Julio 2024

Informe de seguridad

BIMserver.center

BIMserver.center

Tabla de contenidos

Introducción

En la actualidad, la seguridad e integridad de los datos en las plataformas digitales es un deber de todas aquellas organizaciones que gestionen información sensible. BIMserver.center es una plataforma integral de gestión de datos y colaboración en proyectos de arquitectura, ingeniería, construcción y operación, diseñada con un enfoque exhaustivo en la seguridad y protección de la información. Teniendo en cuenta las crecientes amenazas y desafíos en el ámbito digital, se han implementado medidas avanzadas para garantizar la seguridad de los datos y la continuidad operativa de nuestros servicios.

Este documento detalla el enfoque de seguridad de BIMserver.center, describiendo las medidas organizativas y técnicas implementadas para proteger la información de los usuarios. Aborda aspectos clave como datos e infraestructura, control de acceso, seguridad física, gestión de incidentes, recuperación ante desastres, seguridad de API y operaciones de plataforma. Al adoptar las mejores prácticas de la industria y mantenerse a la vanguardia en tecnología de seguridad, se garantiza que los clientes puedan confiar en la resiliencia y fiabilidad de los servicios.

Datos e infraestructura

En BIMserver.center, la protección y gestión adecuada de los datos es fundamental para garantizar la seguridad y confidencialidad de la información. Esta sección describe la arquitectura de almacenamiento y las medidas de protección implementadas para salvaguardar tanto la información personal como los archivos de proyecto, asegurando el cumplimiento de las normativas vigentes y la alta disponibilidad del servicio.

Almacenamiento y protección de datos

BIMserver.center garantiza la seguridad de los datos mediante una arquitectura de almacenamiento basada en una nube híbrida, con servidores propios y externos, en colaboración con OVH como proveedor cloud. Los datos del proyecto se dividen en información privada y pública:

- **Información privada:** La información personal de los usuarios, detalles de proyectos, aportaciones, sus relaciones con otros usuarios y entidades, y las restricciones de acceso, como también la información relativa a las entidades de las cuentas Developers, Education, Corporate y Validation, se almacenan en una base de datos PostgreSQL ubicada en los servidores del centro de datos de CYPE en Alicante, España.

- **Información pública:** Toda la información relativa a los ficheros de los proyectos que los usuarios suben a la plataforma para su uso personal o compartido, está almacenada en servidores dedicados en los centros de datos de OVH en Francia. (https://www.ovhcloud.com/es-es/personal-data-protection)

Cumplimiento y confidencialidad

La información privada, incluyendo datos personales e identificación de edificios, se aloja físicamente en servidores dentro de la UE, asegurando el cumplimiento de la legislación europea y garantizando la confidencialidad en procesos sensibles, como la contratación pública.

Acceso a los datos y control de privacidad

El control de acceso y la privacidad son pilares esenciales para mantener la integridad y confidencialidad de la información en BIMserver.center. En esta sección, se explican los mecanismos de autenticación, autorización y control de privacidad que garantizan que solamente los usuarios autorizados accedan a la información, y se detallan las medidas de seguridad implementadas para proteger las contraseñas y gestionar identidades.

Gestión de identidad y autenticación

BIMserver.center implementa mecanismos robustos de gestión de identidad, autenticación y autorización para garantizar el acceso seguro a la información por parte de los usuarios finales. Los usuarios deben autenticarse con su correo electrónico y contraseña para acceder a la plataforma, ya sea a través de la web, de la aplicación móvil o de aplicaciones conectadas a través de la API pública. Las sesiones de usuario son exclusivas, están protegidas y caducan tras un periodo de inactividad. Los intentos fallidos de acceso se registran y provocan bloqueos temporales para prevenir ataques de fuerza bruta.

Control de acceso a la información

Los usuarios de BIMserver.center podrán especificar el nivel de acceso y visibilidad de las distintas aportaciones de un proyecto. En cualquier momento el propietario y las personas autorizadas podrán restringir la visualización pública de estos proyectos y aportaciones.

Además, algunos trabajadores de BIMserver.center estarán autorizados a manejar, visualizar, modificar y eliminar información almacenada en los servidores de las diferentes plataformas. Para ello, los trabajadores deberán firmar un documento de confidencialidad. La información a la que tendrán acceso estará estrictamente restringida a la que necesiten para realizar su trabajo, así como trabajos de mantenimiento, revisión, administración, soporte, comercial y verificación de la información.

Se especificarán los procesos formales y los responsables para el despliegue de medidas en caso de fallo. Se definirá un responsable para gestionar y definir los accesos de los trabajadores a la información.

Encriptación y seguridad de contraseñas

Las contraseñas de los usuarios están encriptadas mediante un método seguro y no divulgable, el cual por motivos de seguridad se omite en este documento. También se define un mecanismo de seguridad para el seguimiento de las cuentas de usuarios para analizar patrones de comportamiento inusuales y así evitar potenciales amenazas para la información, como el control automático del número máximo de peticiones en un periodo de tiempo desde una misma sesión.

Capacitación en seguridad

Se proporciona capacitación a los empleados que lo requieran sobre seguridad de la información, ética empresarial y prácticas de desarrollo seguro. Incluyendo los procedimientos para establecer los roles de seguridad y las responsabilidades del personal establecidos por BIMserver.center. Cualquier cambio se tendrá que reflejar en el documento de seguridad.

Seguridad física de los centros de datos

La seguridad física de los centros de datos donde se aloja la infraestructura de BIMserver.center es crucial para la protección contra accesos no autorizados y amenazas físicas. Esta sección aborda las medidas de seguridad implementadas para restringir el acceso físico a los servidores y garantizar la integridad de la infraestructura, incluyendo los procedimientos de seguridad adoptados en las instalaciones de OVH.

Restricción de acceso físico

El acceso a la infraestructura de hardware de BIMserver.center está estrictamente controlado. Solamente el personal autorizado puede acceder a ella y con la única finalidad de realizar trabajos de mantenimiento. El personal autorizado con acceso al hardware será conocido y estará documentado. Será necesario también firmar un documento de confidencialidad. El acceso tendrá las suficientes medidas de seguridad para impedir el posible sabotaje y garantizar un funcionamiento continuo.

Las medidas de seguridad incluyen acceso seguro bajo llave del personal autorizado y alarma conectada con empresa de seguridad, que incluye sistema de videovigilancia con grabación de imágenes para el acceso a servidores. Además, un sistema de control y monitorización de la temperatura. Adicionalmente, incluye alarma de incendio y medidas de seguridad antiincendios, como extintores adecuados en las zonas correspondientes.

Infraestructura del proveedor cloud

El acceso a la infraestructura del proveedor cloud, OVH, sigue sus propios protocolos de seguridad, garantizando la protección de las instalaciones según sus certificaciones y en cumplimientos con estándares y normas de la Unión Europea (en el siguiente enlace se puede acceder a más información: OVH Cloud - Security and Compliance).

Gestión de incidentes y recuperación ante desastres

Para asegurar la continuidad operativa y minimizar el impacto de posibles incidentes, BIMserver.center ha implementado estrategias robustas de gestión y recuperación ante desastres. En esta sección se describen los sistemas redundantes, los protocolos de actuación en caso de fallos y las políticas de copias de seguridad que garantizan la rápida recuperación del servicio ante cualquier eventualidad.

Sistemas redundantes y protocolos de recuperación

Para asegurar el funcionamiento ininterrumpido de BIMserver.center, se usan sistemas redundantes de servidores y de líneas de acceso a Internet. También se utilizan Sistemas de Alimentación Ininterrumpida (SAI) para mantener en funcionamiento los servidores en caso de interrupción del suministro eléctrico.

Estas medidas ayudan a minimizar el impacto en el servicio en caso de algún fallo en los componentes del hardware. Al tratarse de un sistema redundante de dos o más canales, en caso de fallo puntual, se asegura el funcionamiento con las mismas garantías de seguridad. En caso de avería, se reemplazarán las piezas por otros equipos cumpliendo las mismas medidas de seguridad que los originales.

Adicionalmente, se define un protocolo de actuación en caso de fallos, que garantiza una pronta recuperación del sistema en caso de caída. El protocolo indica las personas responsables que serán avisadas en caso de detección de un fallo del sistema, para reparar y recuperar el sistema lo antes posible. Se ha establecido un análisis del riesgo de los equipos y posteriormente se han establecido sistemas automáticos de detección de problemas de funcionamiento y notificación por correo electrónico o SMS a los responsables para garantizar un funcionamiento continuo y seguro.

Gestión y respuesta ante incidentes

Como método de gestión y respuesta ante incidentes, se han implementado procedimientos de respuesta rápida para incidentes de seguridad, incluyendo la identificación, contención, erradicación y recuperación.

Además, se han definido medidas automáticas de control de fallos y aviso a las personas responsables para garantizar el correcto funcionamiento. También se han establecido sistemas externos de chequeo automático desde servidores de AWS con monitorización continua del funcionamiento y avisos automáticos a los responsables por correo electrónico o SMS ante caídas o fallos del sistema. De igual modo, los sistemas se han sometido a auditorías internas.

Para la recuperación ante fallos, se establecen varios mecanismos tanto locales como de acceso remoto. Estos mecanismos se han registrado para identificar las medidas a efectuar en cada caso. Una vez finalizados los trabajos se comprueba el correcto funcionamiento y se verifica que todas las medidas de seguridad continúen activas.

Adicionalmente, todos los servidores llevan configurados firewalls estrictos, abriendo solamente los puertos imprescindibles para su funcionamiento. También se incluyen antivirus con actualización automática.

Finalmente, todas las incidencias quedan registradas como control de seguimiento para evitar futuros fallos, siendo parte del proceso de mejora continua y conocimiento acumulativo.

Copias de seguridad

Se definen protocolos de copias de seguridad de los datos y almacenamiento en lugares físicamente independientes del lugar de los datos principales. Las copias de seguridad se almacenarán de forma segura, protegida y aislada, según las certificaciones del proveedor cloud (https://www.ovhcloud.com/es-es/enterprise/certification-conformity). Al tener sistemas redundantes, las copias entre ellos tienen una frecuencia de replicación de un segundo, además de copias de seguridad externas diarias completas.

Seguridad de la API

La API de BIMserver.center permite la integración con terceros de manera segura y eficiente. Esta sección detalla los controles de acceso, los mecanismos de autorización y las medidas de seguridad implementadas para proteger la comunicación y el intercambio de datos a través de la API, lo que asegura que se cumplan los más altos estándares de seguridad.

Controles de acceso y autorización

La API de BIMserver.center garantiza la aplicación de controles de acceso estrictos y de comprobaciones de autorización sólidas para limitar las posibles brechas de seguridad. Se utiliza una autenticación diferida centralizada y segura con *Bearer Token-Autentication*. Estos controles aseguran que sus equipos validen todas las solicitudes de propiedades de objetos, lo cual contribuye a hacer frente a cualquier vulnerabilidad.

Toda la comunicación entre clientes y servidores está cifrada mediante conexión HTTPS con certificado SSL para mantener la confidencialidad de los datos. Adicionalmente, se han implementado mecanismos de control para restringir el uso de cualquier aplicación o utilidad que pueda anular los controles de seguridad del sistema.

La API de BIMserver.center implementa una política de control de acceso estructurada, con una clara definición de roles y funciones, para garantizar el acceso correcto a los usuarios adecuados, aplicando el concepto de principio de mínimo privilegio. Se incluye la gestión de cuentas, en cuanto a auditoría y a eliminación de cuentas inactivas, como también el cierre periódico de sesiones por inactividad. Las cuentas privilegiadas están estrictamente supervisadas.

Gestión de recursos y supervisión

Para cumplir y satisfacer las solicitudes realizadas por los usuarios, se implementa la limitación del consumo de recursos y se monitoriza la velocidad y el uso de recursos para

prevenir riesgos. Para ello, se realiza un seguimiento continuo del sistema por personal cualificado para detectar y registrar ataques, intrusiones o divulgaciones de información no autorizada, con el fin de prevenir agotamientos de recursos y ataques de denegación de servicio (DoS).

Validación de seguridad

La seguridad de la API se gestiona mediante la validación de entradas, la inclusión de URI en listas permitidas y la supervisión del tráfico de red saliente para ayudar a prevenir la falsificación de solicitudes del lado del servidor.

También se establece una acotación de segmentos de red entre servidores web y servidores de bases de datos de forma privada que permite proteger la confidencialidad e integridad de la información solicitada.

Se realizan auditorías internas regulares y revisiones de seguridad para identificar y abordar problemas de desconfiguración de la seguridad. Existe un inventario automatizado de API mediante Swagger y una supervisión continua por parte de un responsable para mantener la seguridad de los puntos finales.

Finalmente, se han establecido medidas de control para detectar errores o cambios no autorizados en hardware, software y firmware, realizando las correcciones necesarias a partir de fuentes oficiales.

Funcionamiento de la plataforma

Para garantizar el correcto funcionamiento y la seguridad de BIMserver.center, se han establecido protocolos operativos y medidas de control. En esta sección se explican las políticas de actualización, las pruebas de rendimiento y carga, y los procedimientos de registro y auditoría que aseguran una operación estable y segura del sistema.

Protocolos de funcionamiento

Se definen las siguientes medidas y protocolos para revisar y garantizar el correcto funcionamiento del sistema:

- Se definen los responsables de revisar y controlar que las plataformas funcionen correctamente.

- Se establecen los protocolos necesarios para que, ante la detección de un error en el funcionamiento de la plataforma, se tomen las medidas necesarias para corregirla y transmitir el problema a los responsables y desarrolladores.

- Se implementan medidas para revisar y garantizar el correcto funcionamiento de las plataformas, definiendo protocolos de actuación, de revisión y test periódicos.

- Se realizan análisis de vulnerabilidad y pruebas de penetración para prevenir el robo y garantizar la privacidad de los datos.

- Según las necesidades de los clientes, se evalúa el uso de recursos y la elasticidad de la infraestructura, recolectando y almacenando información para análisis y escalado de instancias.

- Se realizan pruebas de rendimiento y carga, revisando datos de consumo de tráfico y uso de CPU y comparándolos con los máximos teóricos para evaluar la capacidad del sistema en momentos de estrés.

Gestión de actualizaciones y parches

Las políticas de gestión de actualizaciones, parches y cambios incluyen procedimientos para aplicar parches de seguridad y cambios en la infraestructura y el software, manteniendo la estabilidad y seguridad del sistema. Se definen y publican con antelación las ventanas de mantenimiento (en horarios de bajo uso). Cualquier cambio debe ser correctamente registrado y publicado.

Registro y auditoría

Se habilitan mecanismos que aseguran el registro, la auditoría y la trazabilidad de los eventos, las operaciones, las acciones y las actividades realizadas en los sistemas e infraestructuras. Los registros se resguardan, se protegen contra manipulación, modificación o eliminación no autorizada, y están accesibles y disponibles para los usuarios (si se requieren). El personal autorizado realiza un seguimiento de los registros para asegurarse de que los eventos sean procesados adecuadamente. Finalmente, se establece un archivo de registro de incidencias para su correcto seguimiento y para la identificación de mejoras.

Aspectos legales y de privacidad

Privacidad

BIMserver.center se compromete a ser transparente sobre cómo se recopilan y utilizan los datos personales de los clientes. Para obtener más información, consulte la Declaración de Privacidad de BIMserver.center.

Términos y condiciones de uso

El uso de los servicios y plataformas de BIMserver.center está sujeto a los *Términos y condiciones de uso*, los cuales establecen las reglas y directrices para el uso adecuado de nuestros servicios. Estos términos aseguran que todos los usuarios comprendan y acepten sus responsabilidades y derechos al utilizar nuestras plataformas. Para más detalles, consulte los Términos y Condiciones de Uso de BIMserver.center.

Aviso legal

BIMserver.center proporciona información sobre las limitaciones y responsabilidades legales relacionadas con el uso de sus servicios. Este aviso incluye detalles sobre la propiedad intelectual, exenciones de responsabilidad y otros aspectos legales relevantes para los usuarios de BIMserver.center. Para más información, revise el Aviso Legal de BIMserver.center.

Conclusiones

BIMserver.center tiene un firme compromiso con la protección y seguridad de los datos de la plataforma. Desde el diseño de la infraestructura hasta las políticas operativas, cada aspecto está cuidadosamente estructurado para salvaguardar la integridad y confidencialidad de la información de sus usuarios. Esto se refleja en la implementación de medidas avanzadas de gestión de identidad, autenticación y control de acceso, asegurando que solamente los usuarios autorizados puedan acceder a los datos.

Además, BIMserver.center se compromete a cumplir con las normativas de privacidad y protección de datos, especialmente dentro del marco regulatorio europeo, asegurando que la información sensible se almacene y procese de acuerdo con las leyes aplicables. Esta postura no solamente garantiza la seguridad de los datos, sino que también establece un entorno de confianza donde los usuarios mantienen el control exclusivo sobre su información.

En términos operativos, la plataforma implementa protocolos rigurosos de gestión de incidentes y de recuperación ante desastres para mantener la continuidad operativa y minimizar el impacto de posibles interrupciones. Esto se complementa con políticas claras sobre actualizaciones de software, pruebas de rendimiento y carga, y auditorías regulares para asegurar la estabilidad y seguridad del sistema en todo momento.

A través de estas medidas y estos compromisos, BIMserver.center asegura la protección integral de datos con una estructura robusta y políticas estrictas, priorizando la confianza y control de nuestros usuarios.