ALTIUM 365

Enfoque y prácticas de seguridad

CONTENT

Introducción

Altium 365 es la plataforma de desarrollo electrónico que unifica el diseño, los datos y la colaboración en un único entorno seguro en la nube. Está diseñada para respaldar todo el ciclo de vida del desarrollo electrónico, ya que proporciona la infraestructura moderna que necesitan los equipos de ingeniería para trabajar más rápido, de forma más eficiente y a escala. La plataforma viene incluida con Altium Agile y Altium Develop, y optimiza los flujos de trabajo, aumenta la productividad y acelera la entrega de productos.

En Altium, creemos que el verdadero valor de una plataforma en la nube no se mide solo por lo que permite hacer, sino también por la seguridad con la que protege el trabajo que se le confía. La seguridad está integrada en el núcleo de la arquitectura de Altium 365 y guía la forma en que diseñamos, desarrollamos y operamos la plataforma. Este compromiso nos impulsa a cumplir y superar continuamente los estándares modernos de ciberseguridad.

Este documento técnico te ofrece una visión clara y transparente de las amplias medidas de seguridad en las que se basa Altium 365. Nuestro objetivo es sencillo: mostrarte cómo se protegen tus datos, cómo se diseñan nuestras medidas de seguridad y cómo evoluciona nuestra postura de seguridad para adelantarse a las amenazas emergentes.

A medida que avances por estas páginas, conocerás la planificación, los procesos y los mecanismos de protección que conforman nuestro enfoque, desde las prácticas de desarrollo seguro hasta los controles por capas integrados en toda la plataforma. Verás cómo nuestro rigor de ingeniería, nuestra disciplina operativa y nuestra arquitectura nativa de la nube trabajan mano a mano para proteger tus datos en cada paso.

En definitiva, nuestro objetivo es darte la tranquilidad de saber que tu trabajo colaborativo en Altium 365 está protegido por un marco de seguridad robusto que evoluciona de forma continua. Queremos que te centres en crear e innovar, mientras nosotros nos encargamos de la seguridad que lo protege.

Este documento describe el enfoque y las prácticas de seguridad de Altium 365 a nivel de plataforma; las capacidades específicas pueden variar según la suscripción, el entorno de implementación (p. ej., GovCloud) y la configuración del cliente.

Medidas de seguridad de Altium 365

La seguridad es la base de la confianza, y nuestros clientes confían en Altium 365 para proteger sus activos más valiosos: sus datos, diseños y propiedad intelectual. La seguridad está integrada en cada capa de la plataforma, desde las primeras fases de arquitectura y desarrollo hasta la implementación y las operaciones continuas. Nuestro enfoque es meticuloso, proactivo y evoluciona continuamente, creando un entorno seguro y resiliente para el desarrollo colaborativo de productos electrónicos.

Desarrollo impulsado por la seguridad

Hemos desarrollado la plataforma Altium 365, sus características y funcionalidades teniendo en cuenta la seguridad del usuario. En cada etapa del desarrollo, verificamos rigurosamente las medidas de seguridad implementadas. Esto incluye revisiones exhaustivas de la arquitectura, análisis de dependencias, revisiones de código y pruebas dinámicas de seguridad de las aplicaciones. Nuestro objetivo es identificar, abordar y prevenir de forma proactiva cualquier posible vulnerabilidad de seguridad desde el principio. Además, empleamos pruebas independientes de terceros para garantizar que nuestro marco de seguridad sea sólido.

Protección de Datos Fiable

Amazon Web Services (AWS) constituye la columna vertebral de la seguridad física y la fiabilidad de Altium 365. Almacenamos los datos de los clientes exclusivamente en recursos de AWS y utilizamos específicamente el servicio de base de datos relacional (RDS) para nuestros requisitos respecto a las bases de datos. Para el almacenamiento de datos binarios estándar, utilizamos AWS S3, mientras que FSx se emplea en situaciones que requieren almacenamiento binario de alto rendimiento. También usamos clústeres de Elasticsearch dedicados para proporcionar capacidades de búsqueda de alto rendimiento.

Los datos en reposo en Altium 365 se cifran mediante claves de AWS Key Management Service (KMS). Estas claves utilizan módulos de seguridad de hardware validados según los estándares FIPS 140-2, un estándar de seguridad informática del gobierno de EE. UU. utilizado para aprobar módulos criptográficos. El uso de estas claves de cifrado se registra y supervisa. Los registros se envían posteriormente a nuestro sistema de gestión de eventos e información de seguridad (SIEM), lo que nos permite realizar un seguimiento de cuándo se utilizan las claves de cifrado.

El acceso a la infraestructura de Altium 365 que aloja los datos de los clientes está limitado al personal autorizado conforme al principio de privilegio mínimo. Todos los accesos se registran, son auditables y están sujetos a supervisión continua por parte del equipo de seguridad especializado de Altium.

Comunicación Segura

La comunicación entre los clientes de Altium 365, como puede ser un navegador web, Altium Designer o una aplicación móvil, y la plataforma en la nube Altium 365 solo se permite a través de conexiones seguras y fiables que utilizan el protocolo HTTPS, es decir, un enfoque estándar para asegurar las comunicaciones de internet, a través de puertos estándar.

Autenticación y gestión de identidades

Para acceder a los servicios de Altium 365 que gestionan datos confidenciales de los clientes, los usuarios deben someterse a un proceso de autenticación para cada solicitud. Esta autenticación no se limita a las credenciales tradicionales de nombre de usuario y contraseña; también se integra con sistemas de inicio de sesión único (SSO) o proveedores de identidad (IdP), como Google y Facebook. Estos sistemas pueden utilizar diversas credenciales, entre los que se incluyen las claves de hardware, tarjetas inteligentes o datos biométricos, como huellas dactilares, que no controlamos directamente. Independientemente del método, todas las sesiones tienen una duración limitada por motivos de seguridad y toda la información confidencial de acceso se cifra de forma segura durante la transmisión.

Altium 365 admite el inicio de sesión único mediante el protocolo SAML 2.0. Esta función se integra con los IdP más modernos, incluidos OneLogin, Okta, Microsoft Azure AD y Google Identity. La compatibilidad ampliada con el protocolo SCIM permite organizar el aprovisionamiento y desaprovisionamiento centralizado de usuarios y grupos. Dependiendo del IdP, es posible optar por una protección mejorada con autenticación multifactor (MFA).

Distribución y control

Altium 365 emplea protecciones perimetrales en capas para controlar e inspeccionar el tráfico entrante, incluidos un cortafuegos de aplicaciones web y un equilibrio de carga gestionado. Estos controles ayudan a proteger los puntos de conexión expuestos a Internet y respaldan la disponibilidad al distribuir el tráfico entre los servicios de aplicaciones. El acceso administrativo a los sistemas de producción está restringido al personal autorizado según el principio de privilegio mínimo, y se registra y supervisa.

Arquitectura de tenant único y multi-tenant

Altium 365 funciona con una arquitectura multi-tenant en la que cada tenant (actualmente alineado con el concepto de espacio de trabajo) recibe su propio esquema de base de datos aislado. Este modelo proporciona una sólida separación de datos al tiempo que aprovecha la infraestructura compartida en la nube para lograr eficiencia y escalabilidad. Para las organizaciones que requieren mayor aislamiento, personalización y control operativo, Altium ofrece un entorno de tenant único (STE): una instancia dedicada de la aplicación y de la infraestructura que la respalda. El STE proporciona un alto nivel de aislamiento de datos, un rendimiento predecible y opciones de configuración específicas para cada tenant, combinando la comodidad de un servicio alojado con el control tradicionalmente asociado a las implementaciones locales.

Análisis de vulnerabilidades

Las implementaciones en producción de Altium 365 están sujetas a análisis de vulnerabilidades como parte del proceso de lanzamiento. Los resultados se rastrean hasta su solución o su aceptación documentada del riesgo, de acuerdo con la política de gestión de vulnerabilidades de Altium y los plazos de solución definidos.

Pruebas de terceros

Anualmente, colaboramos con terceros externos para realizar pruebas de penetración y garantizar que mantenemos el nivel más alto de seguridad frente a las amenazas en constante evolución. El equipo de desarrollo revisa todos los comentarios de las pruebas de penetración e implementa las actualizaciones necesarias en nuestros servicios de aplicaciones e infraestructura. Estamos dispuestos a compartir el resumen ejecutivo más reciente de nuestro informe de pruebas de penetración con las partes interesadas, siempre que exista un Acuerdo de Confidencialidad Mutuo (MNDA, por sus siglas en inglés).

Supervisión de seguridad y gestión de incidentes

Hemos implementado una práctica integral de registro y supervisión para permitir la detección temprana y una respuesta eficaz ante incidentes de seguridad. Utilizando el marco de ciberseguridad del NIST como base, el registro y la supervisión son componentes clave de las funciones «Detectar» y «Responder». Estas funciones son esenciales para identificar y comprender eventos y vulnerabilidades de seguridad, lo que mejora la exactitud y precisión de Altium 365. La identificación de incidentes es fundamental en nuestro proceso de respuesta a incidentes, en el que los equipos de seguridad, los sistemas y las herramientas trabajan conjuntamente para reconocer y confirmar posibles incidentes de seguridad. Una vez identificado un incidente de seguridad, activamos nuestro Plan de respuesta a incidentes para garantizar una respuesta rápida y eficaz alineada con los objetivos de seguridad y empresariales de la organización.

Concienciación y formación en seguridad

Altium garantiza que todas las nuevas contrataciones reciban formación sobre concienciación en materia de seguridad durante la incorporación, con cursos de actualización anuales para todo el personal. El equipo de Recursos Humanos realiza un seguimiento de los empleados que no han completado su formación para garantizar el cumplimiento normativo. Además, enviamos periódicamente notificaciones de concienciación en materia de seguridad al personal para informarles de nuevos protocolos y posibles amenazas. Nuestro equipo de Investigación y Desarrollo recibe formación especializada en prácticas de codificación segura. El material de formación se revisa y se actualiza periódicamente para reflejar las prácticas de codificación o los lenguajes de programación.

Privacidad de los datos

Los términos generales de servicio de Altium y la política de privacidad describen los pasos que tomamos para garantizar la privacidad y la seguridad de los datos de los clientes. Estos documentos y nuestros procedimientos internos de apoyo cumplen con las normativas globales de protección de datos, incluidos el RGPD y la Ley de Privacidad del Consumidor de California (CCPA). Este cumplimiento garantiza la confidencialidad, la integridad y la disponibilidad de todos los datos gestionados por Altium, incluida la información que nos confían nuestros clientes y socios comerciales. En el competitivo entorno empresarial global actual, es fundamental mantener la privacidad de los datos a fin de evitar amenazas, incluidos los errores, pérdidas, fraudes o espionaje. Por eso, nuestro enfoque está diseñado para evitar cualquier violación de seguridad en los datos que gestionamos.

Política de cookies

Puedes administrar tus preferencias de cookies a través de la configuración de tu navegador. Algunos navegadores te permiten incluir en una lista segura los sitios de los que aceptas las cookies. Para obtener más información sobre la gestión de las preferencias de cookies, consulta nuestra política de cookies.

Política de retención de datos

Si deja de usar Altium 365, sus datos se conservarán durante los plazos especificados en nuestra política de retención de datos. Una vez transcurrido este periodo, sus datos se eliminarán de nuestros sistemas.

Copias de seguridad y recuperación ante desastres

Altium 365 emplea un sistema automatizado de copias de seguridad para garantizar que todos los datos almacenados en Altium 365 se copien en nuestras regiones de copia de seguridad, eliminando la intervención manual. Contamos con un plan integral de recuperación ante desastres para respaldar la continuidad del negocio de los servicios y las plataformas de producción. En caso de interrupción del sistema, nuestro objetivo es que el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO) sean de 24 horas cada uno. Este plan se revisa y prueba cada 120 días para confirmar su eficacia e incluye políticas y procedimientos detallados para restablecer los servicios en caso de desastre.

> Para obtener más información, visita el Centro de confianza de Altium 365 y consulta las respuestas a las preguntas más frecuentes.

Altium 365 GovCloud

Altium 365 GovCloud es una región dedicada de la plataforma en la nube Altium 365 situada dentro de EE. UU., operada exclusivamente por ciudadanos estadounidenses en la región AWS GovCloud. Elegir un espacio de trabajo de Altium 365 en la región GovCloud puede ayudar a las organizaciones a cumplir con regulaciones del gobierno de EE. UU., como el ITAR y el EAR.

Personas estadounidenses

La operación de la región GovCloud en el lado de Altium está restringida únicamente a pe rsonas de EE. UU Los clientes de Altium determinan y controlan a quién añaden a su espacio de trabajo y a quién otorgan acceso a los datos almacenados en este.

Protección de datos

Control del tráfico saliente

Para protegernos frente a la exportación no autorizada de datos, empleamos un proxy de salida que controla e impide que el tráfico saliente no autorizado salga del entorno.

Funcionalidad limitada

Hemos desactivado, de forma predeterminada, las funcionalidades que podrían provocar involuntariamente la salida de datos desde EE. UU., mitigando así los riesgos asociados a errores de los usuarios.

- **Compartir fuera del espacio de trabajo.** De forma predeterminada, la opción de compartir proyectos, lanzamientos, bibliotecas y paquetes de fabricación (función «Enviar al fabricante») con personas que no forman parte del espacio de trabajo de Altium 365 GovCloud está desactivada. Sin embargo, los administradores pueden modificar esta configuración si es necesario.
- **Espacio personal de Altium 365.** Los usuarios añadidos a un espacio de trabajo de Altium 365 GovCloud no pueden almacenar ningún dato en sus espacios de Altium 365 Personal.
- **Integración de PLM.** El administrador controla la conexión con sistemas PLM de terceros y proporciona la configuración necesaria.
- **Sistemas de cliente.** La responsabilidad de Altium no se extiende a la configuración, la seguridad ni el mantenimiento de los sistemas del lado del cliente, como los navegadores o las herramientas de CAD, conectados a Altium 365 GovCloud. El cliente debe mantener estos sistemas actualizados e instalar todas las actualizaciones y parches necesarios.

Suelo estadounidense

Las regiones AWS GovCloud Este de EE. UU. y Oeste de EE. UU. están gestionadas por empleados con ciudadanía estadounidense ubicados en suelo estadounidense.

Controles de acceso

Acceso al espacio de trabajo desde fuera de EE. UU.

El acceso al espacio de trabajo desde fuera de EE. UU. está bloqueado explícitamente, incluido el acceso de personas estadounidenses que intentan acceder al espacio de trabajo desde otro país. Lee más información sobre el acceso mediante VPN aquí.

Para obtener más información, visita Altium 365 GovCloud.

Cumplimiento: Certificaciones y normativas

El cumplimiento no es solo una casilla que marcar; es un compromiso con la excelencia y una promesa de fiabilidad. En Altium 365, nos tomamos esta responsabilidad muy en serio y nos aseguramos de que nuestra plataforma cumpla los más altos estándares de cumplimiento y certificación.

STAR Level 1 de la CSA: autoevaluación

El programa Security, Trust, Assurance, and Risk (STAR) es una iniciativa de la Cloud Security Alliance (CSA) diseñada para ofrecer un marco de garantía sólido para la computación en la nube. Altium 365 ha alcanzado el STAR Level 1 de la CSA, que es una autodeclaración de cumplimiento de los controles de la Cloud Control Matrix (CCM), comúnmente conocida como Consensus Assessment Initiative Questionnaire (CAIQ). Por lo tanto, Altium 365 figura en el STAR Registry.

Certificación SOC 2 Type 2

Altium 365 cuenta con la certificación Service Organization Control (SOC) 2 Type 2, lo que confirma que mantenemos los más altos estándares de seguridad de datos y sistemas en relación con el principio de seguridad. Este marco de cumplimiento en materia de ciberseguridad fue desarrollado por el Instituto Americano de Contables Públicos Certificados (AICPA) y exige que las empresas se sometan a una auditoría realizada por un auditor externo acreditado por el AICPA. Altium 365 realiza auditorías SOC 2 Type 2 anualmente.

GDPR

Reconocemos la importancia de la privacidad de los datos y nos comprometemos a cumplir los estrictos requisitos establecidos por el Reglamento General de Protección de Datos (RGPD), garantizando que sus datos se traten con el máximo cuidado y respeto.

Cumplimiento del ITAR

Altium 365 GovCloud puede ayudar a nuestros clientes a cumplir con el Reglamento Internacional de Tráfico de Armas (ITAR, por sus siglas en inglés). Esta región especializada satisface las necesidades específicas de nuestros usuarios que trabajan en sectores altamente regulados.

Funciones de seguridad y gobernanza de Altium 365

Altium® proporciona capacidades avanzadas de seguridad, identidad y gobernanza que ayudan a las organizaciones a proteger los datos de diseño confidenciales, mantener el cumplimiento y gestionar el acceso a gran escala.

Control de acceso

- **Permisos de datos básicos**
  Derechos fundamentales de visualización y edición que definen cómo interactúan los usuarios con archivos, carpetas y proyectos en toda la plataforma.
- **Permisos avanzados de datos**
  Controles que van más allá de los derechos de acceso básicos, incluidas las reglas de uso compartido a nivel de organización, la configuración detallada de permisos y las opciones avanzadas de herencia que determinan cómo se accede a los datos o cómo se restringen entre los equipos.
- **Gestión de grupos**
  Estandariza los permisos, las licencias y la visibilidad del espacio de trabajo al asignar el acceso según roles definidos, lo que garantiza un control uniforme y escalable en toda la organización.
- **Compatibilidad con invitados externos**
  Controla cómo se invita, se agrupa y se limita a los colaboradores externos, con reglas de visibilidad y flujos de trabajo obligatorios que mantienen el acceso de los invitados restringido y seguro.
- **Filtro de acceso**
  Busca y audita el acceso efectivo en todos los proyectos, con ajustes rápidos y eliminación de invitados con un solo clic.

Autenticación y aprovisionamiento de usuarios

- **Gestión de la organización**
  Define cómo los usuarios se unen a la organización, cómo se asignan los roles y cómo las reglas basadas en dominios regulan la identidad y el acceso a los recursos internos.
- **Inicio de sesión único (SSO) & SCIM**
  Se integra con el proveedor de identidad existente para centralizar la autenticación y automatizar el aprovisionamiento y desaprovisionamiento de usuarios mediante SCIM.
- **Autenticación multifactor (MFA)**
  Refuerza la seguridad de las cuentas al requerir un paso de verificación adicional, lo que reduce el riesgo de acceso no autorizado incluso si las credenciales se ven comprometidas.
- **Gestión de grupos**
  Admite el aprovisionamiento de identidades al asignar usuarios a roles y perfiles de acceso predefinidos durante la incorporación y a lo largo de todo su ciclo de vida.

Seguridad avanzada

- **Listas blancas de IP**
  Restringe el acceso a la plataforma a direcciones o rangos de IP aprobados, lo que garantiza que solo las redes de confianza puedan acceder a los datos confidenciales de la organización.
- **Registro de eventos**
  Proporciona visibilidad de las acciones de los usuarios y del sistema en todo el espacio de trabajo, lo que facilita la auditoría, las revisiones de seguridad y la generación de informes de cumplimiento mediante registros claros de actividad con marca de tiempo.
- **SIEM (API)**
  Conecta los datos de eventos de Altium Agile con su SIEM actual, lo que permite el análisis centralizado, las alertas y el seguimiento del cumplimiento en toda la organización.

Mantente al día con nuestras últimas actualizaciones de seguridad

Nuestra plataforma sigue avanzando con nuevas funciones que refuerzan la gobernanza, mejoran la visibilidad y respaldan los requisitos de seguridad de las organizaciones modernas de electrónica. La seguridad sigue siendo fundamental, y cada actualización está diseñada para ayudar a los equipos a avanzar con rapidez mientras mantienen el control de los datos confidenciales y regulados.

A medida que evoluciona el panorama del desarrollo de la electrónica y la protección de datos, evolucionamos con él. Nuestro objetivo es ofrecerte mejoras prácticas y escalables que satisfagan las necesidades actuales y que preparen a tu organización para lo que venga después.

Mantente al tanto de las mejoras continuas a medida que ampliamos los controles, profundizamos la supervisión y reforzamos las protecciones, garantizando que la seguridad y la innovación sigan estando alineadas.

Para obtener más información y recursos relacionados, visita altium.com

¿Quieres más información? www.altium.com/platform/trust

La información incluida en este informe técnico es precisa a partir de febrero de 2026. Tenga en cuenta que Altium 365 es una plataforma en constante evolución. Para consultar la versión más reciente de este documento, visita esta página.