de datos se vigilan con medidas de seguridad que restringen el acceso a una sola persona a la vez. Todos los visitantes y contratistas deben presentar una identificación para su admisión e ir acompañados por personal autorizado en todo momento. Solo los empleados con necesidades empresariales legítimas tienen acceso al centro de datos y todas las visitas se registran electrónicamente.

5.7 Prevención contra incendios

Los sistemas de detección y extinción de incendios, como alarmas de humo y tuberías húmedas activadas por calor, se instalan en todos los centros de datos para proteger las salas que contienen equipos informáticos y sistemas de soporte. Los sensores de detección de incendios se instalan en el techo y debajo de un suelo elevado.

5.8 Sistemas de control climático

Los sistemas de control climático de los centros de datos protegen los servidores, enrutadores y otros equipos susceptibles de averiarse si se incumplen los estrictos parámetros ambientales. Tanto los sistemas como el personal en las instalaciones supervisan la situación para evitar que se produzcan situaciones peligrosas, como el sobrecalentamiento. Los sistemas de control realizan automáticamente ajustes que mantienen la temperatura y otras medidas ambientales dentro de los intervalos aceptables.

6. Administración de incidentes de operaciones

Autodesk tiene una política de administración de incidentes que define las prácticas recomendadas para la resolución de incidentes. La política de administración de incidentes de Autodesk hace hincapié en el registro de los pasos de corrección y el uso del análisis de causa principal para crear una base de conocimientos de procedimientos que se puedan llevar a cabo. El objetivo de la política de gestión de incidentes de Autodesk no es solo cerrar incidentes de forma rápida y eficaz, sino también recopilar y distribuir información de incidentes para que los procesos mejoren continuamente y las respuestas futuras se basen en el conocimiento acumulado.

7. Administración de parches

El equipo de infraestructura en la nube tiene una política de administración de parches que ayuda a garantizar una implementación eficaz de los parches. Siempre que sea posible, se ha implementado la automatización para comprobar si hay nuevos parches y preparar listas de implementación que pueda aprobar el personal autorizado de la infraestructura en la nube. La política de parches también define criterios para determinar el impacto de un parche en la estabilidad de los sistemas. Si se identifica que un parche tiene un impacto posiblemente alto, se completarán las pruebas de regresión antes de que se implemente el parche. La administración de cambios realiza un seguimiento de la implementación de parches en los sistemas de producción.

8. Gestión de cambios

El equipo de infraestructura en la nube tiene una política de administración de cambios que incluye las siguientes actividades:

- **Formulario Solicitud de cambio (RFC).** Se debe enviar un formulario RFC para todos los cambios. El formulario incluye el nombre del iniciador del cambio, la prioridad del cambio, la justificación empresarial del cambio y una fecha de implementación del cambio solicitado.

- **Planes de recuperación.** El equipo de infraestructura en la nube crea planes detallados de recuperación antes de la implantación, de modo que el estado del sistema se puede restaurar si un cambio produce una interrupción del servicio. Los planes de recuperación incluyen instrucciones ejecutables definidas en secuencias de comandos que restauran el estado del sistema con un mínimo de pasos manuales.

- **Periodos de mantenimiento definidos.** El equipo de infraestructura en la nube especifica los periodos de mantenimiento programados, de emergencia y ampliados. Los periodos de mantenimiento se programan para las horas de menor actividad.

- **Plan de pruebas.** El equipo de infraestructura en la nube define una serie de pruebas para verificar que se puede acceder a la funcionalidad después de la implantación de un cambio.

- **Ejecución de pruebas.** Una vez completada la implantación, el equipo de infraestructura en la nube y de control de calidad de Autodesk Fusion 360 ejecuta las pruebas para comprobar que la funcionalidad identificada como en riesgo permanece disponible.

9. Administración de capacidades

Dado que el acceso de los clientes a los servicios en la nube se proporciona bajo demanda a través de un modelo de autoservicio, los patrones de tráfico son muy variables y están sujetos a altibajos en el uso. Cuando se produce un pico en el uso, la disponibilidad de un servicio puede verse afectada de forma negativa si se agota el conjunto de recursos informáticos que

alimentan el servicio. Para mantener un alto nivel de disponibilidad, el equipo de infraestructura en la nube implementa una política de administración de capacidad. Estas prácticas incluyen:

- **Registro frecuente del uso de recursos.** El uso de recursos de Autodesk Fusion 360 se recopila a intervalos frecuentes en una amplia gama de componentes de infraestructura, incluidos los volúmenes de almacenamiento virtual, las instancias virtuales y los dispositivos de red virtual. Las estadísticas de uso se almacenan en un repositorio de administración de capacidad.

- **Planificación de la capacidad.** El equipo de infraestructura en la nube utiliza la administración de capacidad para generar un plan de capacidad detallado que documente los niveles actuales de uso y modele los niveles futuros en función del análisis estadístico y el impacto de las próximas mejoras en la funcionalidad empresarial. El plan de capacidad se actualiza según sea necesario o si se detectan cambios significativos en los patrones de uso.

- **Asignación de recursos.** Los recursos informáticos se asignan a medida que los clientes los solicitan. Los recursos informáticos que se han preparado previamente están siempre disponibles. Si se produce un pico de actividad, se crean instancias de los nuevos recursos. Por ejemplo, la disponibilidad de los recursos del navegador de Autodesk Fusion suele lograrse en menos de 10 minutos.

- **Supervisión de la actividad.** Se definen paneles de actividad y alertas en todos los servicios backend, lo que permite a los técnicos observar la actividad del sistema y ejecutar exámenes y análisis tras los incidentes.

10. Alertas y supervisión

Para ofrecer un plazo medio de reparación lo más breve posible, Autodesk utiliza sistemas automatizados para supervisar Fusion 360 y validar el estado del servicio. Cada componente, desde la base de datos hasta los servicios, se supervisa de forma individual.

Si se produce un incidente que afecte al servicio, se generan alertas y se notifica al equipo de infraestructura en la nube mediante un proceso de escalado.

El estado del servicio también describe la interrelación entre los servicios de Autodesk. Un servicio como Autodesk Fusion 360 es muy sensible al servicio ACM (Control de acceso). Cada servicio debe ser resistente cuando falla un servicio dependiente y debe fallar de forma "limpia" cuando ya no puede funcionar sin pérdida de datos para el cliente.

El servicio de centro de controles de estado de Autodesk muestra públicamente el estado del servicio Fusion 360: https://health.autodesk.com.

11. Sin tiempo de inactividad durante las implantaciones

A medida que se aplican parches al entorno de producción, se adopta un enfoque de implementación azul-verde para el navegador de Autodesk Fusion y otros servicios de Fusion 360. Esto ayuda a garantizar que los clientes no experimenten ningún tiempo de inactividad del servicio.

12. Controles operativos de Autodesk Fusion 360

Autodesk Fusion 360 proporciona protección contra el acceso no autorizado a datos confidenciales de los clientes.

- **Restricciones físicas a los centros de datos.** Las restricciones físicas a los centros de datos impiden que partes no autorizadas accedan al hardware y a los sistemas de soporte utilizados por Autodesk Fusion 360.
- **Comprobaciones de antecedentes.** Se requieren comprobaciones de antecedentes para los empleados con acceso físico a los recursos informáticos y los sistemas de soporte utilizados por Autodesk Fusion 360.
- **Replicación de datos.** La replicación de datos copia los datos de los clientes en centros de datos redundantes, de modo que se pueda mantener la continuidad del negocio si se produce una conmutación por error entre las instalaciones.
- **Tecnologías redundantes**. Las tecnologías redundantes, como los equilibradores de carga y las bases de datos en clúster, limitan los puntos únicos de error.

13. Seguridad de Autodesk

El equipo de seguridad de Autodesk es un grupo dedicado de especialistas en seguridad de la información que se centra en identificar y aplicar prácticas de seguridad en el entorno de nube de Autodesk. Las responsabilidades del equipo de seguridad de Autodesk incluyen:

- Revisar la posición de seguridad del diseño y la implementación de la infraestructura en la nube de Autodesk.
- Definir y garantizar la implementación de políticas de seguridad, incluida la administración de identidad y acceso, la administración de contraseñas y la administración de vulnerabilidades.
- Fomentar el cumplimiento de los procedimientos de seguridad establecidos mediante revisiones y auditorías internas.
- Identificar e implementar tecnologías que aseguran la información del cliente
- Contratar expertos en seguridad de terceros para realizar evaluaciones de seguridad de la información
- Supervisar los servicios en la nube para detectar posibles problemas de seguridad y responder a incidentes según sea necesario
- Realizar revisiones anuales de la política de seguridad de Autodesk.

13.1 Exploraciones de vulnerabilidad y pruebas de penetración

Los servicios de Fusion 360 se someten a una prueba de intrusión anual y a análisis periódicos para detectar amenazas y vulnerabilidades de seguridad. La aplicación también se somete a análisis estáticos y a exploraciones de bibliotecas de terceros. Las exploraciones de seguridad y las pruebas de intrusión cubren una amplia gama de vulnerabilidades definidas por el Open Web Application Security Project (OWASP) y SANS Top 25.

13.2 Seguridad de la red

La seguridad de la red se aplica mediante una combinación de controles físicos y lógicos, incluidos el cifrado, los cortafuegos y los procedimientos de endurecimiento de sistemas.

Además, AWS proporciona controles de seguridad de red que protegen sus centros de datos físicos. Para obtener más información, consulte Prácticas recomendadas para la seguridad, la identidad y el cumplimiento.

13.3 Cifrado

Todo el tráfico de red se cifra cuando se transmite a través de Internet al perímetro del entorno de nube de Autodesk. La información confidencial, como las credenciales, la información de sesión de la aplicación, los tokens de acceso y los perfiles de usuario, se cifra en reposo.

13.4 Privacidad

Autodesk es transparente en la forma en que se recopilan y utilizan los datos personales de los clientes. Consulte la Declaración de privacidad de Autodesk para obtener más información.

14. Recursos

Los recursos siguientes proporcionan información general sobre Autodesk y otros temas a los que se hace referencia en la sección principal de este documento.

- **Autodesk**: para ver información sobre Autodesk, visite https://www.autodesk.es.
- **Centro de confianza de Autodesk**: para ver información sobre el Centro de confianza de Autodesk, visite http://trust.autodesk.com.
- **Autodesk Fusion 360**: para ver información sobre Fusion 360, visite http://fusion360.autodesk.com.

La información contenida en este documento representa la visión actual de Autodesk, Inc. en la fecha de publicación y Autodesk no asume ninguna responsabilidad por la actualización de esta información. En ocasiones, Autodesk realiza mejoras y otros cambios en sus productos o servicios, por lo que la información incluida en este documento solo se aplica a la versión de Autodesk Fusion 360 que se ofrece en la fecha de publicación.
Este documento técnico tiene fines meramente informativos. Autodesk no hace garantías, de forma expresa o implícita, en este documento, y la información de este documento técnico no crea ninguna obligación o compromiso vinculante por parte de Autodesk.
Sin limitar ni modificar lo anterior, los servicios de Autodesk Fusion 360 se proporcionan de acuerdo con los términos de servicio aplicables que se encuentran en https://www.autodesk.com/company/terms-of-use/es/general-terms.
Autodesk, el logotipo de Autodesk y Fusion 360 son marcas comerciales registradas de Autodesk, Inc., de sus filiales o de empresas asociadas en EE. UU. o en otros países. El resto de nombres de marcas, nombres de productos y marcas comerciales pertenecen a sus respectivos titulares. Autodesk se reserva el derecho a modificar las ofertas, las especificaciones y los precios de sus productos y servicios en cualquier momento y sin previo aviso, y no se hace responsable de los errores gráficos o tipográficos que puedan existir en el presente documento. © 2022 Autodesk, Inc. All rights reserved.