Estándares de seguridad de Autodesk BIM 360

SONDA

AUTODESK.
Corporate Business Partner

Introducción

Autodesk® BIM 360® es una plataforma de gestión de proyectos de construcción basada en la nube diseñada para mejorar el rendimiento a lo largo del ciclo de vida de un proyecto. Es un producto seguro, basado en la nube, que ofrece los beneficios de la colaboración en el espacio de construcción y al mismo tiempo protege los datos del cliente. La aplicación BIM 360 está diseñada y construida utilizando las mejores prácticas de software en la nube de su clase y está impulsada por Amazon Web Services (AWS), el líder mundial en infraestructura en la nube.
Se han diseñado los servicios para que sean escalables y seguros, proporcionando así a nuestros clientes una aplicación resistente y segura. Sabemos que el negocio de nuestros clientes depende de nosotros y tomamos esa responsabilidad en serio.

Propósito y alcance del documento

El propósito de este documento es describir las operaciones de Autodesk BIM 360, el desarrollo de software y las medidas de seguridad implementadas en el entorno. El alcance de este documento técnico se limita a las siguientes aplicaciones y servicios de BIM 360:

- BIM 360 Documents Management (Docs)
- BIM 360 Field Management (también conocido como Next Generation Field)
- BIM 360 Model Coordination (también conocido como Next Generation Glue® o Coordinate)
- BIM 360 Gestión de proyectos y BIM 360 Insight

Operaciones en la nube

El equipo de Operaciones en la nube es responsable de definir y ejecutar procedimientos para la administración de versiones de aplicaciones, actualizaciones de hardware y sistemas operativos, responsable del monitoreo del estado del sistema y de otras actividades requeridas para el mantenimiento de BIM 360.

Índice

Introducción

Nuestro compromiso con la alta disponibilidad permite a los clientes disfrutar de toda la potencia de BIM 360. Para lograr una alta disponibilidad, BIM 360 emplea sistemas redundantes en su infraestructura de soporte y distribuye la carga en una flota escalable de instancias. El sistema Autodesk BIM 360 consta de varios servidores web o de aplicaciones, sistemas de procesamiento de trabajos en segundo plano, sistemas de ejecución de informes y almacenes de datos y almacenamiento de archivos. Estos servicios se distribuyen en un par de zonas de disponibilidad (Availability Zones, o AZ) de AWS. Cada AZ es un centro de datos independiente dentro de un territorio, por lo que el uso de múltiples AZ protege las aplicaciones BIM 360 de interrupciones.
Para garantizar un alto nivel de servicio, el servicio BIM 360 apunta a una disponibilidad superior al 99,5%.

Continuidad del negocio y redundancia del centro de datos

Nuestro compromiso con la alta disponibilidad permite a los clientes disfrutar de toda la potencia de BIM 360. Para lograr una alta disponibilidad, BIM 360 emplea sistemas redundantes en su infraestructura de soporte y distribuye la carga en una flota escalable de instancias. El sistema Autodesk BIM 360 consta de varios servidores web o de aplicaciones, sistemas de procesamiento de trabajos en segundo plano, sistemas de ejecución de informes y almacenes de datos y almacenamiento de archivos. Estos servicios se distribuyen en un par de zonas de disponibilidad (Availability Zones, o AZ) de AWS. Cada AZ es un centro de datos independiente dentro de un territorio, por lo que el uso de múltiples AZ protege las aplicaciones BIM 360 de interrupciones.
Para garantizar un alto nivel de servicio, el servicio BIM 360 apunta a una disponibilidad superior al 99,5%.

Redundancia del sistema de energía

Para mantener las operaciones las 24 del día, se instalan sistemas de energía eléctrica redundantes en los centros de datos. En caso de falla, una fuente de alimentación ininterrumpida proporciona respaldo a los sistemas eléctricos primarios automáticamente. Los generadores ubicados en cada centro de datos proporcionan energía de respaldo a largo plazo si ocurre una interrupción.

Redundancia de conectividad a Internet

Autodesk BIM 360 utiliza un sistema redundante de múltiples proveedores para mantener la conectividad a Internet en cada uno de los centros de datos.

Duplicación de información

Los datos del cliente se replican entre centros de información en distintas ubicaciones. La duplicación evita la posibilidad de pérdida de datos o retraso en el servicio si se requiere conmutación por error a un centro de datos de respaldo.
Seguridad de infraestructura física

BIM 360 se ejecuta con Amazon AWS en centros de datos seguros. Los centros de datos están protegidos contra el acceso físico no autorizado y los peligros ambientales mediante una variedad de controles de seguridad.

- **Control de acceso a instalaciones.** Los centros de datos están vigilados las 24 horas, los 7 días de la semana por personal de seguridad profesional. Las entradas del centro de datos están protegidas por mantraps (vestíbulo de control de acceso) que restringen el acceso a una sola persona a la vez. Solo los empleados con necesidades comerciales legítimas tienen acceso al centro de datos y todas las visitas se registran electrónicamente. Todos los visitantes y contratistas deben presentar una identificación para ser admitidos y son escoltados por personal autorizado en todo momento.

- **Video vigilancia.** El perímetro de cada centro de datos y las salas que contienen equipos informáticos y de soporte están protegidos por videovigilancia. La videovigilancia se conserva en los medios digitales para que la actividad reciente se pueda ver a pedido.

- **Prevención de incendios.** Los sistemas de detección y supresión de incendios, como las alarmas de humo y las tuberías húmedas activadas por calor, se instalan en cada centro de datos para proteger las habitaciones que contienen equipos informáticos y sistemas de soporte. Los sensores de detección de incendios se instalan en el techo y debajo de un piso elevado.

- **Controles climáticos.** Los controles climáticos del centro de datos protegen servidores, enrutadores y otros equipos que pueden estar sujetos a fallas si se violan los rangos ambientales estrictos. El monitoreo y el personal están en su lugar para evitar condiciones peligrosas, como el sobrecalentamiento. Los sistemas de control ajustan automáticamente la temperatura y otras mediciones ambientales para mantenerlos dentro de los rangos aceptables.

Administración de operaciones de incidentes

BIM 360 tiene una política de gestión de incidentes que define las mejores prácticas para impulsar la resolución de incidentes. La política está guiada por el marco de la Biblioteca de Infraestructura de Tecnología de la Información (Information Technology Infrastructure Library o ITIL) Versión 3.
La política de gestión de incidentes de BIM 360 enfatiza el registro de los pasos de corrección de incidentes y la realización de análisis de causa raíz para construir una base de conocimiento de procedimientos procesables. El objetivo de la política no es solo cerrar incidentes de manera rápida y efectiva, sino también recopilar y distribuir información sobre incidentes para que los procesos se mejoren continuamente y las respuestas futuras sean impulsadas por el conocimiento acumulado.
Visite el Centro de confianza de Autodesk para obtener más detalles.

Administración de parches

El equipo de Cloud Operations tiene una política de administración de parches que ayuda a garantizar su implementación efectiva. Siempre que sea posible, se implementa la automatización para verificar nuevos parches y preparar listas de implementación aprobadas por personal autorizado de Cloud Operations. La política de parches de BIM 360 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, el personal de Operaciones en la Nube completa pruebas de regresión exhaustivas antes de implementar el parche. El equipo de gestión de cambios rastrea la implementación de parches en los sistemas de producción.

Gestión de cambios

El equipo de Operaciones en la nube tiene una política de gestión de cambios, que incluye los siguientes procesos y procedimientos:

- **Formulario de solicitud de cambio** (request for change o 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 comercial del cambio y una fecha de implementación del cambio solicitado.

- **Planes de retroceso.** El equipo de Cloud Operations crea planes detallados de retroceso antes de implementar un cambio para que puedan restaurar el estado del sistema si un cambio causa una interrupción del servicio. Los planes de retroceso incluyen instrucciones ejecutables, definidas en scripts, que restauran el estado del sistema con pasos manuales mínimos.

- **Ventanas de mantenimiento definidas.** El equipo de Operaciones en la nube especifica ventanas de mantenimiento programadas, de emergencia y extendidas. Ellos programan el mantenimiento planificado durante las horas de menor actividad.

- **Plan de prueba.** El equipo de Operaciones en la nube define un conjunto de pruebas para verificar que la funcionalidad sea accesible después de la implementación de un cambio.

- **Ejecución de pruebas.** Una vez que se completa la implementación, los equipos de Operaciones de nube y Control de calidad del producto ejecutan las pruebas para verificar que la funcionalidad en riesgo permanezca disponible.

Gestión de capacidad

Debido a que el acceso del cliente a los servicios en la nube se aprovisiona a pedido mediante un modelo de autoservicio, los patrones de tráfico son muy variables y están sujetos a altos en su uso. Cuando se produce un alto, la disponibilidad de un servicio puede verse afectada negativamente si se agota el conjunto de recursos informáticos que impulsan el servicio.

Para mantener un alto nivel de disponibilidad, el equipo de Operaciones en la nube ha implementado una política de gestión de capacidad. Como parte de la política de gestión de capacidad, el uso de recursos de BIM 360 se recopila a intervalos frecuentes en una amplia gama de componentes de infraestructura, incluidas instancias virtuales, volúmenes de almacenamiento virtual y dispositivos de red virtual. Las estadísticas de uso se almacenan en un repositorio de gestión de capacidad.

Rendimiento y escalabilidad

Para proporcionar un alto nivel de disponibilidad, se ejecutan pruebas de rendimiento y carga durante todo el ciclo de vida de desarrollo de software.

Controles de seguridad operacional de BIM 360

BIM 360 tiene varios controles de seguridad que protegen los datos confidenciales de los clientes contra el acceso no autorizado.

- **Restricciones físicas a los centros de datos.** Las restricciones físicas a los centros de datos evitan que terceros no autorizados accedan al hardware y a los sistemas de soporte utilizados por BIM 360.

- **Verificaciones de antecedentes.** Se requieren verificaciones de antecedentes para los empleados antes de que se les otorgue acceso a los recursos informáticos y los sistemas de soporte utilizados por BIM 360.

- **Ejecución de pruebas.** Una vez que se completa la implementación, los equipos de Operaciones de nube y Control de calidad del producto ejecutan pruebas para verificar que la funcionalidad identificada “en peligro” permanezca disponible.

- **Funcionalidad administrativa.** Las herramientas administrativas de BIM 360 son una forma flexible de gestionar usuarios, otorgar permisos basados en roles y otros controles de acceso para usuarios finales.

- **Tecnologías redundantes.** Las tecnologías redundantes como los equilibradores de carga y las bases de datos agrupadas limitan los puntos únicos de falla.

Gestión de capacidad

El equipo de ingeniería de BIM 360 es responsable de diseñar, implementar y probar la aplicación BIM 360.

El diseño, la programación, las pruebas y el mantenimiento de BIM 360 se basan en un proceso de desarrollo de software que incluye procesos de seguridad según sea necesario.

Durante la etapa de diseño, se producen documentos de diseño detallados de historias de usuarios y los arquitectos los revisan para evaluar la funcionalidad y la escalabilidad del diseño. La fase de diseño utiliza un proceso conjunto de diseño de aplicaciones donde arquitectos e ingenieros de software evalúan la funcionalidad, escalabilidad y características de rendimiento de las historias de los usuarios.

Durante la implementación, los ingenieros y arquitectos realizan revisiones de código de pares para detectar desviaciones de las prácticas de desarrollo de aplicaciones BIM 360.
Todo el código producido durante el proceso incluye pruebas unitarias, integración y verificación de control de calidad. Ninguna historia de usuario está completa hasta que el personal de garantía de calidad verifica los criterios de aceptación.

Como parte del ciclo de vida del desarrollo, el equipo de rendimiento de BIM 360 realiza pruebas de carga durante los sprints (ejercicios de alta intensidad) de desarrollo para detectar cambios que afectan negativamente el rendimiento lo antes posible en el proceso.

Capacitación de empleados

Todos los empleados de Autodesk deben estar de acuerdo en la importancia de la seguridad de la información, como parte de la guía para nuevos empleados. Además, los empleados deben leer, comprender y tomar un curso de capacitación sobre el Código de Conducta de la compañía. El código requiere que cada empleado realice negocios de manera legal, ética, con integridad y con respeto entre colegas, usuarios, socios y competidores de la empresa.

Los empleados de Autodesk deben seguir las pautas de la compañía con respecto a la confidencialidad, la ética empresarial, el uso apropiado y los estándares profesionales. Los nuevos empleados deben firmar un acuerdo de confidencialidad.

La orientación a los nuevos empleados enfatiza la confidencialidad y privacidad de los datos del cliente. Para implementar las mejores prácticas de seguridad, hemos introducido un programa anual de capacitación en seguridad para todos los ingenieros de BIM 360.

Controles de seguridad del producto BIM 360

Autodesk BIM 360 tiene características de seguridad integradas que permiten a los clientes crear políticas detalladas de administración de identidad y acceso. Los administradores y usuarios del cliente pueden usar las herramientas de seguridad de BIM 360 para administrar la propiedad de los elementos de su espacio de trabajo y establecer permisos de uso compartido en sus informes.

Autenticación y cifrado en tránsito

Se requieren credenciales que consisten en una identificación de usuario y una contraseña para acceder a BIM 360. Las credenciales se protegen durante la transmisión de la red y se almacenan solo como salted hash (claves encriptadas), generado por una función de hash criptográfico SHA-2.

Seguridad de datos

Todos los archivos cargados por el cliente BIM 360 se almacenan en la nube en un almacenamiento cifrado. La solución de almacenamiento utiliza cifrado avanzado de 256 bits (AES-256).

Controles administrativos

BIM 360 proporciona a los administradores características de seguridad para crear políticas de administración de identidad y acceso.

- **Asignación de usuarios:** los administradores pueden crear y desactivar usuarios.

- **Uso de seguridad basada en roles:** los roles de BIM 360 permiten a los administradores personalizar los niveles de acceso, para proporcionar controles precisos para restringir el acceso. Un rol es una colección de permisos de datos y funcionalidad relacionados con una función de trabajo. Al proporcionar una forma flexible de asignar permisos basados en roles, BIM 360 se adhiere al principio del mínimo privilegio, que requiere que el acceso de cada usuario a los datos y la funcionalidad se limite a lo que necesitan para completar sus tareas asignadas.

Controles del usuario

Los usuarios pueden controlar el acceso a los elementos, informes y archivos que poseen, con excepción de las restricciones administrativas. Los usuarios también pueden usar el control de versiones de archivos para restaurar versiones anteriores de archivos que han adjuntado a elementos del espacio de trabajo.

Seguridad en la nube

Nuestro equipo de Cloud Security se enfoca en identificar y hacer cumplir la seguridad dentro del entorno de nube Autodesk BIM 360.

Las responsabilidades incluyen:

- Revisar la postura de seguridad del diseño e implementación de la infraestructura en la nube de Autodesk.
- Definir y garantizar la implementación de políticas de seguridad, incluida la gestión de identidad y acceso, gestión de contraseñas y gestión de vulnerabilidades.
- Impulsar el cumplimiento de los procedimientos de seguridad establecidos mediante la realización de revisiones internas y auditoras.
- Identificar e implementar tecnologías que aseguren la información del cliente.
- Involucrar a expertos en seguridad de terceros para realizar evaluaciones de seguridad según sea necesario.
- Monitorear los servicios en la nube para detectar posibles problemas de seguridad y responder a incidentes según sea necesario.

Análisis de vulnerabilidades, pruebas de penetración y auditorías

El equipo de Cloud Security realiza análisis de seguridad y pruebas de penetración de los servicios BIM 360 con regularidad. Los escaneos de seguridad y las pruebas de penetración cubren una amplia gama de vulnerabilidades definidas por Open Web Application Security Project (OWASP) y SANS Top 25.

Análisis de vulnerabilidades, pruebas de penetración y auditorías

La seguridad de la red se aplica mediante una combinación de controles físicos y lógicos, que incluyen cifrado, cortafuegos (físicos o lógicos) y procedimientos de endurecimiento. Los corta-

-fuegos de hardware independientes se implementan en el perímetro de la nube en nuestros centros de datos. Todos los puertos están bloqueados, excepto los necesarios para atender las solicitudes de los clientes. El tráfico de Encryption Network que contiene información confidencial, como credenciales y tokens de sesión, se transmite de forma segura a través de Internet al perímetro de nuestro entorno.

Cumplimiento y estándares de seguridad externas

El equipo de Cloud Security realiza análisis de seguridad y pruebas de penetración de los servicios BIM 360 con regularidad. Los escaneos de seguridad y las pruebas de penetración cubren una amplia gama de vulnerabilidades definidas por Open Web Application Security Project (OWASP) y SANS Top 25.

- Autodesk BIM 360 ha seleccionado el estándar de la industria: SSAE-16 AT 101 SOC 2 para validar nuestra postura de seguridad.
- Autodesk BIM 360 tiene las certificaciones ISO 27001, ISO 27017 e ISO 27018.

Recursos

Autodesk es transparente sobre cómo se recopilan y utilizan los datos personales de los clientes.
Lea la Declaración de privacidad de Autodesk para obtener más información.

Privacidad

Los siguientes recursos proporcionan información general sobre Autodesk e información adicional sobre los temas a los que se hace referencia en este documento.

- Para obtener más información sobre Autodesk, visite: http://www.sonda-mco.com.
- Para obtener más información sobre nuestro marco de seguridad integral, visite: https://www.autodesk.com/trust/security.
- Las aplicaciones BIM 360 están alojadas en AWS. Como tal, la seguridad y la infraestructura son una responsabilidad compartida entre Autodesk y Amazon.