# monday.com Informe técnico de seguridad y privacidad

| Fecha | Versión | Descripción del cambio |
|---|---|---|
| Noviembre de 2021 | 1.0 | Versión final |

La intención de este informe técnico es ofrecer un resumen general de las prácticas de seguridad y privacidad de monday.com vigentes a la fecha de su publicación, y sujeto a cambios sin previo aviso. Cualquier descripción de planes futuros está sujeta a cambios o retrasos, a criterio de monday.com. La finalidad de este informe técnico es solo la de informar y no constituye una asesoría jurídica ni debe interpretarse como un complemento o una incorporación a los términos y condiciones de ningún acuerdo contractual.

# Índice

# 1. Introducción

El sistema operativo de trabajo (Work OS) de monday.com administra los datos de más de 127,000 compañías alrededor del mundo y, con esta responsabilidad, asumimos el compromiso de ofrecer a nuestros clientes los más altos estándares de seguridad y protección de datos. Nos hemos ganado la confianza de nuestros clientes al hacer que la protección de los datos sea nuestra máxima prioridad.

**Declaración de nuestra misión**
Llevar tranquilidad a nuestros clientes al administrar sus datos en el Work OS de monday.com.

**Nuestros equipos**
Las iniciativas relativas a la seguridad de la información de monday.com están bajo la dirección y la supervisión de nuestro CISO (Oficial de seguridad de la información) y el equipo de Seguridad, además de un Foro de Seguridad compuesto por representantes de los equipos de Infraestructura, I+D, Operaciones y TI.
Las iniciativas relativas a la privacidad de monday.com están bajo la dirección y supervisión de nuestro Foro de privacidad, compuesto por representantes de los equipos de Legales, Privacidad y Seguridad y conducidos por nuestro DPO (Delegado de protección de datos).

**Enlaces de utilidad**

Centro de confianza de monday.com
Portal jurídico de monday.com
Página de estado de monday.com
Subprocesadores, subsidiarias y soporte
La seguridad y la privacidad en monday.com - Preguntas frecuentes
Informar vulnerabilidades
Soporte y base de conocimientos
Precios y planes
Blog monday.Engineering

---

# 2. Seguridad de la infraestructura

**Proveedores de alojamiento**

Para alcanzar un alto nivel de disponibilidad y resiliencia, nuestro servicio se aloja en la infraestructura de Amazon Web Services (AWS) en distintas regiones, principalmente en el norte de Virginia (EE. UU.) y en Frankfurt (Alemania),[1] en varias zonas de disponibilidad, con despliegues dedicados a la recuperación de desastres (DR) en distintas regiones. Las cuentas de los clientes están ligadas a una sola región.

Con el modelo de responsabilidad compartida de AWS, AWS gestiona la seguridad de la infraestructura de computación en la nube, mientras que monday.com gestiona la seguridad del software y de los datos que se encuentran en la infraestructura de computación en la nube.

La función de Registro de actividades (que se describe con mayor detalle a continuación, en este documento) hace copias de seguridad de los datos en la Google Cloud Platform (GCP), en EE. UU.

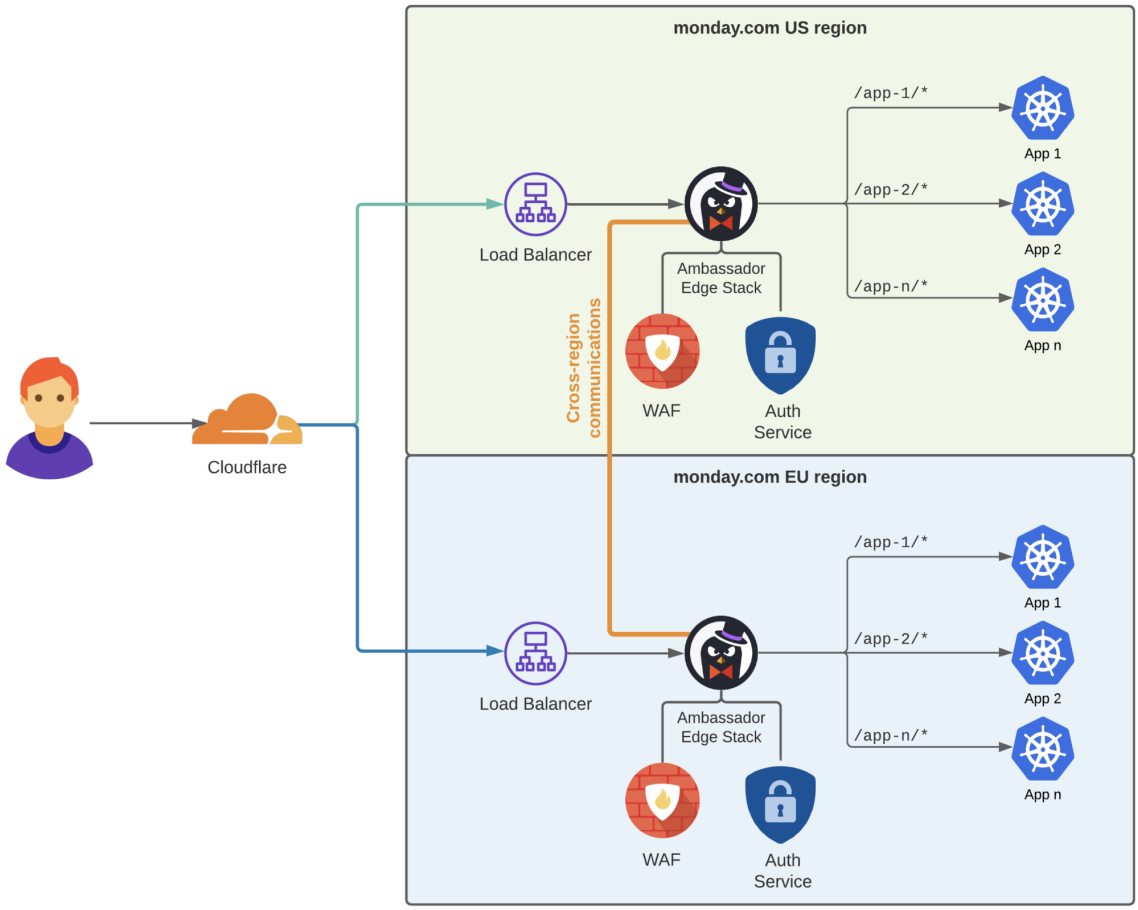
**Arquitectura de la red**

- La arquitectura de la red de monday.com está construida de acuerdo con las mejores prácticas de AWS, que implica la separación entre subredes públicas y privadas.
- monday.com utiliza diversos proveedores de CDN, como Cloudflare y Fastly, para prevenir ataques DDoS y de fuerza bruta. La restricción de velocidad se configura tanto en el extremo como en el nivel de la aplicación.
- Los balanceadores de carga se encuentran en la subred pública, mientras que los componentes internos de la red, como los servidores de aplicaciones web y las bases de datos, se encuentran en la subred privada y no tienen asignadas IP públicas.
- Hay un firewall de aplicaciones web (WAF) para bloquear ataques dinámicos basados en el contenido.
- Se utilizan firewalls en toda la red para ejecutar la lista blanca de IP y el acceso por los puertos permitidos únicamente para los recursos de la red. Las reglas de los Grupos de seguridad se configuran para permitir el acceso únicamente de los puertos requeridos.
- Los sensores del sistema de detección de intrusos en redes (NIDS) se usan junto con los servicios de seguridad nativos de AWS, habilitados para todos los activos de producción.

A continuación, los aspectos más destacados del diagrama de la red de monday.com, para la región de datos de Estados Unidos y de la UE:[2]

[1] Los clientes del Plan Corporativo pueden optar por alojar sus datos en nuestro centro de datos de la UE en Frankfurt, Alemania.

[2] Se puede compartir un diagrama de red de alto nivel, previa solicitud y mediante la firma de un acuerdo mutuo de confidencialidad (MNDA).




Se utiliza en gran medida la Infraestructura como código para garantizar el rastreo y la auditoría de los cambios de la configuración. El equipo de Infraestructura de monday.com lleva a cabo una revisión exhaustiva de la configuración de la red perimetral de manera trimestral e implementa los cambios necesarios para mantener o reforzar la seguridad.

aws partner network

Socio de tecnología avanzada de AWS

monday.com también es un Socio de tecnología avanzada de AWS, lo cual certifica que AWS ha examinado minuciosamente nuestra organización en materia de infraestructura, seguridad de la información, elaboración de las mejores prácticas, etc.

**Seguridad de redes**

Dado que monday.com es una solución basada completamente en la nube, contamos con la ventaja de utilizar modernos controles centrados en los servicios de nube para obtener una visión precisa del perímetro de nuestras redes. Recopilamos y supervisamos los registros de la red a través de NIDS y registros de tráfico de las ubicaciones de borde; además, revisamos las alarmas pertinentes con nuestro sistema de información de seguridad y gestión de eventos (SIEM). Utilizamos herramientas de supervisión de la seguridad que obtienen periódicamente la configuración de nuestros grupos de seguridad y ACL de red desde el proveedor de la nube y generan una visión integral de nuestra red.

El equipo de Infraestructura de monday.com lleva a cabo una revisión exhaustiva de la configuración de la red perimetral de manera trimestral e implementa los cambios necesarios para mantener o reforzar la seguridad. Además, cada año, recurrimos a un auditor independiente para que revise la configuración de nuestra red.

**Acceso a la producción**

El acceso a los activos de la producción se otorga de acuerdo con rol y de conformidad con los principios de necesidad de divulgación de información y de privilegios mínimos. Únicamente nuestro personal de Infraestructura tiene privilegios administrativos (un equipo reducido y limitado de ingenieros expertos). Se exige el uso de nuestra VPN para cualquier acceso a los servidores de monday.com, con la autenticación de nuestro proveedor de identidades (IdP), completamente auditado, la seguridad de las contraseñas y la autenticación multifactor (MFA).
El acceso de nuestros desarrolladores a los activos de producción es mediante el reenvío de puertos Kubernetes y se autentica de manera similar contra nuestro IdP.

**Endurecimiento**

Los servidores están basados en la última versión de Ubuntu LTS (20.04), con un endurecimiento conforme a las normas del CIS (Centro de seguridad de internet).

**Bases de datos**

Las bases de datos que utiliza monday.com incluyen MySQL, Elasticsearch y Redis. Las claves API para sistemas externos, que utilizan nuestras funciones de integración, se almacenan en un clúster específico de replicación automática de HashiCorp Vault.

**Almacenamiento de archivos**

El almacenamiento de archivos se aloja en Simple Storage Service (S3) de AWS, que almacena copias de seguridad de bases de datos y adjuntos. Los adjuntos incluyen cualquier archivo que el cliente carga al servicio de monday.com.
monday.com ofrece un servicio de detección automática de malware para los archivos que los usuarios cargan al servicio; esto garantiza que los archivos externos que se cargan en el servicio no estén infectados. Además, contamos con una lista negra que incluye una cantidad de extensiones de archivos prohibidas. La lista negra de extensiones de archivos contiene tipos de archivos que pueden considerarse peligrosos, como los ejecutables o HTML. Al bloquear estos tipos de archivos, se reduce el riesgo de sufrir una importante infección por malware.

**Multirregión**

A enero de 2021, monday.com se extendió llegando a su primera región de datos en Europa, en Frankfurt, Alemania (actualmente disponible para los clientes del plan Corporativo).
Dado que los principios de la infraestructura son idénticos en la región de Estados Unidos, los clientes de monday.com en la UE pueden disfrutar de la experiencia de monday.com con el mismo nivel de medidas y controles de seguridad, y con la confianza de que se cumple con los principios de la tríada de Confidencialidad, Integridad y Disponibilidad (CIA).
Arriba, se muestran los principales aspectos del diagrama de la red de monday.com.
Tenemos previsto abrir centros de datos en otras regiones más adelante.

## Cifrado y administración de claves

Cifrado en tránsito

Los datos en tránsito a través de las redes abiertas tienen cifrado TLS 1.3 (o TLS 1.2 como mínimo).

Cifrado en reposo

Los datos en reposo tienen cifrado AES-256. Las claves de cifrado se almacenan mediante el Key Management Service (KMS) de AWS. Actualmente, se utiliza una clave maestra de cliente (CMK) de rotación anual para cifrar todos los datos que el cliente envía al servicio de monday.com y que se procesan en su nombre.

Separación de clientes

Contamos con un entorno multiempresa que establece una separación lógica entre clientes. Los datos de los clientes se segmentan a nivel de aplicación, mediante identificadores exclusivos como resultado de una combinación de diferentes parámetros.

En estos momentos, estamos trabajando para habilitar el cifrado a nivel de empresa (TLE) para nuestros clientes. TLE es una capa que asegura el cifrado de los datos en reposo con una clave específica por cuenta y ofrece protección para evitar que los sistemas o el personal no autorizado puedan ver los datos.

TLE ofrece protección ante dos posibles escenarios:

1. **Atacantes:** los datos en los campos de las bases de datos están cifrados, de modo que el tener acceso a la base de datos y extraer la información solo le dará al atacante datos cifrados.
2. **Divulgación accidental:** los datos están cifrados con una clave específica por cuenta de modo que, si se divulgan por accidente entre cuentas, nunca se verán como texto nítido.

Más adelante, tenemos previsto ofrecer a los clientes del Plan Corporativo la opción de usar sus propias claves de cifrado (BYOK: Bring Your Own Key - "traiga su propia clave").

## Copia de seguridad

monday.com hace copias de seguridad de todos los datos que el cliente sube al servicio de monday.com y que se procesan en su nombre. Hacemos copias de seguridad de los datos de los usuarios cada cinco minutos y las distribuimos cifradas en múltiples zonas de disponibilidad de AWS. También hemos establecido sitios de recuperación de desastres (DR) en regiones separadas de AWS a los efectos de la redundancia. Los datos del Registro de actividades se respaldan en GCP.

## Escalabilidad y confiabilidad

En caso de que uno o más componentes fallen, se utiliza la arquitectura de microservicios para asegurar que el impacto en el estado del sistema sea mínimo. El servicio de monday.com está completamente en contenedores y se utilizan Kubernetes para la orquestación; esto posibilita una infraestructura de gran escalabilidad, ideal para suplir la creciente demanda de los clientes a la vez que ofrece una experiencia de calidad para los usuarios finales.

La infraestructura como código se usa en gran medida a través de Terraform para asegurar la auditabilidad y mantenibilidad de los recursos de la infraestructura.

monday.com supervisa de forma continua los parámetros de rendimiento de todos los componentes de la infraestructura y desarrolla su infraestructura a escala. Incluso, realizamos evaluaciones trimestrales a escala con los ingenieros de infraestructura y la gerencia para garantizar que nuestra hoja de ruta ofrezca un servicio de calidad a una cantidad cada vez mayor de clientes y de funciones de productos.

## Acuerdo de nivel de servicio (SLA)

La disponibilidad de nuestro servicio se puede supervisar a través de la Página de estado. En raras ocasiones, hay un tiempo de inactividad del sistema para su mantenimiento. Cuando es necesario y posible, se programa los fines de semana, en horas de poca actividad.

A través de la Página de estado se puede acceder de inmediato a las notificaciones respecto del tiempo de inactividad; allí, los clientes pueden suscribirse para recibir, por email o mensaje de texto, las notificaciones sobre la disponibilidad y los esfuerzos de mitigación de nuestro equipo.

Los clientes del Plan Corporativo cuentan con nuestro compromiso del 99.9% de tiempo de actividad.

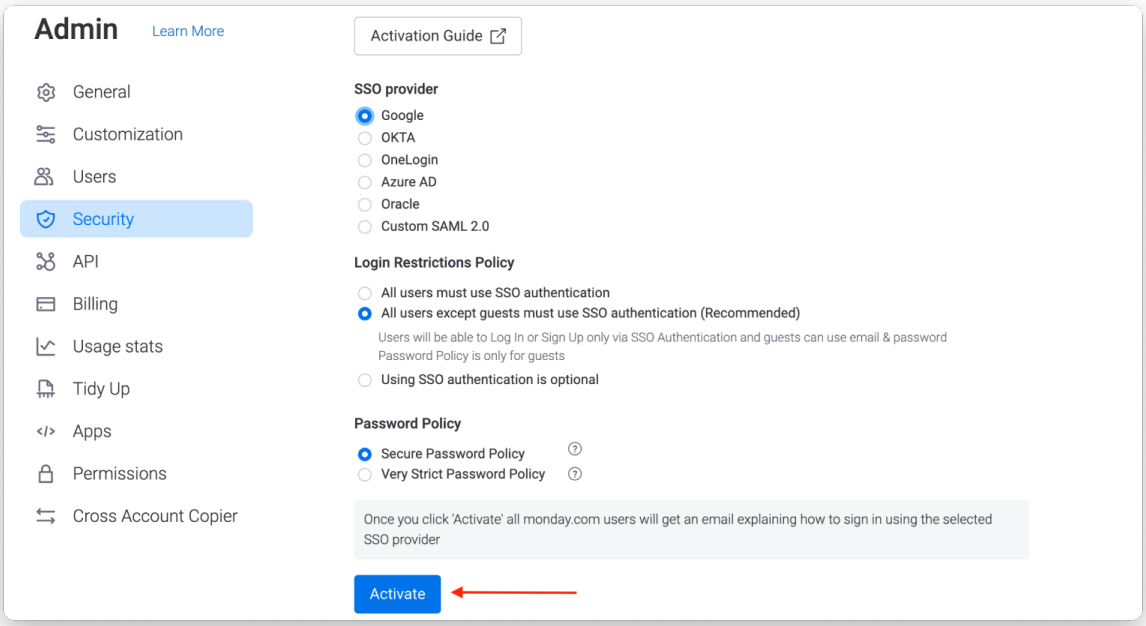
---

# 3. Funciones y características de seguridad

**Autenticación**
monday.com es compatible con los siguientes métodos de autenticación:
Credenciales:
Si elige autenticar a los usuarios de su cuenta mediante el uso de credenciales, ofrecemos administradores con la opción de dos configuraciones de seguridad por contraseña para sus cuentas:

1. con un mínimo de 8 caracteres, que no pueden repetirse ni ser consecutivos; o
2. con un mínimo de 8 caracteres, que no pueden repetirse ni ser consecutivos y la inclusión de al menos un dígito (1, 2, 3), una letra minúscula (a, b, c) y una letra mayúscula (A, B, C).

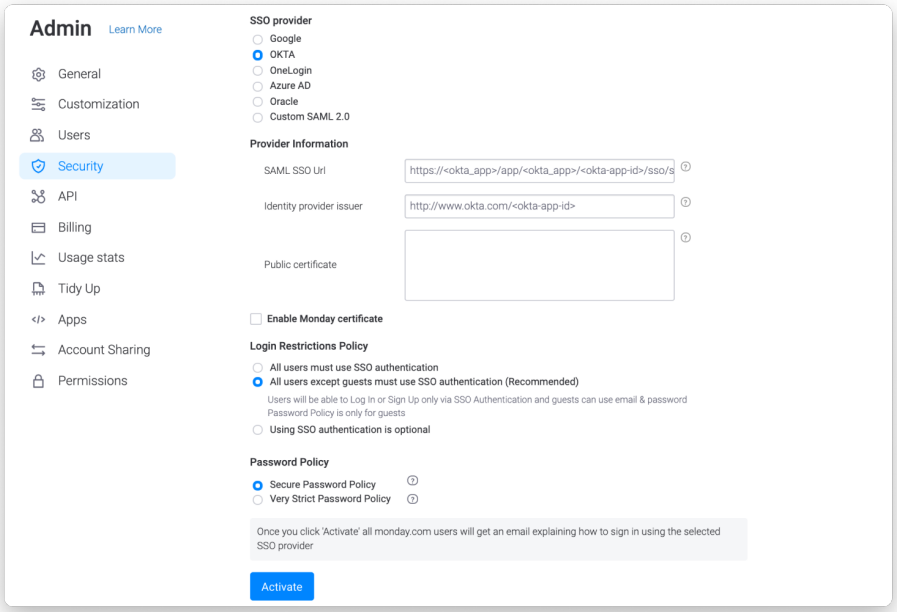
Inicio de sesión único de Google (SSO)
SSO de Google es un sistema de autenticación seguro que alivia la carga de tener que recordar muchas contraseñas, ya que permite a los usuarios iniciar sesión en el servicio de monday.com con su cuenta de Google.
Esta función está disponible únicamente para los planes Pro y Corporativo.




Proveedor de identidades (IdP)
Actualmente, monday.com es compatible con tres proveedores de identidades principales:

1. OKTA
2. Azure AD
3. OneLogin

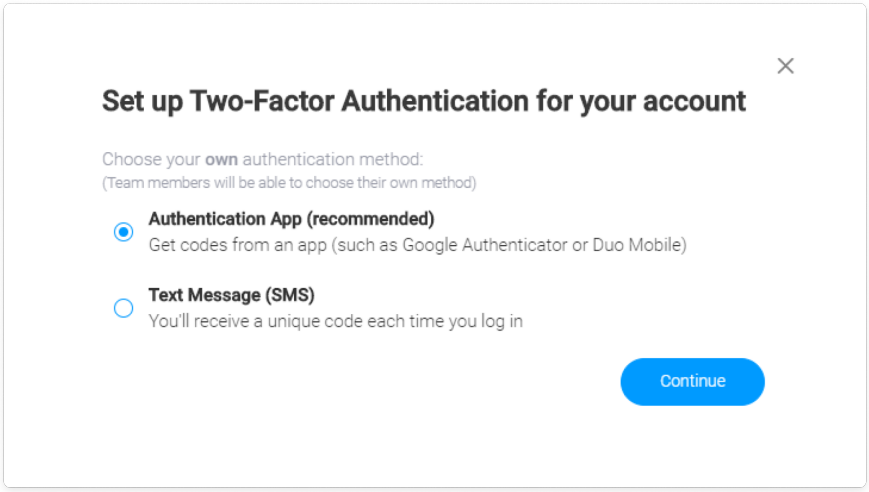
Además, los clientes tienen la opción de usar su propio proveedor, a través de un SAML 2.0 personalizado.
Esta función está disponible únicamente para los clientes del Plan Corporativo.




Autenticación de dos factores (2FA)

Aparte de los dos métodos de autenticación mencionados, los administradores pueden configurar una capa de seguridad extra y habilitar la 2FA por mensaje de texto (SMS) o desde una aplicación de autenticación.

Tenga en cuenta que, si elige integrar su IdP, debe habilitar la 2FA desde su lado.




## Autorización

Aprovisionamiento de SCIM

El sistema de gestión de identidades entre dominios (SCIM) es un protocolo de gestión de usuarios en múltiples aplicaciones que permite aprovisionar (agregar), cancelar el aprovisionamiento (desactivar) y actualizar fácilmente los datos de los usuarios y los equipos en

distintas aplicaciones a la vez. monday.com ofrece tres maneras de configurar el aprovisionamiento de SCIM:

1. Aplicaciones de SCIM actuales en monday.com:
    a. OKTA
    b. Azure AD
    c. OneLogin
2. Integración SCIM personalizada con el proveedor de identidades de su elección.
3. Aprovisionamiento de SCIM con API

La siguiente tabla presenta todos los atributos de **usuario** compatibles con la integración SCIM de monday.com:

| atributo de monday.com | Atributo/s API de SCIM | Descripción |
|---|---|---|
| Nombre (obligatorio) | name, displayName | Nombre de usuario para mostrar |
| Dirección de email (obligatorio) | userName, email | La dirección de email utilizada por el usuario para iniciar sesión en el servicio de monday.com. |
| Activo (obligatorio) | active | Al crear un usuario, este campo debe establecerse en 'true'. Cambiar el valor 'active' del usuario por 'false' lo desactivará en el servicio de monday.com. |
| Posición | title | La posición del usuario en la organización |
| Zona horaria | timezone | La zona horaria del usuario (todas las fechas de la plataforma se ajustarán a esta zona horaria). |
| Configuración regional | locale | monday.com mostrará una versión localizada según las diferentes regiones. |
| Número de teléfono | phoneNumbers | Los números de teléfono del usuario (solo se mostrará el que está marcado como 'primary'). |
| Domicilio | addresses | El domicilio del usuario (solo se mostrará el que está marcado como 'primary'). |
| Tipo de usuario | userType | El nivel de cada usuario en la cuenta. Los valores posibles son: admin, miembro, espectador o invitado (el valor predeterminado es "miembro"). |

La siguiente tabla presenta todos los atributos del **equipo** compatibles con la integración SCIM de monday.com:

| atributo de monday.com | Atributo/s API de SCIM | Descripción |
|---|---|---|
| Nombre (obligatorio) | displayName | Nombre del equipo para mostrar. |
| Usuarios | members | Lista de usuarios asignados al equipo. |

Esta función está disponible únicamente para los clientes del Plan Corporativo.

## Permisos

monday.com le ayuda a controlar quién puede hacer qué cosa en su cuenta. Ofrecemos diversos tipos de permisos que puede personalizar para restringir la visualización o la edición de los datos, entre los que se incluyen:

1. **Permisos de tableros**

   a. Tipos: tableros "Principal", "Compartible" y "Privado".
   b. Restricciones: "Editar todo", "Editar contenido", "Editar por usuario asignado" y "Solo ver"
2. **Permisos de columna**: "Restringir la edición de columna" y "Restringir la vista de columna"
3. **Permisos de panel:**
   a. Tipos: paneles "Principal" y "Privado"
   b. Restricciones: solo los propietarios del panel pueden editar el panel, al igual que sus aplicaciones y widgets
4. **Permisos del espacio de trabajo**
   a. Tipos: espacios de trabajo "Abierto" y "Cerrado"
   b. Restricciones: "Ninguno", "Solo el administrador", "Propietarios del espacio de trabajo" y "Cualquiera"
5. **Permisos de cuenta:** los administradores pueden establecer restricciones ("Ninguno", "Solo el administrador" y "Cualquiera") para las siguientes funciones:
   a. Cargar archivos
   b. Transmitir tableros
   c. Crear tableros principales
   d. Crear tableros privados
   e. Crear tableros compartibles
   f. Crear integraciones
   g. Crear automatizaciones
   h. Crear espacios de trabajo
   i. @mencionar o suscribir a todos los usuarios a la cuenta para una actualización o tablero
   j. Exportar a Excel los tableros, los registros de actividades, los resultados de búsqueda y las actualizaciones

Tenga en cuenta que algunas de las funciones mencionadas podrían no estar disponibles en todos los planes.

## Funciones dentro de monday.com

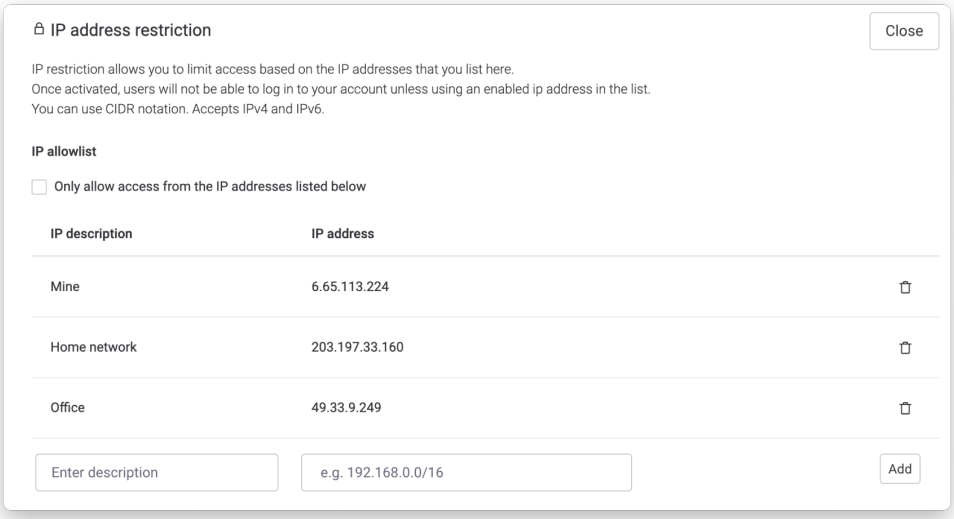
Los roles dentro de monday.com incluyen:

| Rol | Descripción | Puede | No puede |
|---|---|---|---|
| **Administrador** | Un miembro del equipo (o más, si así lo selecciona) que administra su equipo | • Supervisar toda la cuenta<br>• Gestionar todo, desde los usuarios y los tableros hasta la seguridad y la facturación (como se describe abajo, en la sección "Panel de administrador") | |
| **Miembro** | Tiene acceso a la edición<br><br>(La cantidad de miembros que puede invitar depende de su plan) | • Crear y editar tableros, elementos y carpetas<br>• Invitar a otros miembros dentro de un tablero o elementos<br>• Ver todos los tableros principales<br>• Ser invitado a tableros compartibles o privados<br>• Editar su perfil | |

| | | | |
|---|---|---|---|
| | | • Comunicar y agregar adjuntos | |
| **Espectador** | Solo puede ver los tableros, no tiene derechos de edición<br><br>(Puede invitar a una cantidad ilimitada de espectadores independientemente del plan adquirido) | • Ver todos los tableros en el espacio de trabajo principal de la cuenta<br>• Abrir un elemento y leer actualizaciones<br>• Buscar o filtrar dentro de un tablero<br>• Ser invitado a tableros compartibles o privados<br>• Editar la sección de su perfil<br>• Invitar a nuevos espectadores<br>• Abrir las vistas de tablero<br>• Ser asignado a un elemento<br>• Ser agregado a un equipo<br>• Exportar tableros a Excel | • Crear o eliminar un tablero nuevo<br>• Realizar cambios a cualquier contenido, estructura o configuración de un tablero<br>• Actualizar un elemento o dar "me gusta" a una actualización que otro publique<br>• Suscribirse o suscribir a otros a un elemento/tablero<br>• Ser asignado como el propietario de un tablero<br>• Invitar a alguien a un tablero compartible<br>• Crear un equipo |
| **Invitado** | No pertenece a su organización, por ejemplo, un proveedor, un cliente, un trabajador autónomo o un asesor externo | • Ser invitado a tableros compartibles<br>• Desempeñarse como un miembro | • Ver información en los tableros principales o privados |

## Restricciones de direcciones IP

Los administradores pueden predefinir un conjunto de direcciones IP autorizadas las cuales podrán acceder a su cuenta. Así, usted puede restringir qué usuarios pueden acceder a su cuenta según el contexto; por ejemplo, quienes se unan desde un lugar específico (es decir, desde la oficina) o quienes usen determinada VPN. Cualquier usuario que intente ingresar con una dirección de IP que no esté en la lista de direcciones autorizadas recibirá un mensaje de error y no podrá continuar.
Esta función está disponible únicamente para los clientes del Plan Corporativo.

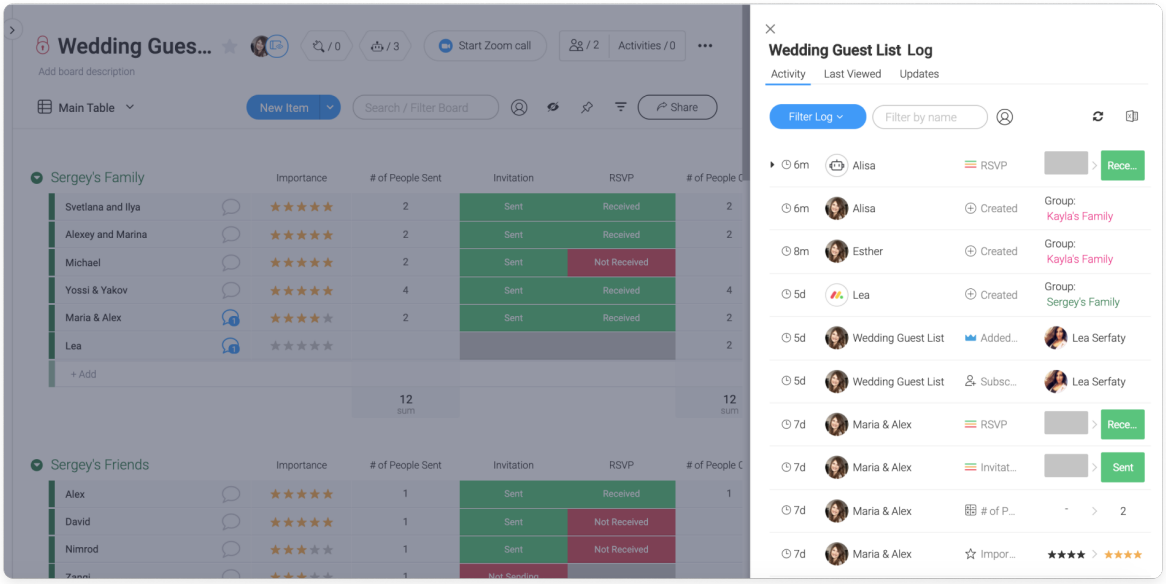



## Registros

### Registro de actividades

Hay dos tipos de Registros de actividades:

1. El **Registro de actividades del tablero** muestra toda la actividad previa de un tablero en una lista, que incluye fechas, estados, movimiento entre grupos, automatizaciones y permisos. La información que se muestra en el Registro de actividades del tablero varía según su nivel: el plan Básico mantiene solamente la actividad de la última semana; el Plan Estándar mantiene los datos de las actividades por 6 meses; mientras que los planes Pro y Corporativo mantienen un registro de hasta 1 año.



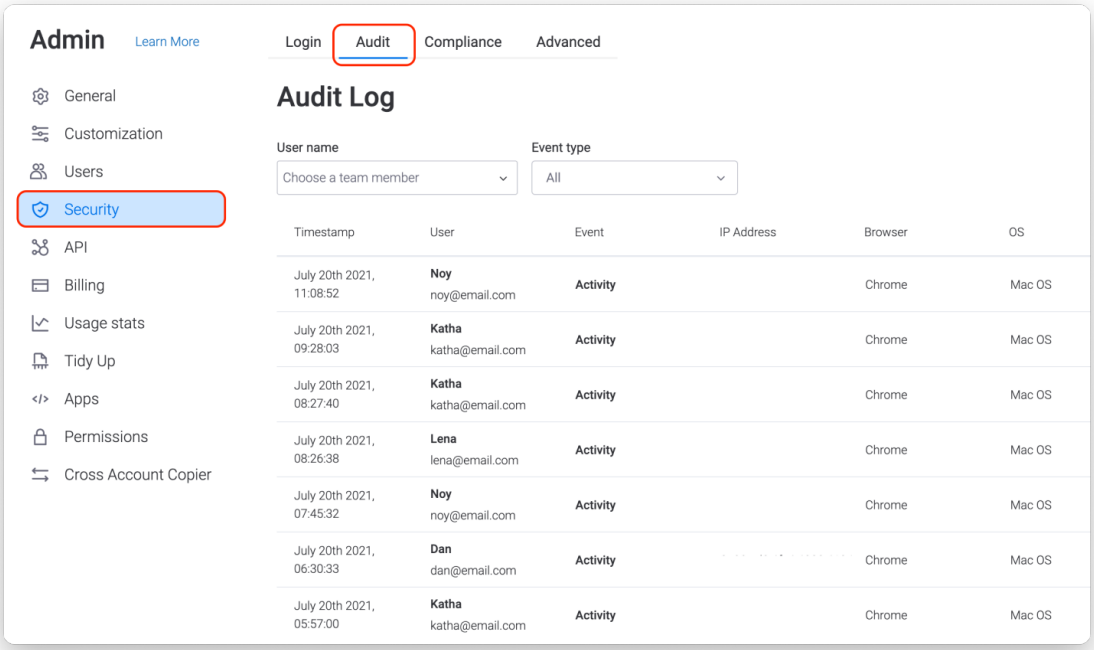

2. El **Registro de actividades de elemento** rastrea todas las actualizaciones de un elemento individual. En el Registro de actividades de elemento puede ver todo el historial relacionado con las actualizaciones de ese elemento y cuándo ocurrieron exactamente. Todas las actualizaciones se ordenan de más recientes a más antiguas. Puede establecer un Recordatorio para cualquier actualización.

Puede exportar fácilmente a Excel el Registro de actividades de elemento o el Registro de actividades de tableros con solo oprimir un botón.

## Registro de auditoría

El Registro de auditoría ofrece a los administradores de cuentas un informe detallado de toda la actividad relacionada con la seguridad de la cuenta. En esta sección, puede ver la última vez que los usuarios ingresaron y salieron de la cuenta, desde qué dispositivo lo hicieron y su dirección de IP de la sesión. De este modo, puede supervisar cualquier actividad sospechosa y activar el modo pánico, de ser necesario.

El registro también muestra eventos de posible vulnerabilidad, como los inicios de sesión fallidos, las descargas de adjuntos y los datos de tablero exportados. Esta función está disponible únicamente para los clientes del Plan Corporativo.




**Interoperabilidad y portabilidad**

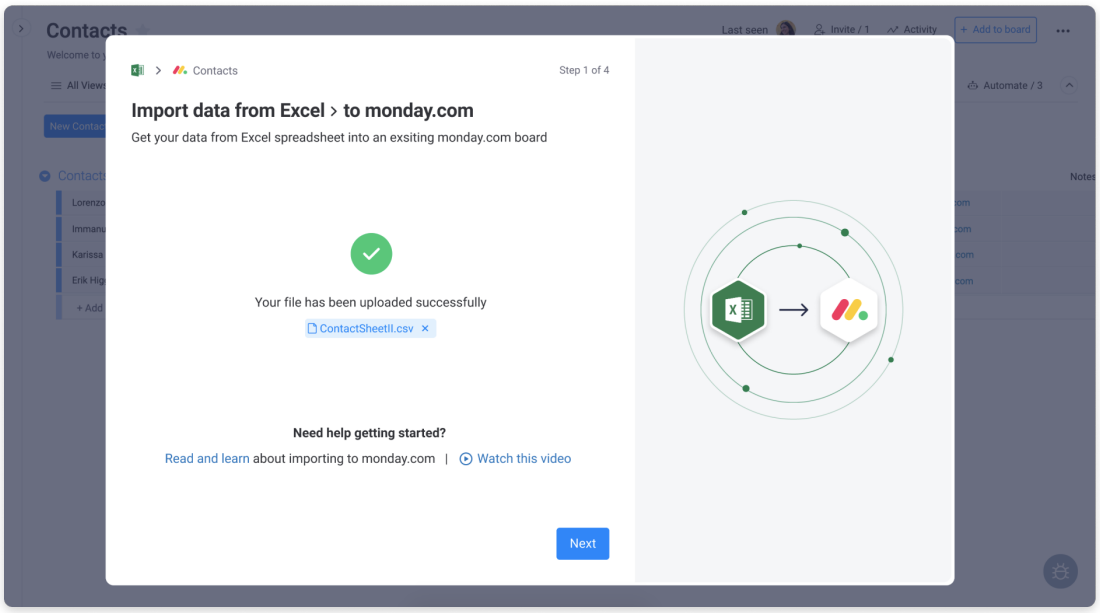
Integración

monday.com admite integraciones a diversas soluciones de software para crear flujos de trabajo personalizados. Puede conectar las herramientas que ya utiliza a monday.com para administrar todo el trabajo de su equipo desde un solo lugar.
Las integraciones son opcionales y se pueden deshabilitar desde el Panel de administrador.

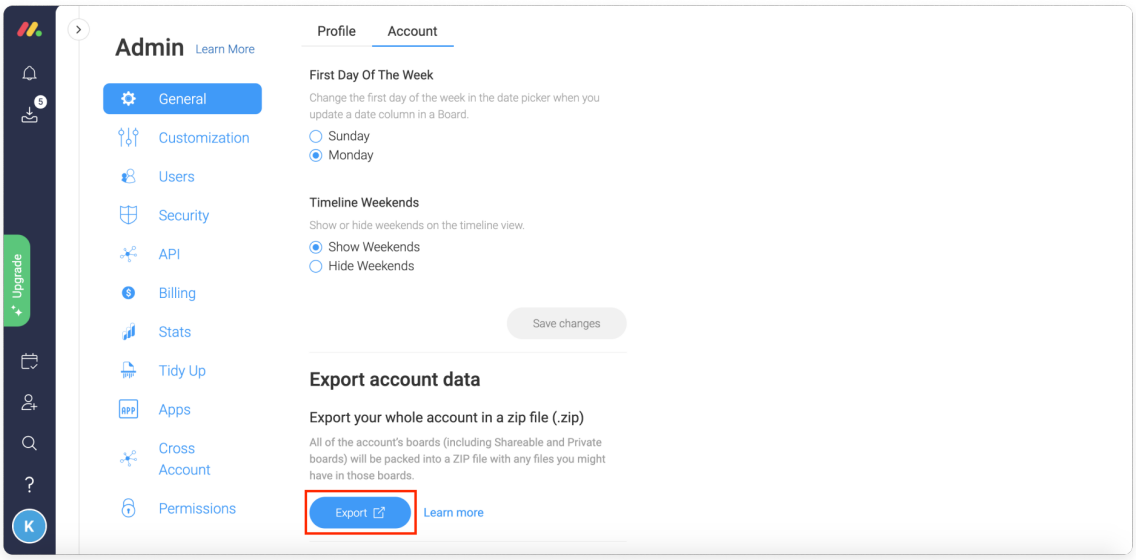
Importación y exportación de Excel

monday.com ofrece a los clientes dos funcionalidades en lo que respecta a la administración de datos:

1. Transformar los datos de una hoja de cálculo de Excel a un tablero de monday.com (nuevo o existente)



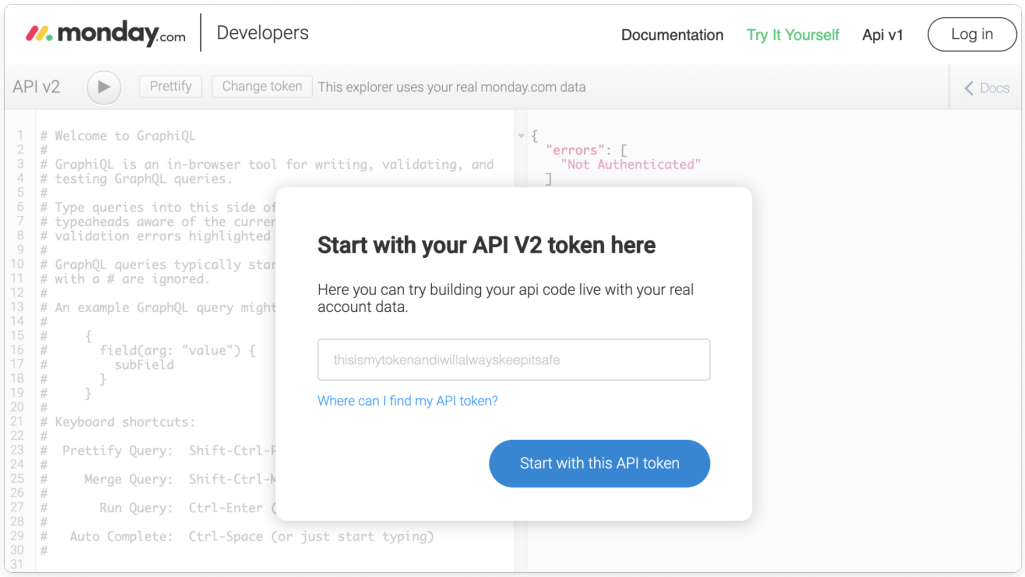

2. Exportar datos monday.com:
    a. Exportar tableros a Excel.
    b. Exportar todos los datos de la cuenta a través del panel de administrador. Se exportará como un archivo zip con las hojas de Excel y los archivos cargados a la cuenta.



## API

monday.com ofrece una API GraphQL. Forma parte del marco de trabajo de las aplicaciones y posibilita que los desarrolladores accedan y actualicen los datos en sus cuentas de monday.com mediante programación.
Los casos de uso de la API incluyen:

- Acceder a los datos del tablero para presentar un informe en el panel de monday.com
- Crear un elemento nuevo en un tablero al generar un registro en otro sistema
- Importar datos de otra fuente mediante programación




## El panel de administrador

En el panel de administrador, los administradores de su cuenta pueden administrar todo, como los ajustes de seguridad, los usuarios de la cuenta, la personalización de la cuenta, la facturación y más.

### Dominio autorizado

Los administradores pueden optar por dos configuraciones:

1. Solo los administradores pueden invitar a miembros y espectadores a la cuenta desde cualquier dominio de correo electrónico.
2. Los administradores pueden determinar un dominio de correo electrónico de donde los usuarios pueden registrarse en la cuenta.

### Bloqueo del dominio de correo electrónico

Los administradores pueden evitar que los usuarios creen nuevas cuentas de monday.com para determinados dominios de correo electrónico. Esta función es especialmente útil para evitar las cuentas de monday.com redundantes dentro de la misma organización; en particular, aquellas que poseen múltiples dominios empresariales, lo cual puede repercutir en el cumplimiento de las normas de gestión de datos empresariales.

Con el fin de bloquear la creación de cuentas, los dominios de correo electrónico se pueden enviar al servicio de monday.com para revisar y verificar su propiedad. Serán dirigidos a los administradores de las cuentas, quienes los incorporarán a la cuenta de la organización principal.
Esta función está disponible únicamente para los clientes del Plan Corporativo.

## Modo pánico

Al activar el modo pánico, su cuenta se bloqueará temporalmente y nadie podrá acceder a ella hasta que el administrador de la cuenta envíe una solicitud a nuestro equipo de Satisfacción del cliente. Esta función es de vital importancia cuando los datos de inicio de sesión de uno de los miembros de su equipo se ven comprometidos.
Esta función está disponible únicamente para los clientes del Plan Corporativo.

## Administración de sesión

En la sección de seguridad del Panel de administración, los administradores pueden hacer clic en la pestaña de sesiones para ver los datos de las sesiones de todos los usuarios, controlar y restablecer cualquier sesión.
Esta función está disponible únicamente para los clientes del Plan v.

## Generación de tokens de API

Solo los administradores pueden otorgar permisos para generar tokens de API GraphQL en su cuenta (para todos, para administradores únicamente o para nadie). De este modo, se evita que los usuarios generen tokens de API y los compartan por error mediante herramientas de terceros o que los expongan públicamente al ponerlos en un repositorio público y vulnerar los datos sensibles de la cuenta. Cuando un usuario no pueda generar tokens recibirá una advertencia.
Esta función está disponible únicamente para los clientes del Plan Corporativo.

## Directorio de contenido

En el directorio de contenido encontrará un panorama general de todos los espacios de trabajo, tableros, paneles, y documentos de trabajo que se encuentran en la cuenta. Además, con cada una de estas funciones, podrá ver los propietarios, los suscriptores, la fecha de creación, la última fecha de actualización y si está disponible o no públicamente para el resto de los miembros de la cuenta.

* Tenga en cuenta que este informe técnico no contiene una lista exhaustiva de las funciones que se pueden gestionar a través del Panel de administración. Encontrará más información en nuestros artículos de soporte.
En los diferentes capítulos de este documento se abordan otras de las funciones que pueden gestionar los administradores de cuenta, como la configuración de inicio de sesión, la autenticación de dos factores, el aprovisionamiento de SCIM, los permisos, la restricción de direcciones IP, las aplicaciones de monday, el registro de auditoría, los tokens API y el cumplimiento con la ley HIPPA.

---

# 4. Seguridad de aplicaciones

### Ciclo de vida de desarrollo de software seguro (S-SDLC)

- monday.com utiliza la metodología de OWASP Top 10, que añade seguridad a nuestro ciclo de vida de desarrollo de software (S-SDLC).
- Todo el código se somete a pruebas de seguridad de tipo estático (SAST) y con revisión de pares como parte del proceso de CI/CD, para garantizar la calidad del código antes de su implementación en la producción.
- Se realizan pruebas de seguridad de aplicaciones dinámicas (DAST) al menos semanalmente.
- Hacemos énfasis especialmente en la preparación de pruebas específicas para las nuevas funciones que se lanzan, mientras que las funciones más antiguas llevan años de evaluación.
- Analizamos y supervisamos de manera continua la vulnerabilidad de nuestra aplicación durante la implementación y después.
- Todas las bibliotecas de terceros del lado del servidor se revisan automáticamente en busca de vulnerabilidades de divulgación pública a través de una herramienta de análisis de composición de software (SCA).

### Firewall de aplicaciones web (WAF)

Se utiliza un firewall de aplicaciones web (WAF) para filtrar, supervisar y bloquear el tráfico a nivel de aplicación, el cual ofrece protección contra los ataques conocidos.

### Gestión de vulnerabilidades

Las vulnerabilidades están centralizadas en un backlog de desarrollo y se clasifican según nuestra evaluación de impacto en la confidencialidad, integridad y disponibilidad del servicio, y de los datos del cliente. El nivel de vulnerabilidad se determina mediante un Sistema común de puntuación de vulnerabilidades (CVSS). Nuestro departamento de investigación y desarrollo (I+D) inicia entonces el proceso de corrección dentro de plazos preestablecidos, en virtud de la gravedad, y de acuerdo con nuestra Política interna de gestión de revisiones.


### Campeones en materia de seguridad

Nuestra comunidad interna de campeones en materia de seguridad está compuesta por desarrolladores de todos los equipos de I+D. Estos campeones reciben formación avanzada en seguridad y están calificados para impartir orientación en seguridad y llevar a cabo revisiones de seguridad del código siempre que sea necesario.

### Pruebas de penetración

Todos los años, un tercero independiente diferente lleva a cabo pruebas de penetración de las aplicaciones, que incluyen métodos de evaluación manuales y automáticos.
Además, nuestro equipo de Seguridad de aplicaciones realiza auditorías de seguridad y pruebas de penetración periódicamente con diversas funciones que requieren de una profunda comprensión de nuestra arquitectura y mecanismos de seguridad interna.
Como parte de nuestras pruebas de penetración internas y externas, se utilizan herramientas de análisis de redes en nuestros servidores de producción.

**Programa de recompensas por errores**


monday.com cuenta con un programa interno y privado de recompensas por errores en HackerOne, que permite que investigadores de seguridad de todo el mundo investiguen e informen de manera ética y responsable las vulnerabilidades en materia de seguridad a nuestro equipo de Seguridad. Determinadas características reciben promociones especiales en HackerOne para que la comunidad de seguridad enfoque sus investigaciones y esfuerzos en estas áreas.

Como parte del programa, contamos con un tablero de puntuación de los más destacados para los hackers.

---

# 5. Seguridad de TI

### Seguridad para endpoints

Todas las estaciones de trabajo de los empleados cuentan con la protección de una solución EDR administrada de forma centralizada, para detectar y aislar el malware. Nuestra solución EDR es supervisada de manera continua por un equipo de SOC gestionado las 24 horas del día, todos los días de la semana, durante todo el año.
Todas las estaciones de trabajo están cifradas con FileVault/BitLocker, protegidas por contraseña y con un tiempo actividad de pantalla establecido en 10 minutos.
Además, podemos aplicar parches y borrar de forma remota una máquina mediante un administrador de dispositivos.

### Política de contraseñas

Nuestra política de contraseñas estipula que las contraseñas deben tener 12 caracteres como mínimo y contener lo siguiente:

1. una letra mayúscula
2. una letra minúscula
3. un número
4. un símbolo

Se utiliza una solución empresarial de gestión de contraseñas, las contraseñas preestablecidas se cambian periódicamente, está técnicamente prohibida la reutilización de contraseñas y el uso de contraseñas comunes y las contraseñas expiran después de los 120 días.

### Administración de accesos e identidades

Nuestro equipo de TI es quien otorga el acceso a los sistemas en virtud de la función, a través de nuestro proveedor de identidades empresariales (IdP), de acuerdo con lo estipulado por el departamento de RR. HH. y de conformidad con los principios de necesidad de divulgación y de privilegios mínimos.
El acceso del usuario se modifica en un plazo de hasta 24 horas después de una modificación en la condición de empleo o la desvinculación. Además, con el fin de garantizar la validez de los privilegios de acceso, se realizan revisiones trimestrales en lo que respecta al acceso de los usuarios. Cualquier acceso que ya no sea necesario se elimina y se documenta.

### Protección del correo electrónico

monday.com usa Google Workspace como nuestro proveedor de servicio de correo electrónico, con protección de retransmisión suministrada por terceros. Se utilizan protocolos DMARC y SPF. Los empleados reciben constantemente instrucción sobre las prácticas más recomendadas para prevenir el phishing y se hacen evaluaciones periódicas.

### Puntos de acceso inalámbrico

monday.com utiliza tecnologías estándar de la industria para garantizar la seguridad de las comunicaciones inalámbricas en nuestras oficinas centrales. Utilizamos WPA2 Enterprise, además de otras herramientas, para garantizar el oportuno desaprovisionamiento y el no repudio en toda la red y para supervisar los puntos de acceso (AP) no autorizados.

# 6. Seguridad funcional

**Acceso a los datos del cliente**
monday.com trata todos los datos que envían los clientes al servicio de monday.com, y que procesamos exclusivamente a nombre del cliente, como si se tratase de una "caja negra"; es decir que monday.com no accede a los datos del cliente para la prestación del servicio; además, tratamos todos los datos que envía el cliente con el máximo nivel de sensibilidad y confidencialidad.
El acceso de monday.com a los datos del cliente está alcanzado por los límites establecidos en los Términos de servicio o en el acuerdo respectivo suscrito con el cliente, según cada caso particular.

**Recursos humanos**
Verificación de antecedentes
Nuestras oficinas centrales se encuentran en Israel, donde la verificación de antecedentes no es habitual y está restringida por la ley. Las verificaciones que realizamos incluyen la revisión de los antecedentes laborales y llamadas para pedir referencias a gerentes directos anteriores.

Contrato de empleo
Todos los contratos de empleo de monday.com contienen cláusulas y disposiciones de confidencialidad que dan lugar a la desvinculación inmediata ante el incumplimiento de determinadas obligaciones y compromisos.
Además, monday.com tiene una política de seguridad de RR. HH. que define las responsabilidades y las actividades de seguridad necesarias durante el periodo del empleo, desde la contratación hasta la terminación de la relación laboral.

Uso aceptable
monday.com tiene una política de uso aceptable que se somete a revisión todos los años por parte del equipo de Seguridad y un Foro de seguridad más amplio. Nuestros empleados deben firmar la aceptación de dicha política al incorporarse a la empresa o al realizarse algún cambio sustancial.

Formación y concienciación
Como parte de su proceso inicial de incorporación, y al menos una vez al año en lo sucesivo, los empleados de monday.com reciben formación en lo que respecta a las obligaciones de seguridad y privacidad de la información que deben observar. La formación incluye tanto tutoriales como trabajos por escrito, y es supervisada por el equipo de Seguridad.
Se destinan Semanas de Seguridad y Privacidad cada tres meses para reforzar la concienciación entre los empleados.
Además, hay sesiones de formación específica según la necesidad (por ejemplo, cuando los desarrolladores reciben formación sobre temas de codificación segura).

Terminación de la relación laboral
El acceso del usuario se modifica en un plazo de hasta 24 horas después de una modificación en la condición de empleo o la desvinculación, además se exige la devolución de los equipos de la

compañía. Con el fin de garantizar la validez de los privilegios de acceso, se realizan revisiones trimestrales en lo que respecta al acceso de los usuarios.

**Pruebas de equipo rojo**
Dos veces al año, realizamos pruebas de equipo rojo sobre nuestra posición de defensa, que incluyen pruebas internas de penetración, ataques a la infraestructura y simulaciones de vulnerabilidad. Las pruebas de equipo rojo las llevan a cabo compañías externas líderes de asesoría en materia de seguridad ofensiva y defensiva, que utilizan técnicas de ataques sofisticadas, de última generación, que nos permiten distinguir de manera exclusiva los posibles riesgos y vulnerabilidades de seguridad.

**Dirección y gestión de riesgos**
monday.com cuenta con un proceso continuo de gestión de riesgos con la finalidad de identificar de manera proactiva las vulnerabilidades en sus sistemas y evaluar las amenazas nuevas y aquellas que puedan surgir contra las operaciones de la compañía. monday.com se somete a una evaluación de riesgos como parte de la certificación ISO 27001, la cual se realiza cada año.

**Respuesta y gestión de incidentes**
El plan de respuesta a incidentes (IRP) de monday.com fija las pautas para la detección de incidentes de seguridad y privacidad, su alcance al personal pertinente, las comunicaciones (internas y externas), la mitigación y el análisis post mortem.
El Equipo de Respuesta a Incidentes (IRT) incluye representantes de Seguridad, I+D, Legales, representantes de otros equipos según cada caso y, de ser necesario, una empresa externa de respuesta a incidentes.

Notificación
De conformidad con los términos de la sección 7 de nuestro Anexo sobre el procesamiento de datos ("Gestión y notificación de incidentes relativos a los datos"), después de tener conocimiento de un incidente con los datos, monday.com notificará a los clientes afectados sin mayor demora.
Se informará a los clientes afectados la naturaleza de la vulnerabilidad, los efectos perjudiciales que monday.com tenga conocimiento, las acciones que monday.com haya implementado y los planes para solucionar o mitigar el incidente al momento de la notificación.

**Recuperación de desastres y continuidad de la actividad**
monday.com cuenta con un plan de continuidad de la actividad en consonancia con la certificación ISO 27001 para hacer frente a los desastres que puedan afectar a nuestra oficina física (donde no se mantiene ninguna parte de nuestra infraestructura de producción).
Además, tenemos un Plan de recuperación de desastres (DRP) para abordar los desastres que pudieran afectar nuestro entorno de producción, el cual incluye el restablecimiento de la funcionalidad central del servicio desde nuestro sitio de específico de recuperación de desastres (DR). Las pruebas se realizan dos veces al año, como mínimo. La prueba de DR de monday.com puede adoptar la forma de un recorrido, un simulacro de desastre o una evaluación de los componentes.

## Retención y eliminación de datos

### Retención de datos

monday.com retendrá aquella información de su propiedad bajo el control de monday.com durante el periodo necesario para cumplir con los objetivos descritos en nuestra Política de privacidad. Los datos que monday.com procese en nombre del cliente se retendrán de conformidad con nuestros Términos de servicio, nuestro Anexo sobre el procesamiento de datos y otros acuerdos comerciales con los clientes en cuestión.

### Eliminación de datos

Los clientes de monday.com tienen todo el control de los datos que envían y pueden modificarlos, exportarlos o eliminarlos en cualquier momento con los medios que tienen disponibles a través de la interfaz de usuario del servicio.
Al finalizar o expirar su suscripción, los clientes pueden solicitar la eliminación de sus datos como parte del proceso de cierre de la cuenta. Los datos del cliente se eliminarán dentro de los 90 días de la solicitud, de los cuales, 30 días se destinan al proceso de reversión y los otros 60 días, al proceso de eliminación.
De forma alternativa, los clientes pueden optar por conservar los datos de la cuenta en la plataforma; en tal caso, podremos mantenerlos como también podremos eliminarlos en cualquier momento a nuestra entera discreción.

### Destrucción de datos

Nuestro servicio se aloja en AWS, y la copia de seguridad de determinados datos se encuentra en GCP. Ambos proveedores de computación en la nube implementan estrategias para la distribución y la eliminación de los datos de propiedad exclusiva que posibilitan el almacenamiento seguro de los datos sensibles en un entorno multiempresa. El retiro de los medios de almacenamiento lo realizan los proveedores mencionados mediante las técnicas detalladas en la publicación 800-88 del NIST.

## Supervisión y registros

monday.com recopila y supervisa los registros de red mediante un sistema de detección de intrusos en la red (NIDS), registros de tráfico desde ubicaciones de borde, registros a nivel de aplicación para monitorear y auditar eventos y registros a nivel de sistema para auditar el acceso y las operaciones con privilegios elevados. Los registros se transmiten a nuestra solución de información de seguridad y gestión de eventos (SIEM), donde un equipo de SOC gestionado los supervisa de forma continua (las 24 horas, todos los días del año).

## Gestión de la cadena de suministros

### Subprocesadores

monday.com exige que sus subprocesadores (tanto en la región de datos a nivel global como en la región de datos de la UE) cumplan con los estándares de la industria en lo que respecta a la seguridad y la privacidad de los datos y considera ambas áreas como críticas al seleccionar a los subprocesadores. Entre otras medidas, nos aseguramos de que todos los subprocesadores dispongan de los Anexos sobre el procesamiento de datos y demás documentos y protecciones pertinentes, y llevamos a cabo evaluaciones en materia legal, de privacidad y de seguridad de la información, además de auditorías mediante cuestionarios; todo de conformidad con los estándares de la industria y los requisitos normativos. Las evaluaciones de los subprocesadores se realizan al menos una vez al año.

Gestión de proveedores

monday.com dispone de un programa central de gestión de repositorio de activos para los servicios y el software que utilizamos. El mantenimiento del repositorio de activos es constante y está a cargo de los equipos de Seguridad, Legales, Privacidad y Contratación; el proceso de aprobación se comunica a todos los empleados.

Al comenzar con la utilización y la renovación de los servicios o del software, los diferentes equipos clasifican a los proveedores con quienes trabajamos según el nivel de datos de más alta sensibilidad, a los efectos de determinar su aptitud para el nivel de riesgo en cuestión y los evalúan según los estándares de la industria y los requisitos normativos.

**Seguridad física**

Oficinas de monday.com

Los activos físicos de TI en las oficinas de monday.com se limitan a equipos portátiles y dispositivos de red de oficina. Los dispositivos de red de oficina están protegidos en una sala de servidores dentro de un entorno controlado, protegidos por contraseña y monitoreados por CCTV las 24 horas, todos los días del año. El acceso físico a las oficinas se controla mediante identificación biométrica. Al ingresar a nuestras oficinas, las visitas son registradas y deben estar acompañadas por un empleado de monday.com en todo momento durante su estancia en la oficina. Todos los empleados deben denunciar cualquier incidente relativo a una actividad sospechosa, el acceso no autorizado a las instalaciones y el robo o la pérdida de pertenencias.

Seguridad del centro de datos

monday.com recurre a las medidas de seguridad físicas y ambientales de primer nivel tanto de AWS como de GCP, lo cual redunda en una infraestructura de alta resistencia. Para obtener más información sobre estas prácticas de seguridad, consulte los siguientes enlaces: https://aws.amazon.com/security/, https://cloud.google.com/security/

---

# 7. Cumplimiento, privacidad y certificaciones

**Garantía de las auditorías y el cumplimiento**
monday.com ha desarrollado sus programas de seguridad y privacidad de conformidad con diversos programas de cumplimiento de la industria, además de las principales normas de privacidad y protección de datos vigentes en los territorios donde se ofrece nuestro servicio:

ISO 27001, 27017, 27018, 27032 y 27701
monday.com cumple con las normas internacionales de la ISO (Organización Internacional de Normalización) y administra la seguridad de la información, el servicio en la nube y la privacidad en virtud de ellas. Todos los años, nos sometemos a una auditoría a cargo de un tercero independiente y contamos con 5 certificaciones ISO:

- **ISO/IEC 27001:2013** es la norma de seguridad mundial más rigurosa en lo que respecta a los sistemas de gestión de seguridad de la información (ISMS).
- **ISO/IEC 27018:2014** determina los objetivos de control comúnmente aceptados, los controles y las directivas para la aplicación de medidas de protección de la información de identificación personal (IIP), de conformidad con los principios de privacidad que estipula la norma ISO/IEC 29100 para entornos de computación en la nube pública.
- **ISO/IEC 27017:2015** establece controles y guías de implementación tanto para proveedores de servicios de nube como clientes de servicios de nube. Fija pautas para los controles de seguridad de la información que rigen para la prestación y el uso de los servicios en la nube, al proporcionar más orientación para la aplicación de los controles pertinentes.
- **ISO/IEC 27032:2012** fija pautas para mejorar el estado de la ciberseguridad, al señalar aspectos exclusivos de la ciberseguridad y su dependencia de otros dominios de seguridad, particularmente la seguridad de la información, la seguridad de la red, la seguridad de internet y la protección de la infraestructura de información crítica (CIIP).
- **ISO/IEC 27701:2019** especifica los requisitos y fija pautas para el establecimiento, la implementación, el mantenimiento y la mejora continua de un Sistema de Gestión de Información de Privacidad (PIMS).

Aquí encontrará todas nuestras certificaciones.

SOC 1, SOC 2 y SOC 3
monday.com ha obtenido los siguientes controles de organización de servicios (SOC):

- Informe **SOC 1 Tipo II**, que analiza los controles que pueden ser interés para los informes financieros de los clientes.
- Informe **SOC 2 Tipo II**, que manifiesta nuestro compromiso con el cumplimiento de las normas más rigurosas de la industria en materia de seguridad, disponibilidad y confidencialidad. Certifica que los controles de monday.com cumplen con los criterios y principios de servicios de confianza del AICPA (Instituto Americano de Contadores Públicos Certificados) y los requisitos de seguridad de la ley HIPAA.

- **Informe SOC 3**, que es una versión resumida de nuestro informe SOC 2 Tipo II y está disponible para el público.

Las auditorías se realizan anualmente y están a cargo de un tercero independiente; además, se emite un informe que abarca de abril a marzo cada año.
Puede acceder a los informes SOC de monday.com a través de los siguientes enlaces: SOC 1, SOC 2 y SOC 3.


## Cloud Security Alliance (CSA)

La Cloud Security Alliance (Alianza de Seguridad en la Nube - CSA) es una organización sin fines de lucro con la misión de "promover el uso de las mejores prácticas a fin de garantizar la seguridad en la computación en la nube y facilitar educación sobre los usos de la computación en la nube para contribuir a la seguridad de todas las demás formas de computación".

monday.com participa en la autoevaluación voluntaria del Registro STAR (Seguridad, Confianza, Garantía y Riesgo) de la CSA para documentar nuestro cumplimiento con las mejores prácticas publicadas por la CSA. Nuestro Cuestionario de la Iniciativa de Evaluaciones de Consenso (CAIQ) completo es gratuito y está disponible para el público en el sitio web de la CSA.

## Ley de Portabilidad y Responsabilidad del Seguro Médico de EE. UU. (HIPAA)

La finalidad de la Ley de Portabilidad y Responsabilidad del Seguro Médico de EE. UU. (HIPAA) es proteger los datos de la atención médica. Las organizaciones como los hospitales, consultorios médicos, planes de salud o compañías que manejan información médica protegida (PHI) debe cumplir con la ley HIPAA. Esto puede extenderse a las compañías que trabajan con dichas entidades y tienen contacto con la información médica protegida en nombre de tales.

monday.com ofrece a los clientes del Plan Corporativo una configuración de cuenta que cumple con la ley HIPAA, de manera que los clientes puedan enviar su información sensible relativa a la salud. Nuestros clientes dentro del marco de la ley HIPAA deben suscribir un Contrato de asociación comercial (BAA) para garantizar la debida protección y tratamiento de la información médica protegida en su nombre, antes de que envíen sus datos relativos a la ley HIPAA.

## monday.com y el Reglamento General de Protección de Datos (GDPR)

Nuestro programa de Privacidad global se enmarca dentro de la normativa de protección de datos más integral y avanzada del mundo, con el Reglamento General de Protección de Datos (GDPR) de la UE y el Reino Unido como "principio rector".

Entre otras cosas, el Foro de privacidad de monday.com supervisa de manera continua el desarrollo de los procesos y productos de toda la organización, como también las distintas actividades relativas al uso de los datos personales con el fin de asegurar la observancia de los

principios del GDPR, que incluyen los principios de privacidad por diseño, la minimización de los datos y la limitación del almacenamiento, la legalidad y la equidad de procesamiento, y la transparencia de nuestras actividades y fines.

## Política de privacidad

En este enlace encontrará la Política de privacidad de monday.com, que describe nuestras prácticas de privacidad y procesamiento de datos en lo que respecta a los datos personales que procesamos para desempeñar nuestro rol como entidad responsable de los datos.

## Anexo sobre el procesamiento de datos (DPA)

Todos los Términos de servicio del monday.com como los contratos de clientes contienen un Anexo sobre el procesamiento de datos que garantiza la protección y el debido procesamiento de los datos personales en nombre del cliente. Puede ver y ejecutar nuestro Anexo sobre el procesamiento de datos (DPA) en línea.

## Transferencias de datos personales al extranjero

Las oficinas centrales de monday.com se encuentran en Israel, con subsidiarias ubicadas en EE. UU., Reino Unido, Australia y Brasil; además, contamos con equipos de soporte en Ucrania y Guatemala. Nuestros subprocesadores también están registrados en distintos países, como se detalla en la página de subprocesadores.

Al transferir datos personales desde el EEE (Espacio Económico Europeo) y el Reino Unido hacia otros países, recurrimos a los mecanismos de transferencias legales que establecidos por el GDPR, como las "decisiones de adecuación" tomadas por la Comisión Europea (es decir, las decisiones que consideran que el Reino Unido e Israel ofrecen un nivel de protección adecuado para los datos personales que se originan en la UE), y las cláusulas contractuales estándar de la UE, que se encuentran aquí y aquí.

## Responsables y procesadores de datos

El GDPR define y distingue dos roles primarios en lo que respecta a la recopilación y el procesamiento de los datos personales: los responsables de datos y los procesadores de datos. Un responsable de datos determina el medio y el propósito del procesamiento de los datos personales, mientras que un procesador de datos es una parte que procesa los datos en nombre del responsable de datos.

- monday.com es una entidad responsable del tratamiento de los datos personales de sus clientes, usuarios y visitas del sitio web. Esto se explica con mayor detalle en nuestra Política de privacidad.
- monday.com es el procesador de los datos personales que los clientes y usuarios envían a la plataforma (en los tableros y los elementos dentro de la cuenta de monday.com), y procesa dichos datos en nombre de los clientes. Esto lo hacemos de conformidad con el Anexo sobre el procesamiento de datos suscrito con el cliente. Nuestros "subprocesadores" son los proveedores externos de servicio con quienes trabajamos para procesar dichos datos.

## monday.com y la ley CCPA

En su capacidad como "proveedor de servicios", monday.com se compromete a cumplir con los requisitos aplicables estipulados en la Ley de

Privacidad del Consumidor de California de 2018 (CCPA) y las regulaciones del fiscal general de California, habida cuenta de regulaciones similares en todo el mundo (como el GDPR) y la evolución de los estándares de la industria; a los fines de garantizar que nuestros clientes puedan continuar utilizando monday.com sin interrupciones y procesar la información personal de los consumidores de California en cumplimiento con la CCPA.
Aquí puede encontrar más información.

La Ley de privacidad de Australia (APA) y los Principios de privacidad de Australia (APP)
La Ley de privacidad de Australia (APA) y los Principios de privacidad de Australia (APP) establecen el marco que rige para recopilar, procesar, utilizar y compartir la información personal, y otorga a los individuos mayor control sobre la manera de manejar su información. monday.com se compromete a cumplir con los requisitos estipulados en la APA y los APP.
Aquí puede encontrar más información.

Auditorías internas
Nuestros equipos de Seguridad, Privacidad, Infraestructura, I+D, TI, Operaciones y Legales destinan Semanas de Seguridad y Privacidad cada tres meses, en las que se llevan a cabo diversas actividades de auditoría, como revisiones de los accesos de usuarios, revisiones de las configuraciones de los firewall, inspecciones de transparencia en el lugar de trabajo, actividades y formación en materia de concienciación, etc.

## Informes a autoridades gubernamentales

monday.com no permite el acceso injustificado a los datos de los clientes bajo nuestro dominio por parte de las autoridades gubernamentales. En muy raras ocasiones las autoridades (de los EE. UU. o de otros lugares) nos solicitan que demos a conocer datos relativos al cliente. En los pocos casos en que hemos recibido tales solicitudes en años anteriores, el alcance era limitado y sobre motivos muy legítimos como para solicitar dichos datos (por ejemplo, ante la sospecha de una actividad ilegal relacionada con una cuenta en particular).
Después de que una solicitud de esa índole haya sido revisada por nuestros equipos de Legales y de Privacidad para garantizar su legitimidad y justificación, la divulgación de los datos se limitará estrictamente a lo que fuera necesario por ley. Recurrimos a todo lo que está a nuestro alcance en materia comercial para notificar a nuestros clientes antes de divulgar cualquier dato, excepto que se nos prohíba hacerlo o que no podamos hacerlo debido a un posible riesgo.[3] Del mismo modo, nos comprometemos a hacer todo lo posible en materia comercial para rechazar, de conformidad con las leyes aplicables, cualquier solicitud de vigilancia masiva relativa a los datos personales protegidos por el GDPR o el GDPR del Reino Unido, incluido lo estipulado en la sección 702 de la ley FISA.

## PrivacyTeam y DPO

monday.com cuenta con la protección de PrivacyTeam, una de las principales firmas de consultoría de privacidad de Israel, con quien trabaja estrechamente para garantizar la protección y la privacidad de los datos del cliente. Aquí puede encontrar más información.
monday.com ha designado al experto en privacidad Aner Rabinovitz, de PrivacyTeam, como responsable de la protección de los datos, para que se encargue de supervisar y asesorar con

[3] Puede encontrar más información en la sección 4 (“Intercambio de datos”) de nuestra Política de privacidad.

respecto al cumplimiento continuo de la privacidad en monday.com, y como punto de contacto en temas de privacidad para los interesados y las autoridades de control.

---

# 8. Epílogo

Este informe técnico ofrece un panorama general del enfoque de monday.com en lo que respecta a la seguridad y la privacidad. Dada la complejidad de estos temas, seguramente tenga otras preguntas e inquietudes.
Puede encontrar más información en nuestro Centro de confianza y en el Portal de legales.
Para más detalles sobre la seguridad de la información o la forma de proteger la privacidad que tiene monday.com, también puede comunicarse con nuestros equipos a través de security@monday.com o dpo@monday.com, además del soporte general disponible las 24 horas, todos los días del año, a través de support@monday.com.
¿Desea denunciar un problema de seguridad o vulnerabilidad? Escríbanos a security@monday.com o envíe un informe a través del formulario de HackerOne, en https://monday.com/security/form/.

DESCARGO DE RESPONSABILIDAD: Esta versión es una traducción del original en inglés que se proporciona solo para fines de conveniencia. El original en inglés es la versión oficial y legalmente vinculante y prevalecerá en caso de discrepancia.