INFORME

Seguridad y privacidad de Asana

Cómo Asana protege tus datos

Índice

Última actualización: octubre de 2022[1]

[1] En este informe se describe el estado actual de la seguridad de Asana, que puede modificarse en el futuro con los nuevos lanzamientos de características y productos.

Introducción

Los clientes confían sus datos a Asana para poder centrarse en el trabajo realmente importante para sus negocios. Por eso, no solo nos enfocamos en crear una solución de gestión del trabajo colaborativa y fácil de usar, sino que, además, garantizamos que los datos de nuestros clientes estén seguros.

En este informe, aprenderás cómo Asana prioriza la seguridad, la disponibilidad y la confidencialidad en todo esto:

- Infraestructura
- Producto
- Entorno operativo y físico
- Privacidad, certificaciones y cumplimiento normativo

A pesar de que la mayor parte de este informe se puede aplicar a cualquier tipo de plan de Asana, está escrito en el contexto de los siguientes planes de Asana: Premium, Business y Enterprise.[2] En el caso de que las funciones no se encuentren disponibles para todos los planes, se especificará.

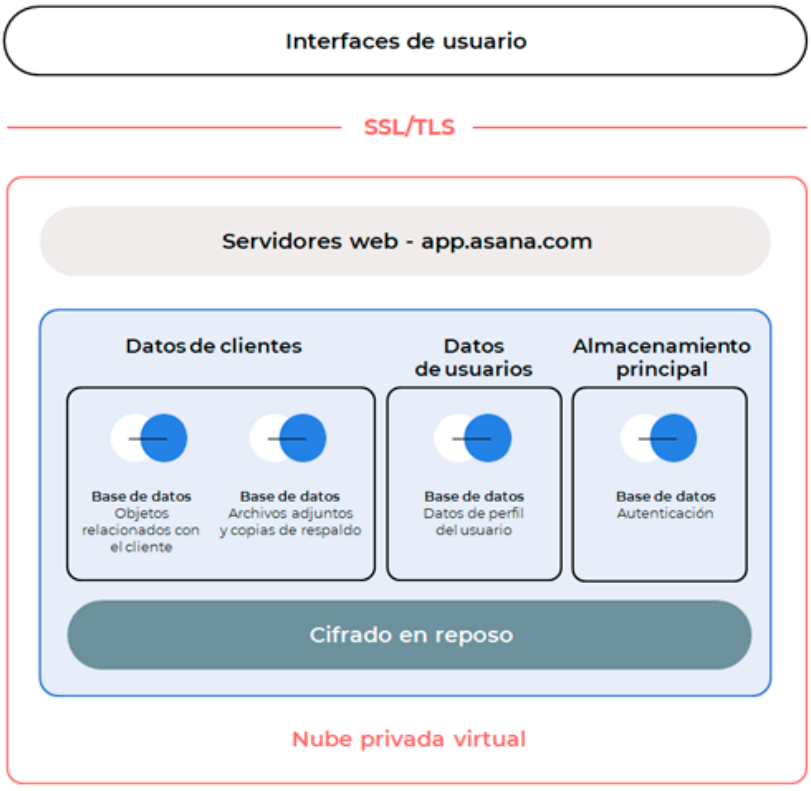
[2] Para obtener más información sobre los planes de Asana, consulta asana.com/es/pricing.

Infraestructura

Asana usa ofertas de servicios informáticos en la nube, principalmente de Amazon Web Services (AWS), como base fundamental de la plataforma de Asana.

AWS gestiona la seguridad y conformidad normativa de la infraestructura informática de la nube, y Asana gestiona la seguridad y conformidad normativa del software y de los datos que se guardan en la infraestructura informática de la nube. Consulta el modelo de responsabilidad compartida de AWS.[3]

Asana usa la red virtual privada en la nube (VPC) de Amazon y ha diseñado una arquitectura de red segura, escalable y fácil de gestionar con los servicios de red y las bases fundamentales que ofrece AWS. La mayor parte de la plataforma de Asana funciona con los servicios de *Elastic Compute Cloud* (EC2) de Amazon, una solución confiable, fácil de adaptar y segura para procesar los datos de los clientes. A continuación, puedes ver un diagrama simplificado de la infraestructura de Asana.



[3] http://aws.amazon.com/es/compliance/shared-responsibility-model

Nuestra infraestructura de producción está protegida para que solo nuestras máquinas de balanceo de cargas puedan recibir tráfico web externo. A cada huésped se le asigna un rol y los grupos de seguridad se utilizan para definir el tráfico esperado entre estos roles.

Servidores web

La capacidad segura, confiable y basada en la nube de Amazon EC2 constituye la mayor parte de nuestro entorno de servidores web. Los servidores web procesan los datos de los clientes y brindan las funcionalidades de la aplicación a nuestros usuarios, mientras interactúan con otras partes de nuestra infraestructura.

Bases de datos

Las bases de datos son Relational Database Service (RDS) de Amazon, que ejecuta una base de datos MySQL administrada.

Almacenamiento principal

Almacena datos como contraseñas cifradas (sal y *hash* de contraseñas, *bcrypt*) e información de autenticación para los diferentes usuarios. También almacena otros metadatos que permiten el enrutamiento del tráfico.

Datos de clientes

Almacena toda la información que los clientes completan o cargan en Asana, incluidos los proyectos y las tareas.

Datos de usuarios

Almacena información relacionada con los perfiles de usuarios, como los nombres y las direcciones de email.

Almacenamiento de archivos

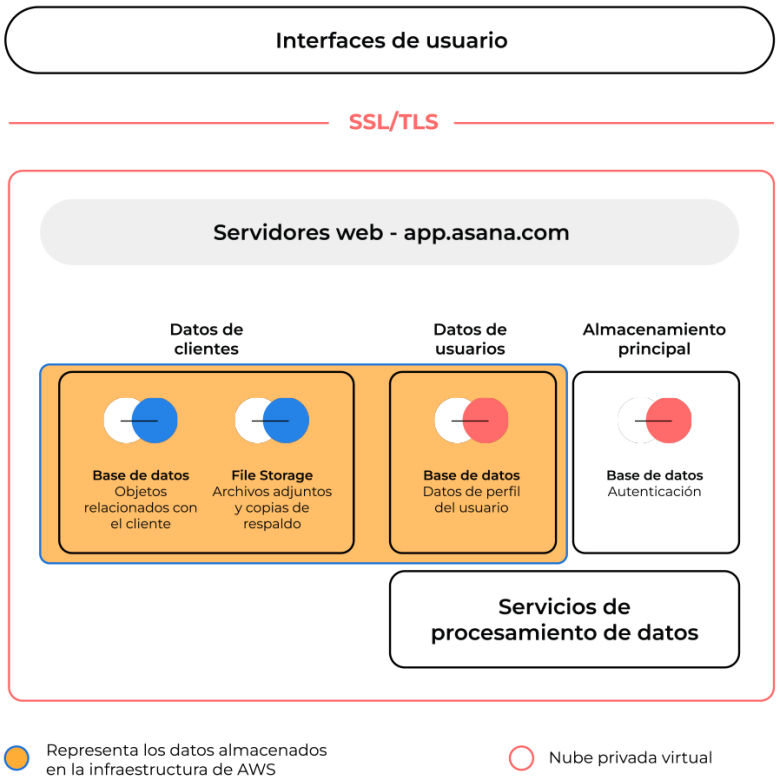
Los servidores de almacenamiento son Simple Storage Service (S3) de Amazon. Almacenan archivos adjuntos y copias de respaldo de las bases de datos. Los archivos adjuntos pueden ser cualquier archivo que se haya cargado a una tarea de Asana directamente desde una computadora. Los que provienen de plataformas de colaboración para contenido alojadas en la nube se crean como enlaces a esas plataformas, pero no se guardan en los servidores de almacenamiento de Asana.

Ubicaciones de los centros de datos

Asana ofrece centros de datos de AWS en múltiples ubicaciones a los clientes de Asana Enterprise que necesitan que sus datos se almacenen en una ubicación específica:

- Infraestructura de Europa: los datos del cliente y la mayoría de los datos de los usuarios se almacenarán en AWS de Frankfurt (Alemania), con copias de seguridad en AWS de Dublín (Irlanda).
- Infraestructura de Australia: los datos del cliente y la mayoría de los datos de los usuarios se almacenarán en AWS de Sídney (Australia), con copias de seguridad en AWS de Dublín (Irlanda).
- Infraestructura de Japón: los datos del cliente y la mayoría de los datos de los usuarios se almacenarán en AWS de Tokio (Japón), con copias de seguridad en AWS de Osaka (Japón).

Este es un diagrama simplificado de la infraestructura de Asana para los clientes que solicitan residencia de datos.



Seguridad de los datos

Cifrado

Las conexiones a app.asana.com están cifradas con encriptación de 128 bits y son compatibles con TLS 1.2 y versiones posteriores. Las conexiones se cifran y autentican con AES_128_GCM y se usa ECDHE_RSA como mecanismo de intercambio de claves. Asana es compatible con la confidencialidad directa y AES-GCM, y prohíbe las conexiones inseguras con RC4 o TLS 1.1 y versiones anteriores. Los inicios de sesión y las transferencias de datos confidenciales se realizan solo a través de TLS. Asana garantiza el cifrado en reposo con claves secretas AES de 256 bits.[4]

Gestión de claves para empresas

Asana ofrece a ciertos clientes Enterprise la opción de usar sus propias claves de cifrado para encriptar sus datos de Asana. Los clientes pueden usar el Servicio de administración de claves (KMS) de Amazon Web Services (AWS) para sus claves de cifrado. Los clientes que usan la gestión de claves para empresas (EKM) con Asana controlan las claves de cifrado para la base de datos del dominio, los archivos adjuntos, la búsqueda y la mayoría de los datos de los usuarios en la organización. Para obtener más información y configurar la gestión de claves para empresas en Asana, envía un email al equipo de ventas a sales@asana.com.

[4] Para obtener más información sobre qué datos están cifrados en Asana, consulta el diagrama en la página 6.

Solución multiinquilino

Asana es una aplicación web multiinquilino, lo que significa que la infraestructura se comparte entre las instancias de los clientes. La autenticación de cuentas, la separación de campos de bases de datos lógicas y los controles de gestión de sesiones se implementan para limitar el acceso de los clientes a los datos asociados con su organización.

Escalabilidad y confiabilidad

Asana utiliza Amazon Web Services, lo que garantiza la escalabilidad del servicio. Las bases de datos se replican sincrónicamente para que podamos recuperarnos rápidamente ante una falla en la base de datos. Como precaución adicional, tomamos instantáneas periódicamente de la base de datos y las enviamos de forma segura a un centro de datos de respaldo para poder restaurar el acceso de los clientes, incluso en caso de una falla en la región principal de AWS.

Nivel de disponibilidad del sistema

Asana se compromete a ofrecer un tiempo de disponibilidad del servicio del 99.9 % a los clientes Enterprise. Los clientes pueden ver y suscribirse a las actualizaciones de estado del sistema en status.asana.com. Allí se comparte la disponibilidad de la aplicación web, la aplicación móvil y la API durante las últimas 12 horas, 7 días, 30 días y 1 año.

Copias de respaldo

Las instantáneas de la base de datos se toman diariamente. Las copias de seguridad cuentan con la misma protección que las bases de datos de producción. Garantizamos el almacenamiento entre regiones de las copias de seguridad.

Funciones de seguridad del producto

Asana proporciona a los usuarios y administradores las funciones necesarias para proteger sus datos. Estas funciones brindan un control administrativo completo y visibilidad de los datos del cliente. La disponibilidad de las siguientes funciones varía según el plan de Asana. Consulta los planes en asana.com/es/pricing.

Administradores

Los administradores pueden gestionar equipos al agregar miembros e invitados y anular su acceso a medida que se incorporan o abandonan la empresa o el flujo de trabajo. También pueden usar nuestra API de administración para gestionar las exportaciones de dominios, las configuraciones, los permisos, las aplicaciones de terceros y la configuración de equipos y usuarios.

Concesión y anulación de acceso a usuarios

Asana permite que los usuarios y administradores controlen quién tiene acceso a sus propios datos.

- Los usuarios y administradores pueden invitar a miembros e invitados (miembros externos) a sus organizaciones y equipos.
- Los administradores pueden eliminar a cualquier miembro o invitado de la consola del administrador.

Además, los clientes Enterprise pueden integrar Asana con su proveedor de identidades (IdP) en la nube a través del estándar del sistema de gestión de identidades entre dominios (SCIM) para aprovisionar y anular el aprovisionamiento de usuarios junto con el resto de sus soluciones SaaS.[5]

Seguridad de inicio de sesión

Los administradores de Asana pueden decidir qué mecanismo usarán los usuarios para iniciar sesión en sus cuentas de Asana. Hay tres opciones diferentes: credenciales de Asana, inicio de sesión único de Google o inicio de sesión único con SAML 2.0.

Medidas de seguridad de las contraseñas

Si se permite que los usuarios inicien sesión en sus cuentas con las credenciales de Asana, los administradores pueden especificar qué nivel de seguridad se requiere para las contraseñas. Al solicitar contraseñas "fuertes" se obliga a los usuarios a usar al menos 8 caracteres e incluir tres de las siguientes opciones: minúsculas, mayúsculas, números y caracteres especiales. Las contraseñas personalizadas permiten a los administradores determinar la complejidad de los requisitos para las contraseñas en su dominio.[6] Los administradores también pueden establecer el restablecimiento de las contraseñas para todos los usuarios de la organización.

Autenticación de dos factores (2FA)

Los administradores de los planes Enterprise pueden requerir la autenticación de dos factores para los inicios de sesión de Asana.[7]

Inicio de sesión único de Google (SSO)

Los administradores pueden solicitar a los usuarios de la organización que inicien sesión en Asana con su cuenta de Google Workspace (anteriormente, G Suite).

[5] https://asana.com/es/guide/help/premium/scim
[6] https://asana.com/es/guide/help/premium/authentication#gl-force
[7] https://asana.com/es/guide/help/premium/admin-console-mandatory-2fa

Inicio de sesión único con SAML

Los administradores Enterprise pueden configurar su proveedor de identidades y solicitar a los usuarios que inicien sesión en Asana con las credenciales de su cuenta de IdP en la nube. Esto se configura a través del estándar de autenticación SAML. Los administradores Enterprise pueden establecer la duración del tiempo de espera de SAML desde la consola del administrador en Asana.

API de registros de auditoría

La API de registros de auditoría de Asana permite a los administradores Enterprise detectar amenazas de seguridad en Asana a través de Splunk, Panther o cualquier proveedor de gestión de eventos e información de seguridad (SIEM) de su elección que se pueda integrar en Asana. Con nuestra integración lista para usar de Splunk y Panther, los equipos de TI pueden ver y monitorear actividades clave relacionadas con el cumplimiento en Asana directamente desde el panel de Splunk. Además, los administradores pueden proteger de forma proactiva los datos de su organización y tomar medidas cuando se producen actividades sospechosas al implementar alertas personalizadas oportunamente.[8]

Administración de espacios de trabajo aprobados

La función para administrar espacios de trabajo aprobados de Asana permite a los administradores Enterprise restringir el uso de Asana a un conjunto de espacios de trabajo aprobados en un dispositivo o red administrados. Esta característica también está disponible a través de una asociación con Netskope.

Permisos de acceso

Los administradores y usuarios pueden invitar a otros usuarios a acceder a sus datos. Al invitar usuarios a unirse a una organización, se les puede asignar diferentes privilegios. Es posible invitar usuarios en el nivel del objeto (tarea, proyecto, equipo u organización) con diferentes tipos de acceso. Los permisos se definen para el usuario en el nivel del objeto en lugar de asignarse en el nivel del usuario. Un mismo usuario puede tener acceso solo para comentar en algún contenido, contenido completamente oculto para él, contenido “disponible a pedido” y contenido con acceso completo para ver y modificar. Puedes consultar la información específica sobre cada objeto y tipo de permiso en la Guía de Asana: asana.com/es/guide.

[8] https://asana.com/es/guide/help/api/audit-log-api

Objetos de Asana

Tareas

Las tareas en Asana pueden ser privadas o públicas y estar incluidas en un proyecto privado o uno público.

Tarea:	Con acceso para:
Tarea privada	Solo el colaborador de la tarea
Tarea pública	Todos los miembros de la organización
Tarea en un proyecto privado	Colaborador de la tarea y miembros del proyecto
Tarea en un proyecto público	Colaborador de la tarea, miembros del proyecto y miembros del equipo
Subtarea	Colaborador de la tarea y quienes tienen acceso a la tarea madre

Proyectos

Los proyectos en Asana pueden ser privados o públicos. Si un usuario tiene acceso a un proyecto, entonces tiene el mismo acceso a todas las tareas y conversaciones dentro de ese proyecto. Los usuarios se pueden agregar a un proyecto con acceso de edición o solo para comentar. Los administradores Enterprise pueden establecer un nivel de privacidad predeterminado para los equipos en su organización.

Proyecto:	Con acceso para:
Proyecto privado	Miembros del proyecto
Proyecto público	Miembros del equipo y del proyecto
Proyecto público en un equipo público	Miembros de la organización, del equipo y del proyecto

Equipos

Los equipos en Asana pueden ser ocultos, públicos o de membresía por solicitud. Si un usuario pertenece a un equipo, entonces tiene acceso a todas las conversaciones del equipo y los proyectos públicos dentro de ese equipo.

Equipo:	Con acceso para:	Pueden unirse:
Oculto	Miembros del equipo	No
Público para la organización	Miembros del equipo y la organización	Sí
Membresía por solicitud	Miembros del equipo	Después de la aprobación

Organizaciones

Las organizaciones en Asana son los objetos en el nivel más alto que incluyen equipos, proyectos y tareas.

Usuarios

Los usuarios en Asana tienen sus cuentas individuales vinculadas a sus direcciones de email. A esa cuenta se le puede otorgar acceso a diferentes objetos de datos como se mencionó anteriormente. Además, de forma predeterminada, las cuentas de usuario tienen acceso a una organización en función de su dominio de email.

Miembros con acceso completo

La membresía de una organización se basa en el dominio asociado a una dirección de email. Para ser miembro en una organización, debes tener una dirección de email asociada a uno de los dominios de email aprobados por la organización.

Los miembros de una organización pueden:

- Crear equipos nuevos
- Ver una lista completa de los equipos a los que pueden solicitar unirse dentro de la organización
- Ver nombres y direcciones de email de otros miembros e invitados en la organización
- Acceder a proyectos y tareas públicos de la organización

Invitados

Puedes colaborar con clientes, contratistas y cualquier otra persona que no tenga una dirección de email con un dominio aprobado por tu organización. Estos usuarios serán invitados de la organización. Los invitados tienen acceso limitado en la organización y solo pueden ver lo que se comparte explícitamente con ellos.

Un invitado de la organización solo puede unirse a equipos con una invitación. No pueden crear, ver ni enviar una solicitud para unirse a ningún equipo adicional.

Miembros con acceso limitado

Cada equipo tiene sus propios miembros y proyectos. Aquellas personas que no tengan acceso a todos los proyectos dentro del equipo se mostrarán como *miembros con acceso a proyectos específicos* en la pestaña de miembros de la configuración del equipo.

Los *miembros con acceso a proyectos específicos* pueden ver proyectos y tareas en los que fueron agregados, pero no conversaciones u otros proyectos del equipo.

Gestión de invitados

Los administradores con planes Enterprise pueden decidir quién tiene la posibilidad de agregar miembros externos (invitados). Los administradores pueden seleccionar una de las siguientes tres opciones para decidir quién tiene la capacidad de invitar personas a la organización:

- Solamente los administradores
- Administradores y miembros de la organización
- Todos (incluidos los miembros y los invitados de la organización)

Gestión de administración de aplicaciones

Los administradores con planes Asana Enterprise pueden decidir qué integraciones de terceros pueden usar los usuarios con sus cuentas de Asana y bloquear cualquier integración no deseada. Visita asana.com/es/apps para saber qué aplicaciones de terceros están disponibles.[9]

Control de datos

Los clientes pueden exportar o eliminar datos de Asana y automatizar exportaciones de dominio completo a través de nuestra API.

[9] https://asana.com/es/guide/help/premium/app-management

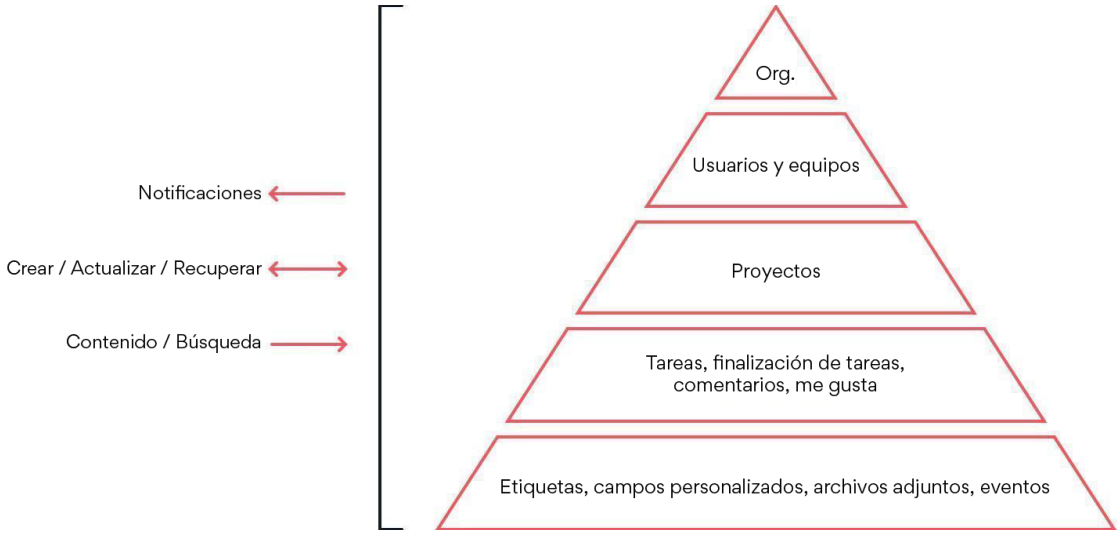
Plataforma de Asana

Integraciones

Asana permite que los usuarios accedan a sus cuentas mediante la interfaz de programación de aplicaciones (API)[10]. La API de Asana es una interfaz RESTful que te permite actualizar y acceder a gran parte de tus datos en la plataforma mediante programación y también reacciona automáticamente cuando hay cambios. Proporciona URL predecibles para acceder a los recursos y usa funciones incorporadas de HTTP para recibir comandos y generar respuestas. Esto facilita la comunicación con Asana desde una amplia variedad de entornos, desde utilidades de línea de comandos hasta complementos de navegador para aplicaciones nativas. Los clientes pueden usar estas API para crear soluciones personalizadas o para integrar otro software. Asana es compatible con OAuth 2.0 o con el token de acceso personal como método de autenticación con la API.

Para obtener más información sobre la API de Asana, visita asana.com/es/developers.

La ilustración a continuación muestra un resumen de las acciones que se pueden realizar y de los objetos con los que se puede trabajar.



De forma predeterminada, cualquier software o script tendrá los mismos permisos que el usuario que lo ejecuta. Los datos para trabajar se limitan a los datos a los que el usuario tiene acceso. Cuando se requiere acceso adicional, los clientes Enterprise pueden usar cuentas de servicios.

Cuentas de servicio

Los clientes de Asana Enterprise pueden usar cuentas de servicio para acceder a todo su contenido. Por ejemplo, las cuentas de servicio se pueden usar para realizar una exportación completa de datos de la organización o para monitorear la actividad del equipo. Puedes encontrar más información en la Guía de Asana[11].

[10] https://asana.com/es/guide/help/api/api
[11] https://asana.com/es/guide/help/premium/service-accounts

Aplicaciones de terceros

Con la API de Asana es posible implementar cientos de integraciones listas para usar, que los clientes pueden aprovechar para mejorar o complementar su experiencia con Asana. Asana se integra con muchas herramientas para optimizar los flujos de trabajo de los clientes y aumentar la productividad. Es posible integrar herramientas de terceros de otros proveedores. Las funciones de estas herramientas de terceros incluyen las siguientes:

- Sincronización de mensajes entre aplicaciones
- Automatización del flujo de trabajo
- Extensiones de plataformas
- Desarrollo de software
- Importación de datos
- Uso compartido de archivos
- Informes
- Seguimiento del tiempo
- Ingesta de datos

Puedes encontrar un directorio de aplicaciones de terceros en asana.com/es/apps.

Seguridad de la aplicación

Protección del código que desarrollamos

El equipo de seguridad de las aplicaciones de Asana trabaja continuamente para mejorar los métodos que se usan para identificar errores de seguridad en nuestra aplicación con la ayuda de investigadores de seguridad internos y externos, herramientas de última generación, modelos de amenazas y pruebas de seguridad. Una vez que se identifica y confirma un error de seguridad, se informa al equipo de gestión de vulnerabilidades para que se aborde de manera oportuna.

El servicio de Asana es una aplicación de software como servicio basada en la web. Los usuarios pueden acceder a sus datos a través del navegador web, la aplicación móvil (iOS y Android) o la interfaz programática de aplicación (API).

Los servicios y componentes de Asana están escritos principalmente en JavaScript, TypeScript, Python y Scala, basados en el marco para aplicaciones React. Asana se desarrolla bajo las mejores prácticas de seguridad definidas por la Fundación OWASP y se mantiene en todo momento un enfoque de seguridad por diseño. Por lo tanto, hemos implementado mecanismos integrales para evitar los riesgos de seguridad, que incluyen, entre otros, los siguientes:

- Inserción de errores
- Autenticación defectuosa
- Exposición de datos confidenciales
- Entidades XML externas (XXE)
- Control de acceso defectuoso
- Configuración incorrecta de seguridad
- Secuencias de comandos entre sitios (XSS)
- Deserialización insegura
- Uso de componentes con vulnerabilidades conocidas
- Registro y monitoreo insuficientes
- Falsificación de solicitud entre sitios (CSRF)
- Redireccionamientos y retransmisión no validados

Terceros independientes realizan auditorías de Asana cada año para todos los principales 10 temas según OWASP. También realizamos nuestras propias pruebas de seguridad internamente en áreas que requieren un análisis particularmente detallado de la efectividad de los controles de seguridad.

Protección del código del que dependemos

Para garantizar que usamos la versión más segura de bibliotecas y componentes de terceros de los que dependemos como parte de nuestra experiencia con el producto, el equipo de seguridad de las aplicaciones ejecuta un programa que responsabiliza a nuestros equipos de ingeniería de instalar actualizaciones en las bibliotecas de terceros. Las bibliotecas y los componentes se actualizan de manera oportuna cuando existe la posibilidad de que se vea afectada la seguridad de nuestro producto.

Seguridad operativa

Información de seguridad de Asana

Asana mantiene un programa formal de gestión de seguridad de la información con personal dedicado exclusivamente a la seguridad que depende del director de seguridad de Asana. Esta organización es responsable de implementar controles de seguridad y supervisar Asana a fin de identificar actividades sospechosas.

Información confidencial

Asana trata todos los datos de los clientes como confidenciales. Nuestras políticas y procedimientos restringen el acceso a la información confidencial a aquellos empleados que deben acceder a dicha información confidencial como parte de su trabajo, y solo en aquellas circunstancias en las que se requiere el acceso a dicha información confidencial para brindar un servicio específico al cliente. En estas circunstancias, se indica al empleado que acceda solo a la cantidad mínima de información necesaria para realizar la tarea en cuestión.

Recursos humanos

Todos los empleados o contratistas de Asana deben firmar un acuerdo de confidencialidad e invenciones. Los empleados de Asana deben realizar una capacitación formal de concientización sobre seguridad al ser contratados y anualmente después de eso.

Todos los ingenieros de Asana firman una política de acceso a los datos donde se describe el acceso y uso apropiado de los datos. Además, contamos con puertas de enlace en cada punto de entrada a los datos de los clientes. Cualquier acceso a los datos se registra y se guarda indefinidamente.

Asana tiene una política de sanciones disciplinarias por violaciones de esta política.

Revisiones y políticas de acceso de usuarios

Trimestralmente, la gerencia revisa el acceso de los usuarios a los sistemas dentro del alcance para verificar su adecuación continua y elimina cualquier acceso que ya no sea necesario. Tras la desvinculación de un empleado, se elimina el acceso.

Seguridad física

Oficinas de Asana

Nuestras oficinas están aseguradas con tarjetas de acceso registrado, y todas las oficinas tienen sistemas de alarma contra intrusos. Los visitantes se registran en la recepción. Todos los empleados deben informar sobre cualquier actividad sospechosa, acceso no autorizado a las instalaciones o incidentes como robos u objetos perdidos.

Seguridad del centro de datos

Asana usa los controles físicos y del entorno de AWS.[12]

[12] http://aws.amazon.com/es/compliance/data-center/controls

Seguridad de la red

Supervisamos la disponibilidad de la red de nuestra oficina y los dispositivos en ella. Recopilamos registros generados por dispositivos de red como firewalls, servidores DNS, servidores DHCP y enrutadores en un lugar central. Se llevan registros de red para la aplicación de seguridad (firewall), los puntos de acceso inalámbricos y los conmutadores.

Seguridad de TI

Todas las laptops y estaciones de trabajo están aseguradas mediante cifrado total de disco y dotadas con imágenes gestionadas en forma central. Aplicamos actualizaciones a las máquinas de los empleados regularmente y controlamos las estaciones de trabajo para detectar malware. También tenemos la capacidad de implementar parches críticos y eliminar de forma remota una máquina a través del administrador de dispositivos. Siempre que es posible, usamos la autenticación de dos factores para asegurar aún más el acceso a nuestra infraestructura corporativa. Asana ejecuta escaneos de seguridad regularmente.

Gestión de riesgos y vulnerabilidades

Asana mantiene procesos continuos de gestión de riesgos previstos para identificar vulnerabilidades de forma proactiva dentro de los sistemas de Asana y para evaluar las nuevas amenazas que emergen en las operaciones de la empresa.

Asana mantiene un proceso de escaneo en busca de vulnerabilidades para sistemas externos e internos en el entorno de producción. El equipo de seguridad de Asana lleva a cabo escaneos de vulnerabilidades al menos con una frecuencia trimestral y corrige vulnerabilidades en base a las valoraciones. Los escaneos en busca de vulnerabilidades también se llevan a cabo después de cualquier cambio importante que se haga al entorno de producción según lo determine el director de seguridad.

Pruebas de penetración

Anualmente, Asana contrata a una empresa de evaluación de seguridad profesional (evaluadores de penetración) para identificar cualquier vulnerabilidad que pueda afectar nuestro producto, datos y sistemas. El alcance de estas pruebas abarca la infraestructura, la aplicación (web y móvil), la red externa y la red interna. Solucionamos los problemas identificados y ponemos el informe de hallazgos a disposición de los clientes para que lo revisen.

Recompensas por detección de errores

Contamos con un programa externo de recompensas por errores[13] donde pagamos a los investigadores de seguridad que descubren vulnerabilidades. Nuestro equipo de seguridad clasifica activamente los informes y paga hasta el doble por hallazgos de errores con la misma gravedad, en comparación con nuestros pares. Este programa genera un compromiso hasta 10 veces mayor que el de nuestros pares y, en última instancia, nos permite ofrecer un producto más seguro.

[13] http://asana.com/es/bounty

Ciclo de desarrollo de software

Asana tiene varios programas de seguridad relacionados con las diferentes etapas del ciclo de desarrollo de software para garantizar que nuestros ingenieros cuenten con el respaldo de la mejor garantía de seguridad de la industria para crear un producto que proteja de manera eficaz a nuestros clientes.

La garantía de nivel de ideación y diseño se utiliza para identificar los cambios planificados que tienen el potencial de afectar la seguridad. Se aplica un proceso estandarizado a todas las iniciativas de diseño de software nuevo y los cambios seleccionados de riesgo medio a alto se revisan y abordan con el equipo de seguridad del producto antes de pasar a la etapa de implementación. Esto ayuda a identificar posibles problemas de diseño con anticipación y evita que los clientes se vean afectados por ellos.

La garantía de nivel de implementación y lanzamiento garantiza que los desarrolladores de Asana tengan disponibles los métodos y las herramientas para identificar y prevenir errores de seguridad en el código. Asana utiliza el sistema de control de versiones Git. Los cambios en el código base de Asana pasan por un conjunto de pruebas automatizadas. Ciertos cambios de alto riesgo pasan por una ronda de revisión manual por parte del equipo de seguridad de la aplicación. Cuando los cambios de código superan las pruebas del sistema de automatizado, se envían a un servidor de prueba donde los empleados de Asana revisan los cambios antes de enviarlos a los servidores de producción y la base de clientes. También implementamos una revisión de seguridad específica para cambios y características particularmente sensibles. Los ingenieros de Asana tienen la capacidad de seleccionar cuidadosamente actualizaciones críticas e insertarlas inmediatamente en los servidores de producción.

Además de una lista donde se publican todos los cambios de control de acceso, tenemos un conjunto de pruebas de unidad automáticas que verifican que las reglas de control de acceso estén escritas correctamente y se apliquen según lo previsto.

Respuesta a incidentes

Asana mantiene un plan de respuestas a incidentes diseñado para establecer respuestas razonables y uniformes a incidentes de seguridad y ante las sospechas de incidentes de seguridad. Un incidente de seguridad o un supuesto incidente de seguridad implica la destrucción ilegal o accidental, la pérdida, el robo, la modificación, la divulgación no autorizada o el acceso a los datos privados o personales que se transmitan, almacenen o de algún modo se procesen en Asana. Estos procesos de respuesta a incidentes detallan el modo en que el equipo de seguridad de Asana clasifica, investiga, corrige e informa acerca de los incidentes de seguridad. Asana ha contratado compañías dedicadas a dar respuesta a incidentes y a peritos digitales externos para actuar en caso de que ocurra una vulneración de datos.

Continuidad del negocio y recuperación ante catástrofes

Asana ha preparado un plan de continuidad del negocio para cortes prolongados del servicio que puedan ser causados por catástrofes imprevistas o inevitables. El objetivo es restaurar los servicios en la mayor medida posible y en un marco razonable de tiempo. Asana ha documentado un conjunto de políticas y procedimientos para la recuperación posterior a catástrofes con sistemas e infraestructura tecnológica vitales. Asana prueba anualmente el plan de recuperación ante desastres y publica los resultados para los clientes.

Los principales centros de datos de Asana están alojados en AWS en Virginia, EE. UU. Aquellos clientes que cumplen con ciertos requisitos (plan Enterprise) pueden solicitar que sus datos se almacenen en Frankfurt (Alemania), Sídney (Australia) o Tokio (Japón). En caso de pérdida de uno de los centros de datos de AWS, los procedimientos de recuperación activarán los nodos de otro centro de datos. Para los casos de catástrofes mayores, hay un sitio para la recuperación posterior a catástrofes alojado en el centro de datos de AWS en Ohio (EE. UU.) para los datos de EE. UU., en Dublín (Irlanda) para los datos de la Unión Europea y Australia, y en Osaka (Japón) para los datos de Japón.

Retención y eliminación de datos

Asana conserva la información del cliente durante el período necesario para cumplir con los propósitos descritos en la Política de privacidad. Si el representante autorizado de un cliente lo solicita, después de una verificación, los clientes pueden pedir que se exporte o elimine el dominio de los datos del cliente. Asana también puede acordar la preservación de la confidencialidad de cualquiera de los datos guardados de los clientes y solamente procesará activamente tales datos del cliente después de la fecha de solicitud para cumplir con las leyes de las que es objeto.

Supervisión

Asana usa Amazon CloudWatch y Cloudtrail, combinados con scripts personalizados que extraen datos importantes de los registros y los envían a los servicios de monitoreo. Asana supervisa la utilización de la capacidad de la infraestructura informática y física tanto internamente como para los clientes a fin de garantizar que el nivel de servicio coincida con los acuerdos. Tenemos escaneos de seguridad automatizados en nuestra red y aplicaciones, además de controles y alertas para los núcleos en los servidores. Un script de monitoreo se ejecuta semanalmente para validar que los cambios de código se revisaron correctamente.

Ciertos registros de las máquinas y aplicaciones se guardan indefinidamente y por lo general se guardan en el almacenamiento a largo plazo en S3. Los registros informáticos más detallados se almacenan solamente en las máquinas que los generan y por lo general se guardan durante dos semanas.

Gestión de proveedores y subprocesadores

Asana toma medidas razonables para seleccionar y retener solo a aquellos proveedores de servicios de terceros que mantendrán e implementarán medidas de seguridad acordes a nuestras propias políticas. Antes de que se implemente el software o se pueda utilizar un proveedor de software en Asana, el personal de seguridad, privacidad y TI de Asana revisa cuidadosamente los protocolos de seguridad, las políticas de retención de datos, las políticas de privacidad y el historial de seguridad del proveedor. Cualquier proveedor que no pueda demostrar su capacidad de proteger correctamente los datos de Asana y de los usuarios finales puede ser rechazado. Anualmente se realizan reevaluaciones de proveedores clave.

Como condición para permitir que un subprocesador procese los datos de clientes, Asana (y sus filiales, según corresponda) firmarán un acuerdo escrito con cada subprocesador. El contrato incluirá obligaciones para la protección de los datos que deben garantizar un nivel de seguridad al menos equivalente al de las medidas técnicas y organizativas implementadas por Asana para proteger los datos personales de los clientes ante cualquier destrucción, pérdida, alteración o divulgación o acceso sin autorización que se produzca, sean de carácter accidental o ilegal.

Los clientes pueden registrarse para recibir notificaciones sobre cambios en los subprocesadores y revisar los subprocesadores actuales en nuestra página de subprocesadores.[14]

[14] http://asana.com/es/terms#subprocessors

Privacidad, certificaciones y cumplimiento normativo

Declaración de privacidad

En la Declaración de privacidad de Asana se informa sobre nuestras prácticas actuales de procesamiento de datos. Esta se actualiza regularmente. En la Declaración de privacidad se describen los datos que recopilamos y procesamos y se brinda información sobre cómo las personas pueden ejercer sus derechos de privacidad según las leyes pertinentes.[15]

Transferencias internacionales de datos

Las leyes de protección de datos de la Unión Europea exigen que las organizaciones utilicen un mecanismo legal reconocido para transferir datos de la Unión Europea a países que no tienen un marco de protección de datos similar, incluido Estados Unidos.

A pesar de que ya no es válida la transferencia de datos personales desde la Unión Europea y Suiza hacia los Estados Unidos bajo los marcos del Escudo de la Privacidad de UE-EE. UU. y de Suiza-EE. UU, el Anexo sobre procesamiento de datos de Asana incluye cláusulas contractuales estándares, que continúan sirviendo como mecanismos legales para la transferencia de datos personales fuera del EEE. Asana también usa estas cláusulas contractuales estándares con todos los subprocesadores.

Asana ha implementado muchas medidas complementarias para proteger los datos personales transferidos desde el EEE, como las que se enumeran en este informe. Seguimos las mejores prácticas de la industria, como cifrar las transferencias de datos de la Unión Europea a EE. UU. por parte de Asana mediante el uso de la plataforma de Asana.

A pesar de que no podemos depender del Escudo de la Privacidad para transferir datos del EEE y de Suiza, Asana ha decidido mantener su certificación del Escudo de la Privacidad para seguir protegiendo los datos ya transferidos bajo el Escudo de la Privacidad y por su compromiso con las medidas de seguridad para la protección de los datos.

Las normativas regulatorias en esta área continúan evolucionando y nosotros seguimos de cerca las normativas nuevas de las autoridades en materia de protección de datos. En Asana mantenemos nuestro compromiso con la privacidad de los datos de los clientes y seguiremos trabajando para asegurarnos de cumplir con las leyes de protección de datos.

RGPD

El Reglamento General de Protección de Datos (RGPD) es una ley europea con la que se establece la protección de los datos personales de los residentes en la UE y que entró en vigencia el 25 de mayo de 2018. Bajo el RGPD, las organizaciones que recopilan, mantienen, usan o de algún modo procesan los datos personales de los residentes de la UE (independientemente de la ubicación de la organización) deben implementar ciertas medidas de seguridad y privacidad de esos datos. Asana ha establecido un programa integral de conformidad con el RGPD y se compromete a colaborar con sus clientes y proveedores en sus esfuerzos por cumplir con el RGPD. Algunas medidas importantes que ha tomado Asana para alinear sus prácticas con el RGPD son las siguientes:

- Revisiones de nuestras políticas y contratos con socios, proveedores y usuarios
- Mejoras de nuestras prácticas y procedimientos de seguridad
- Revisión y vinculación estrictas de los datos al momento de recopilarlos, usarlos y compartirlos

[15] https://asana.com/es/terms#privacy-policy

- Creación de documentación más sólida sobre seguridad y privacidad internas
- Capacitación de los empleados acerca de los requisitos del RGPD y las mejores prácticas de privacidad y seguridad en general
- Creación y evaluación rigurosa de una política de derechos de los interesados y un proceso de respuesta. A continuación, brindamos detalles adicionales sobre las áreas centrales del programa de cumplimiento del RGPD de Asana y cómo los clientes pueden usar Asana para respaldar sus propias iniciativas de cumplimiento del RGPD.
- Designación de un responsable de la protección de datos (DPO), a quien se pueda contactar en **dpo@asana.com**.

APPI

La Ley de Protección de Información Personal (APPI) es la principal ley de protección de datos en Japón que regula la protección de la información personal. Se aplica a los operadores comerciales que manejan información personal de individuos en Japón. Asana tiene el compromiso de procesar y proteger la información personal según lo exige la APPI y sus enmiendas. El Anexo de procesamiento de datos de Asana[16] abarca (1) nuestros compromisos de protección de datos para garantizar que cumplimos con la APPI; (2) cómo ayudaremos a nuestros clientes con sus obligaciones en virtud de la APPI; y (3) las medidas técnicas y organizativas implementadas para proteger la información personal.

Anexo sobre procesamiento de datos

Bajo el RGPD, los "controladores de datos", es decir, las entidades que determinan los propósitos y los medios del procesamiento de datos, deben celebrar acuerdos con otras entidades que procesan datos en su nombre (llamados "procesadores de datos"). Asana ofrece a sus clientes un sólido Anexo de procesamiento de datos (DPA) en virtud del cual Asana se compromete a procesar y proteger los datos personales de acuerdo con la ley aplicable. Esto incluye las cláusulas contractuales estándares actuales y el compromiso de Asana de procesar los datos personales de acuerdo con las instrucciones del controlador de datos. El Anexo de procesamiento de datos se puede consultar en nuestra página de Términos[17] y se incorpora por referencia en el acuerdo de suscripción correspondiente entre Asana y el cliente.

Aplicación de la ley

Asana se rige de acuerdo a las directrices de solicitud de datos según lo exige la ley y que se indican en nuestra página de directrices.[18]

[16] https://asana.com/es/terms#data-processing
[17] https://asana.com/es/terms#data-processing
[18] https://asana.com/es/terms#law-enforcement-guidelines

Certificaciones, atestaciones y cumplimiento

Asana asume el compromiso constante de garantizar que nuestros servicios cumplan con los estándares globales de seguridad, privacidad y cumplimiento. Asana actualmente mantiene las siguientes certificaciones y atestaciones:

SOC 2 Tipo II: Asana ha superado con éxito sus auditorías SOC 2 (Tipo II) de los controles implementados para la seguridad, la disponibilidad y la confidencialidad. Lograr esta certificación SOC 2 (Tipo II) significa que un proveedor externo e independiente ha validado los procesos y las prácticas que hemos establecido en relación con los tres criterios de control.

ISO/IEC 27001:2013: Asana mantiene una certificación ISO/IEC 27001:2013 para demostrar su conformidad con los requisitos definidos en el estándar ISO/IEC 27001:2013 para establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información.

ISO 27017:2015: demuestra la conformidad de Asana con los controles de seguridad de la información aplicables a la provisión y el uso de servicios en la nube.

ISO 27018:2019: demuestra las medidas que Asana ha implementado para proteger la información de identificación personal (PII) de acuerdo con los principios de privacidad de ISO/IEC 29100 para el entorno de informática en la nube pública.

ISO 27701:2019: demuestra el compromiso de Asana de establecer, mantener y mejorar continuamente el sistema de gestión de información privada como una extensión de ISO 27001 para la gestión de la privacidad dentro de la organización.

Cumplimiento de la Ley HIPAA

Asana proporciona protecciones de seguridad y privacidad que permiten a los clientes usar Asana en conformidad con la Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU. (HIPAA). Los clientes que están sujetos al cumplimiento de la Ley HIPAA y desean almacenar información de salud protegida (PHI) en Asana deben comprar un plan Enterprise y celebrar un acuerdo de asociación comercial (BAA) con Asana. Para obtener más información sobre el cumplimiento de la Ley HIPAA en Asana, comunícate con el equipo de ventas de Asana.[19]

Registro CSA STAR

La autoevaluación de nivel 1 del Cuestionario de la iniciativa de evaluaciones de consenso de CSA (CAIQ) completada por Asana está disponible en el Registro CSA STAR.[20]

[19] https://asana.com/es/guide/help/premium/hipaa-compliance
[20] https://cloudsecurityalliance.org/star/registry/asana-inc/services/asana/

Conclusión

En Asana, usamos nuestra plataforma todos los días con confianza para alinear el trabajo de nuestros equipos de todo el mundo. Más de 100 000 empresas hacen lo mismo. Nuestra prioridad es mantener tus datos seguros, para que trabajes con tranquilidad.

Asana ofrece una seguridad completa del producto para toda tu organización. Contamos con un programa establecido de confianza y cumplimiento para proteger tus datos. Para obtener más información sobre las opciones de pago de Asana, envía un email a nuestro equipo de ventas a sales@asana.com.

Si quieres informar un problema de seguridad, envíanos un email a security@asana.com.