

Tableau Online: Seguridad en la nube

Contenido

Seguridad operativa	4
Mantenimiento del sistema	4
Seguridad de datos y privacidad	4
Escudo de la privacidad	4
Copia de seguridad y recuperación.....	5
Recuperación ante desastres	5
Gobernanza de datos	5
Filtros de usuarios y fuentes de datos	6
Seguridad del usuario	7
Acceso y autenticación	7
Roles y permisos.....	8
Seguridad de transmisión (red)	9
Cifrado	9
Seguridad de aplicaciones	9
Arquitectura multiinquilino	10
Dashboards administrativos.....	10
Conclusión	10

Introducción

La seguridad y la privacidad de sus datos son fundamentales para el éxito de su organización. Por este motivo, protegerlas es una prioridad principal para Tableau. Este informe proporciona una descripción general de cómo funciona Tableau para garantizar la seguridad y la disponibilidad de los datos de clientes en Tableau Online.

Los datos publicados en Tableau Online están protegidos por funcionalidades de seguridad de nivel empresarial que incluyen:

- Seguridad física
- Seguridad operativa
- Seguridad de datos y privacidad
- Seguridad de cuentas
- Seguridad de datos en tránsito
- Seguridad de aplicaciones

Detrás de todo esto, hay una infraestructura continuamente supervisada con el fin de garantizar su disponibilidad, rendimiento, capacidad y seguridad. El resultado de esta supervisión se utiliza para impulsar mejoras regulares que contribuyan a garantizar la confidencialidad, la integridad y la disponibilidad de sus datos.

Tableau implementó un modelo de seguridad de múltiples capas diseñado para proporcionar una protección eficaz contra una amplia variedad de amenazas conocidas y de día cero. Como parte del protocolo de respuesta ante incidencias de Tableau, las brechas de seguridad se notificarán por medio del sitio web de Trust (<https://trust.tableausoftware.com>) o directamente a los clientes afectados. Los informes de incidencias incluirán el alcance, la gravedad y la resolución.

Tableau se esfuerza continuamente por mantener un servicio hospedado seguro y de primer nivel. Así, puede tener la confianza de que sus datos están protegidos.

Seguridad operativa

SOC 2 e ISAE 3402

Cada año, Tableau trabaja con una empresa de contabilidad pública certificada independiente para realizar una auditoría detallada de los objetivos y las actividades de control de Tableau Online. Tableau se enorgullece en anunciar que los procedimientos de control para el servicio de Tableau Online se han verificado en un informe SOC 2 de tipo II que se preparó según los términos de la Declaración de Normas de Compromisos de Certificación n.º 16 (SSAE 16) y la Norma Internacional de Compromisos de Certificación (ISAE) n.º 3402. El informe SOC 2 de tipo II de Tableau Online se encuentra disponible a pedido.

Centros de datos

Los servicios de Tableau Online están hospedados en centros de datos de clase empresarial auditados de manera independiente. Estos centros incorporan redundancia en todos los servicios fundamentales. Los centros de datos están equipados con extinción de incendios y otros sistemas de supervisión diseñados para detectar problemas del entorno y responder a estos antes de que causen una interrupción. Además, los proveedores de hospedaje mantienen contratos con otros proveedores para garantizar que pueden seguir adelante con las operaciones en caso de que haya una interrupción sostenida en el suministro eléctrico.

Tras la celebración de un acuerdo de no divulgación, Tableau puede compartir los informes de auditoría para sus proveedores de centros de datos a pedido. Para obtener más información, comuníquese con su representante de cuenta de Tableau.

Mantenimiento del sistema

El equipo responsable del mantenimiento de la infraestructura de Tableau Online realiza un mantenimiento regular para garantizar la estabilidad, la seguridad y el rendimiento del sistema. Las ventanas de mantenimiento programado se publican en el sitio de Tableau Trust con un mínimo de dos días de antelación. Los administradores de sitios reciben también notificaciones por correo electrónico acerca de la próxima tarea; además, los usuarios ven una notificación al iniciar sesión en el sitio de Tableau Online.

Seguridad de datos y privacidad

Escudo de la privacidad

En relación con los datos personales de residentes del Espacio Económico Europeo (EEA), Tableau es un **Participante activo** certificado en el **Marco del Escudo de la privacidad** y está sujeto a las facultades de investigación y de control de la Comisión Federal de Comercio (Federal Trade Commission).

Copia de seguridad y recuperación

Las copias de seguridad se componen de todos los elementos fundamentales. Los soportes de las copias de seguridad están cifrados y siempre se mantienen en instalaciones protegidas. Las copias de seguridad basadas en disco se almacenan en instalaciones de centros de datos protegidas. Las copias de seguridad que se realizan para proveedores de copias de seguridad externos se cifran en las etapas de tránsito y almacenamiento. Solo los administradores de sistemas autorizados tienen acceso a las copias de seguridad.

De acuerdo con la política de copias de seguridad de Tableau Online, las copias de seguridad diarias se conservan durante 31 días.

Estas copias de seguridad permiten a Tableau restaurar todo el sistema de Tableau Online. Las copias de seguridad no permiten actualmente la restauración de un único sitio de cliente. Esto significa que Tableau no puede restaurar datos o libros de trabajo de clientes individuales que se hayan perdido a causa de incidentes que no fueran errores del sistema.

Recuperación ante desastres

Para cada instancia del servicio de Tableau Online, Tableau mantiene centros de datos principales y de respaldo en ubicaciones geográficamente diversas. Si un centro de datos principal no se encuentra disponible, los sistemas se instalan en el sitio de respaldo. Este último se reconfigura para administrar el tráfico de producción. Después, los datos se restauran a partir de la copia de seguridad más reciente.

Debido a que Tableau Online es una aplicación de solo lectura y a que, por lo general, los datos los proporcionan fuentes de datos administradas por clientes, se pueden volver a publicar visualizaciones tomando la información directamente de la fuente en lugar de tener que restaurar a partir de una copia de seguridad. Esto permite reducir enormemente el objetivo de punto de recuperación.

Gobernanza de datos

Sus datos son suyos, aunque se almacenen en Tableau Online. Solo las personas que usted autoriza tienen acceso a los datos o libros de trabajo almacenados en su sitio. Los empleados y otros clientes de Tableau no tienen acceso a sus datos. La única excepción es un número reducido y controlado de administradores confiables de Tableau. Estos son responsables de administrar los sistemas que ejecutan el servicio. Existe un proceso documentado para autorizar a los usuarios a este nivel de acceso. Además, todo el acceso de nivel administrativo se revisa y aprueba trimestralmente.

Tenga en cuenta que la mayor parte de sus datos permanece almacenada de manera segura en sus propias fuentes de datos. Solo los libros de trabajo, las extracciones de datos y los datos en caché se almacenan en Tableau Online.

Tableau tiene acceso a métricas que se relacionan con la utilización del sistema, el estado de la cuenta y el rendimiento. Además, puede supervisarlas. Dichas métricas incluyen, entre otros:

- Almacenamiento total utilizado por cuenta y por usuario
- Ancho de banda total utilizado por cuenta y por usuario
- Número total de libros de trabajo y vistas por cuenta y por usuario
- Fechas y horas de acceso por usuario (inicios de sesión)
- Número y tipo de fuentes de datos (por ejemplo, SQL Server, Salesforce.com) por cuenta y por usuario
- Fechas y horas de actualizaciones de datos por cuenta y por usuario
- Métricas de rendimiento de sitios

Los datos se introducen en Tableau Online de una de estas cuatro maneras:

1. Publicando un libro de trabajo con los datos incorporados en él.
2. Tomando datos de una fuente local y colocándolos en una extracción de datos de Tableau. Este método siempre genera una extracción de datos, no una conexión en tiempo real. Por este motivo, no hay necesidad de crear una red privada virtual (VPN) ni una vía segura a su entorno corporativo. Para las fuentes de datos a las que Tableau Online no puede llegar directamente, puede publicar extracciones de datos y usar el cliente de sincronización de Tableau Online para programar actualizaciones automáticas.
3. Conectándose a un servicio web por medio de una interfaz de programación de aplicaciones (API). Para la mayoría de las fuentes de datos en la nube, como Salesforce.com o Google Analytics, se utiliza la conexión de API para generar extracciones de datos que puedan programarse para actualizarse regularmente.
4. Por medio de una conexión directa a datos hospedados en una plataforma en la nube. Para estas **fuentes de datos**, Tableau Online puede crear una conexión en tiempo real o una conexión basada en extracciones.

Filtros de usuarios y fuentes de datos

Puede definir una medida de seguridad adicional en sus libros de trabajo y fuentes de datos agregando filtros de usuarios y fuentes de datos. El filtro de usuarios es un tipo de filtro especial que le permite limitar los datos que una persona determinada puede ver en una vista publicada. Por ejemplo, en un informe de ventas que se comparte con administradores regionales, puede querer permitir que solo el administrador regional de la zona oeste vea las ventas de la zona oeste, el administrador regional de la zona este vea las ventas de la zona este, y así sucesivamente. En lugar de crear una vista separada para cada administrador, puede definir un filtro de usuarios que permita que cada administrador vea los datos de una región en particular.

Los filtros de usuarios se definen para campos individuales. Los usuarios o grupos obtienen permiso para ver un subconjunto de los miembros de ese campo. En el ejemplo del informe de ventas anterior, el filtro de usuarios se define para el campo Región, con lo que cada administrador obtiene permiso para ver una determinada región.

Los filtros de fuentes de datos funcionan de manera similar a los filtros de usuarios. Permiten configurar un filtro en una fuente de datos publicada que se aplicará globalmente. Los filtros de fuentes de datos pueden ser útiles para restringir los datos que pueden ver los usuarios cuando publica un libro de trabajo o una fuente de datos. Cuando publica una fuente de datos en Tableau Online, esta y las extracciones o los archivos asociados se transfieren en su totalidad al servidor. Cuando publica una fuente de datos, puede definir permisos de acceso para descargar o modificar la fuente de datos. También puede elegir los usuarios y grupos que pueden emitir consultas a esa fuente de datos remotamente a través de Tableau Online. Cuando los usuarios tienen permiso de consulta pero no de descarga, puede compartir un modelo de datos enriquecido que tenga campos calculados, alias, grupos y conjuntos, entre otros, solo para consulta.

Además, los usuarios que consultan esta fuente de datos nunca podrán ver ni modificar los filtros de fuentes de datos presentes en la fuente de datos publicada originalmente. Sin embargo, todas las consultas de los usuarios estarán sujetas a esos filtros de fuentes de datos. Se trata de una excelente forma de ofrecer acceso a un subconjunto restringido de sus datos.

Seguridad del usuario

Acceso y autenticación

Solo los usuarios que usted agregue explícitamente a su sitio tendrán acceso a su contenido y sus libros de trabajo. Los administradores que usted designe serán responsables de todas las funciones de administración de cuentas, incluidas la de agregar y quitar usuarios y la de asignar permisos. La administración de cuentas está completamente bajo su control. Si un usuario ya no cuenta con autorización en su sitio, simplemente quítelo y ya no tendrá acceso al contenido almacenado en Tableau Online.

Hay dos métodos de autenticación disponibles dentro de Tableau Online. Usted dispone de la flexibilidad de configurar su sitio para que use uno de ellos o ambos.

1. Cuenta de Tableau

Las cuentas de Tableau se utilizan de manera predeterminada y están protegidas en un almacén de identidades mantenido por Tableau. Este método de autenticación proporciona a los administradores de sitios la capacidad para configurar rápidamente a los usuarios sin la necesidad de integrarse con un proveedor de identidades independiente. Las cuentas son administradas por los clientes y permiten la autenticación segura a Tableau Online. También se utilizan para acceder a otros servicios y recursos de Tableau, como el sitio web de Tableau, el portal del cliente/de socios de Tableau y los foros de Tableau.

Los usuarios se autentican utilizando su dirección de correo electrónico como nombre de usuario y una contraseña seleccionada por el usuario. Cuando los administradores agregan usuarios a su sitio, estos últimos reciben un correo electrónico con instrucciones sobre cómo configurar la contraseña. Los administradores no configuran las contraseñas de usuarios ni pueden recuperar las contraseñas almacenadas. Las contraseñas se cifran y aleatorizan mediante un sólido algoritmo de hash.

Las cuentas se bloquean durante un período de 10 minutos después de 10 intentos fallidos. El tiempo de bloqueo se duplica con cada intento fallido sucesivo. Un usuario no puede tener más de cinco sesiones abiertas al mismo tiempo. Cada sesión tiene un tiempo de espera de ocho horas.

Las contraseñas deben tener un mínimo de ocho caracteres de longitud y deben incluir letras y números.

2. SAML

SAML permite a los administradores configurar su sitio con inicio de sesión único utilizando su propio proveedor de identidades (IdP) compatible con SAML 2.0. Para obtener más información, consulte la sección de autenticación de sitio de la [Guía de productos en línea](#).

Nota: Las funcionalidades relacionadas con SAML y el inicio de sesión único actualmente solo están disponibles a pedido. Para solicitar estas funcionalidades, comuníquese con Soporte de Tableau.

Tableau Online implementa un tiempo de espera de sesión que expira después de dos horas de inactividad.

Roles y permisos

El acceso dentro de Tableau Online se controla a través de una combinación de roles y permisos de sitios. Cada usuario que se agrega a Tableau Online debe tener un rol de sitio asociado. El rol de sitio lo asigna el administrador y determina los niveles de permisos que se otorgan a un usuario, incluido si el usuario puede publicar, interactuar o solo ver el contenido que se publica en Tableau Online. Si desea conocer más detalles acerca de los roles de sitios, [haga clic aquí](#). Los permisos se asignan al contenido (proyectos, libros de trabajo, vistas y fuentes de datos) y también pueden asignarse a usuarios individuales o grupos. Al especificar permisos, se utilizan reglas para especificar quién tiene permitido trabajar con determinado contenido.

Los permisos pueden usarse para otorgar permisos como crear, ver, modificar o eliminar. Los permisos asignados a un proyecto controlan el nivel de acceso predeterminado a todos los libros de trabajo y todas las vistas que se publican en dicho proyecto. Los administradores pueden crear grupos como “Usuarios de finanzas” para facilitar la administración de permisos.



La ventana de permisos

Hay más de 20 personalizaciones con parámetros disponibles que administrar la seguridad de objetos. Para obtener más información, consulte la sección [Administrar permisos](#) en la documentación en línea.

Seguridad de transmisión (red)

Cifrado

Toda la comunicación entre el cliente (Tableau Desktop o un navegador compatible) y Tableau Online se cifra por medio de TLS. Este sistema proporciona protección de los datos en tránsito.

Las conexiones a fuentes de datos pueden cifrarse o no en función de las funcionalidades de cifrado de la fuente de datos. Los clientes deben conocer las opciones de cifrado disponibles para las fuentes de datos que planean usar.

Además, los productos de Tableau poseen numerosos mecanismos de seguridad incorporados que ayudan a evitar la suplantación, la interceptación y la inyección de código SQL. Tableau también prueba activamente sus productos para detectar vulnerabilidades y responde a nuevas amenazas con actualizaciones periódicas.

Tenga en cuenta que las funcionalidades que utilizan correo electrónico, como la suscripción, utilizan correos electrónicos enviados a través de SMTP. Este protocolo, de manera estándar, no está cifrado.

Seguridad de aplicaciones

La seguridad de aplicaciones es una combinación de prácticas de diseño seguras que incluyen la definición de requisitos de seguridad, el modelado de amenazas, las revisiones de código y pruebas de seguridad. Las pruebas de vulnerabilidad, automatizadas y manuales, se realizan como parte del proceso de desarrollo. En ellas se emplean empresas de seguridad de terceros para llevar a cabo las pruebas de penetración de aplicaciones antes de los grandes lanzamientos.

Tableau se compromete a trabajar con terceros expertos en seguridad para probar, descubrir, validar y abordar los problemas de seguridad.

Además, Tableau implementó un servicio de detección de vulnerabilidades de terceros que analiza continuamente los recursos y servicios de Internet de la empresa, incluido Tableau Online, para encontrar vulnerabilidades. Cualquier descubrimiento genera una alerta que se evalúa para determinar la gravedad y el impacto. La prioridad de los esfuerzos de corrección que se requieran se basa en esta evaluación.

Arquitectura multiinquilino

Tableau Online es una solución multiinquilino. No proporciona entornos dedicados para cada cliente. La aplicación implementa la segregación entre clientes particionando lógicamente los usuarios, los datos y los metadatos por sitio. Todos los datos cargados en el servicio o vinculados con este se conectan programáticamente con el cliente propietario de los datos. Estos controles garantizan que un cliente no pueda acceder a los datos de otro cliente.

Dashboards administrativos

Tableau Online publica un conjunto predeterminado de dashboards que proporcionan estadísticas de uso para su sitio. Entre los detalles disponibles se encuentran la actividad del usuario, los recuentos de vistas y el uso de la fuente de datos. Los administradores pueden usar estos dashboards predeterminados para conocer cómo se está utilizando su sitio.

Para obtener información acerca de cómo se usan estos dashboards, consulte la sección [Vistas administrativas](#) de la guía de productos en línea.

Conclusión

El servicio de Tableau Online está diseñado y se ejecuta sobre la base de un modelo de seguridad sólido, respaldado por prácticas recomendadas del sector y validado por terceros expertos en seguridad. Tableau es consciente de la importancia que tienen sus datos y asume la responsabilidad de protegerlos muy seriamente.

Acerca de Tableau

Tableau ayuda a las personas a transformar los datos en información útil para generar un impacto positivo. Conéctese con facilidad a datos almacenados en cualquier formato y lugar. Haga, rápidamente, análisis ad hoc que revelen oportunidades ocultas. Arrastre y suelte para crear dashboards interactivos con análisis visuales avanzados. Después, compártalos con toda su organización y permita que sus compañeros de equipo exploren los datos por sí mismos. Multinacionales, empresas pequeñas y emergentes... Todo el mundo usa la plataforma de análisis de Tableau para ver y comprender sus datos.

Recursos

[Descargar versión de prueba gratuita](#)

[¿Por qué análisis de negocios en la nube?](#)

[5 prácticas recomendadas para crear dashboards de campaña eficaces \(en inglés\)](#)

[Ver todos los informes](#)

