miro

Seguridad y cumplimiento normativo en Miro:

Protección confiable de nivel empresarial

miro

Índice

Resumen

Para sobrevivir, las empresas deben innovar.. Miro les ofrece un espacio de trabajo visual líder que las ayuda a hacer precisamente eso. Más de 180 000 organizaciones innovadoras y exitosas confían en Miro, entre ellas, el 99% de las empresas de la lista Fortune 100, como Google, Cigna, Nike, Ikea, Deloitte y Cisco.

Miro las ayuda a elaborar estrategias y planificaciones, a diseñar productos y servicios centrados en el cliente y mucho más. Sin embargo, para conectar a los equipos y empleados globales, es necesaria una plataforma segura y fiable que les permita trabajar en colaboración con información confidencial. Además, todos los miembros de la organización necesitan el acceso adecuado en el momento adecuado.

En este documento técnico, resumiremos cómo Miro ayuda a las organizaciones a innovar manteniendo como prioridad la **seguridad de la infraestructura de nivel empresarial, el cumplimiento normativo, los controles de seguridad de los productos** y la **privacidad.**

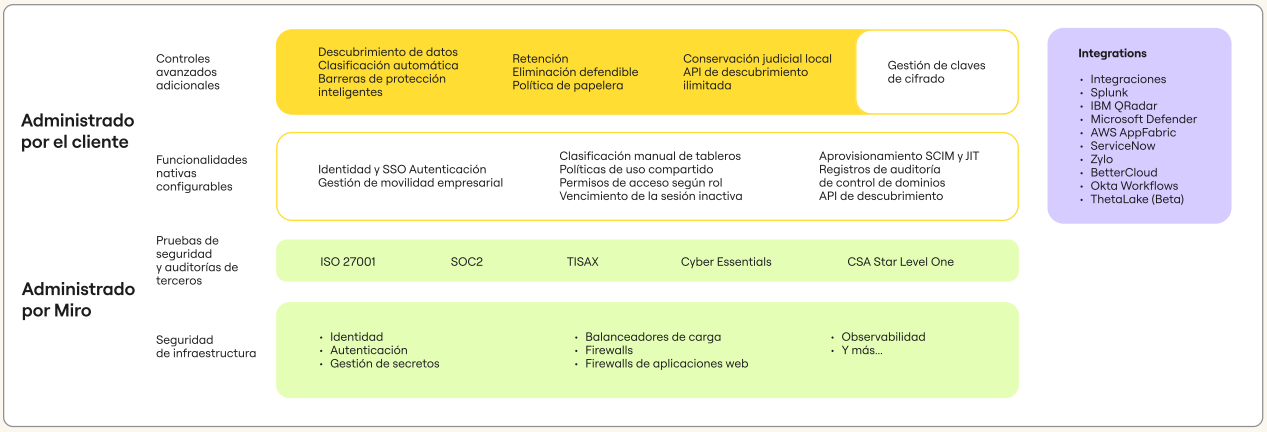
Nuestra responsabilidad compartida

El objetivo de este documento es explicar nuestras áreas de responsabilidad e informar sobre todas las opciones disponibles para reforzar aún más la seguridad de una organización que
usa Miro.

Este diagrama resume nuestro enfoque en materia de seguridad. Las dos capas inferiores son las que Miro controla para garantizar la seguridad de la información y respaldar nuestras obligaciones de cumplimiento normativo. Las dos capas superiores representan las funciones que incorporamos y que se pueden configurar según las necesidades de seguridad y cumplimiento normativo del cliente.

Revisaremos estas características en detalle a lo largo de este documento.

Arquitectura de seguridad y cumplimiento normativo de Miro



Seguridad de la infraestructura

Como plataforma de software como servicio (SaaS) de nivel empresarial, la protección de la información es una parte importante de nuestra postura general en materia de seguridad. Esto incluye recursos tecnológicos físicos, tales como computadoras y sistemas de redes, así como recursos en la nube. Mantener a salvo estos recursos no solo ayuda a protegerse contra los ataques tradicionales de ciberseguridad, sino también contra amenazas físicas como los robos en persona y los desastres naturales. A su vez, protege la información de nuestros clientes.

Centros de datos

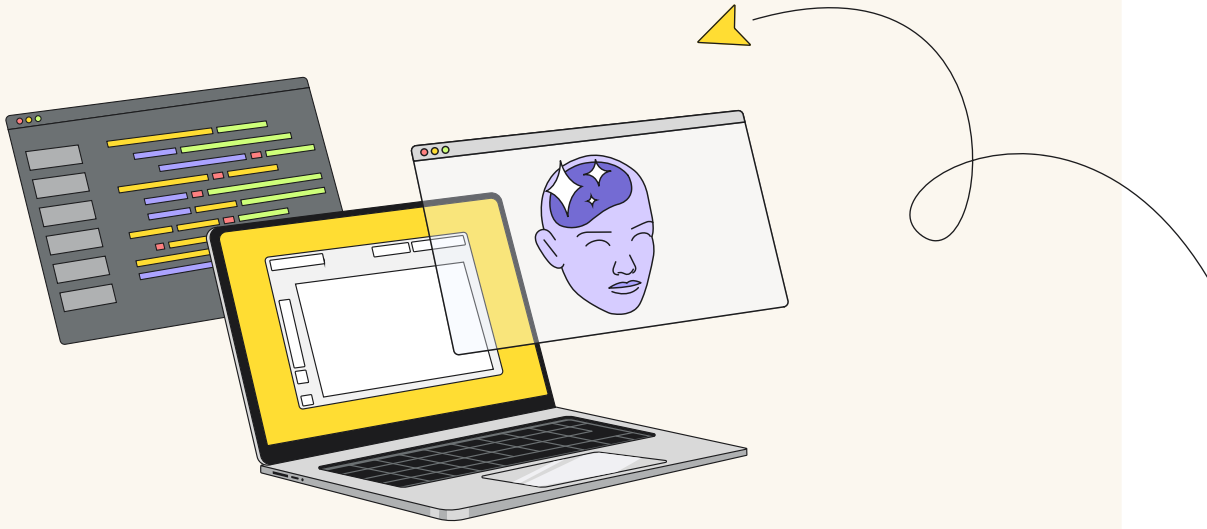
Miro utiliza principalmente Amazon Web Services (AWS) para su infraestructura de informática en la nube y aprovecha las funcionalidades de seguridad de AWS para proteger los datos y las cargas de trabajo alojados. La informática en la nube se basa en un modelo de responsabilidad compartida.

AWS aplica estrictas medidas de seguridad que incluyen diversos controles físicos en los centros de datos, garantías de privacidad de los datos y sólidos controles de sus servicios. Los entornos informáticos de AWS se auditan continuamente y cuentan con certificaciones de organismos de acreditación de distintas áreas geográficas y sectores: SOC 1/SSAE 16/ ISAE 3402 (anteriormente SAS 70), SOC 2, ISO 9001/ISO 27001, FedRAMP, DoD SRG y PCI DSS Nivel 1.

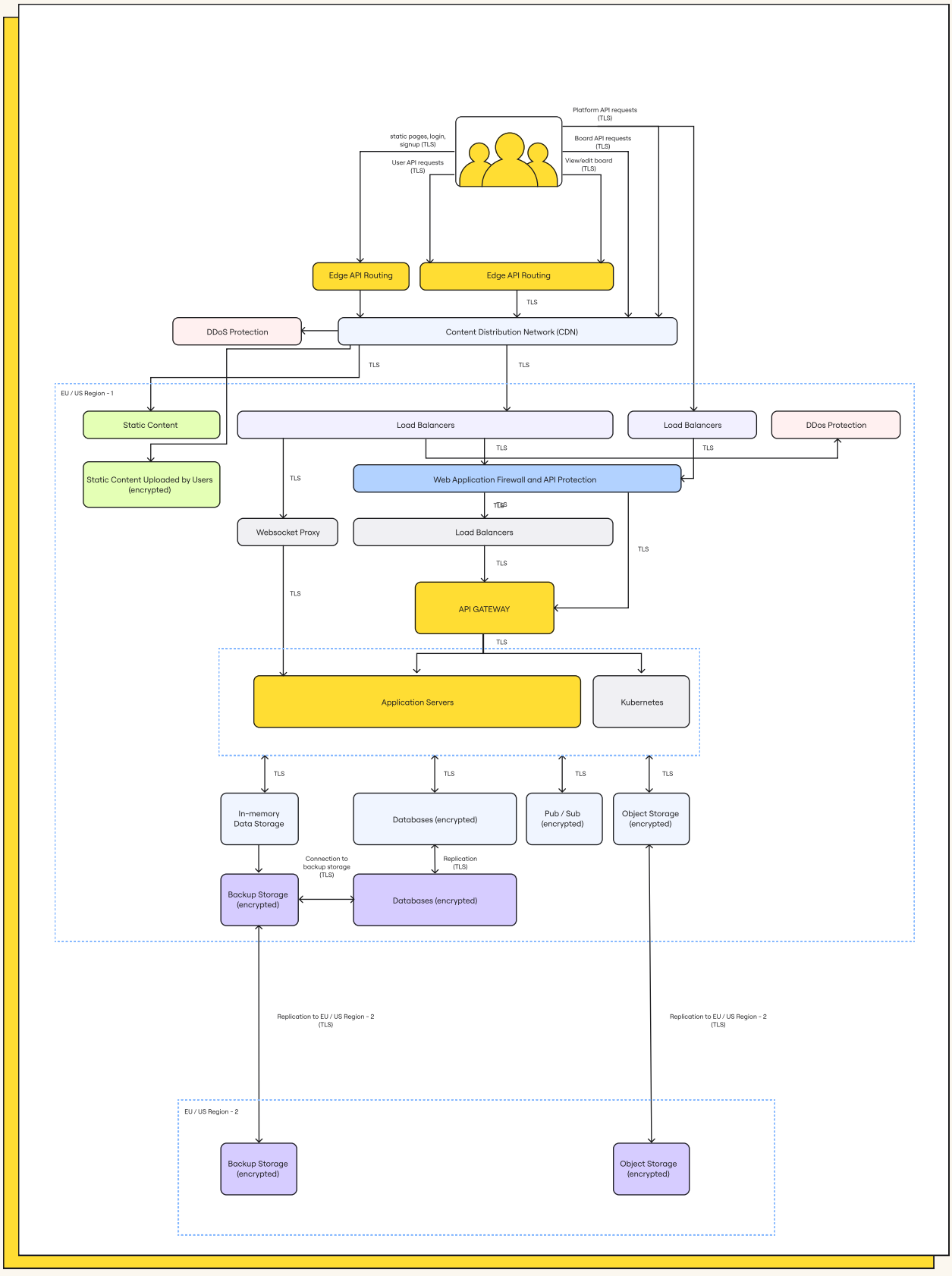
Los sistemas de producción primaria de Miro se alojan en centros de datos de AWS situados en la UE (Irlanda) y EE. UU. (Ohio). Además, se utilizan centros de datos de AWS situados en la UE (Fráncfort) y EE. UU. (Virginia) para guardar las copias de seguridad, y pueden ponerse en funcionamiento de acuerdo con el plan de recuperación ante desastres.

Dentro de la infraestructura en la nube de AWS, Miro es responsable de configurar la seguridad lógica, de la red y de las aplicaciones de la infraestructura en la nube siguiendo las prácticas recomendadas del sector y el marco AWS Well-Architected Framework. Las medidas de protección se aplican siguiendo un enfoque por capas con el principio del menor privilegio y la denegación de manera predeterminada, a menos que se dé permiso expresamente. La gestión y el acceso se limitan estrictamente a determinados empleados y requieren la autenticación multifactor (MFA) y acceso desde dispositivos gestionados mediante una red privada virtual (VPN).

Para obtener más información, consulta la Responsabilidad compartida de AWS.



Flujo de datos en la UE y EE. UU.

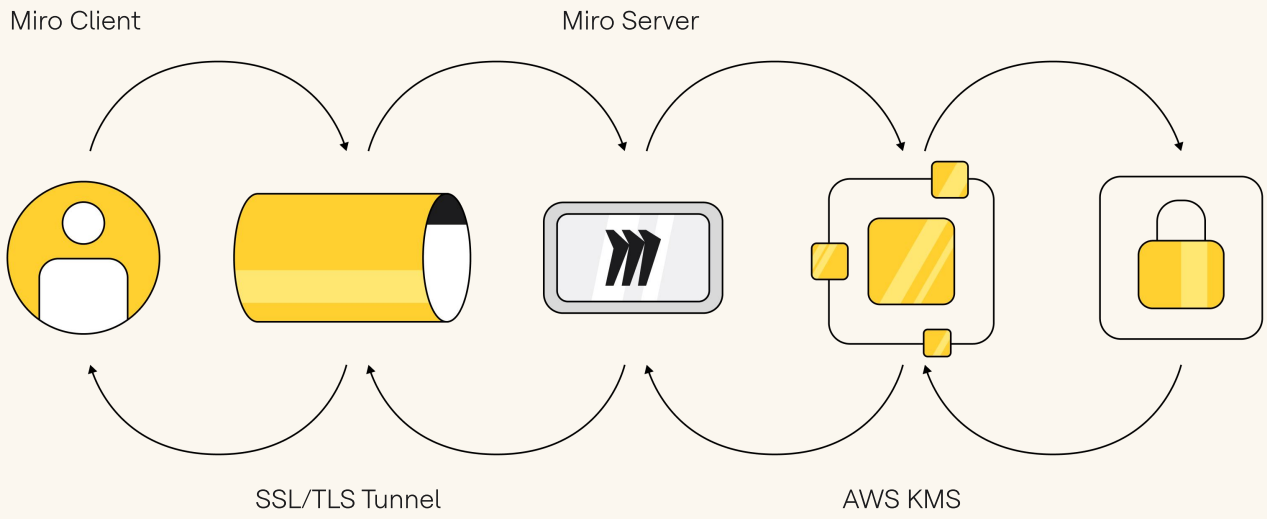


Cifrado de los datos

Para proteger los datos de los usuarios, Miro emplea diversos métodos de cifrado para equilibrar la seguridad de los datos y los requisitos técnicos de nuestros clientes empresariales.

Miro se adhiere a los últimos estándares de cifrado para la protección de los datos, tanto en reposo como en tránsito. Eso significa que Miro admite el cifrado **Advanced Encryption Standard (AES) de 256** bits en reposo y **Transport Layer Security (TLS) 1.3**, además de la versión 1.2, para los datos en tránsito. En conjunto, ayudan a garantizar el cifrado de extremo a extremo en todo el ciclo de vida de los datos

Cifrado en Miro



Para obtener más información, descarga nuestro documento técnico sobre cifrado.

Gestión de claves de cifrado

En el diseño de la infraestructura de gestión de claves de Miro, se han tenido en cuenta los controles de seguridad operativos, técnicos y de procedimiento, con un acceso directo muy limitado a las claves. Los procesos de generación, intercambio y almacenamiento de claves de cifrado se distribuyen para lograr un procesamiento descentralizado. Miro gestiona las claves mediante el servicio AWS Key Management System (KMS) con una clave alojada en su propia cuenta de AWS.

- **Claves de cifrado de archivos:** las claves de cifrado de archivos se crean, almacenan y protegen mediante los controles y las políticas de seguridad de la infraestructura del sistema de producción.
- **Claves SSH internas:** el acceso a los sistemas de producción se restringe con pares de claves SSH únicas. Un sistema interno gestiona el proceso de intercambio seguro de claves públicas y las claves privadas se almacenan de forma segura.
- **Distribución de claves:** Miro automatiza la gestión y distribución de claves sensibles únicamente a los sistemas necesarios para las operaciones. El sistema de distribución de claves se basa en AWS KMS.

Gestión de secretos

Los datos confidenciales, tales como contraseñas, claves API, credenciales de bases de datos y certificados, se almacenan de forma segura en nuestros sistemas de gestión de secretos. El acceso a nuestros sistemas de gestión de secretos solo se autoriza a los servicios que requieren dichos secretos y se limita a un pequeño número de nuestros ingenieros de operaciones.

Control de acceso y autenticación

Los controles técnicos de acceso y las políticas internas de Miro prohíben a los empleados acceder arbitrariamente a los tableros de los usuarios y a otra información sobre las cuentas de los usuarios. Solo un pequeño número de ingenieros responsables del desarrollo de los servicios centrales de Miro tienen un acceso limitado a las tareas de solución de problemas y únicamente con el consentimiento explícito de los usuarios. El personal de soporte de Miro no tiene acceso al contenido de los tableros, a menos que los invite el cliente. Cuando un empleado deja la empresa, pierde inmediatamente el permiso de acceso.

Seguridad de la red

Miro mantiene la seguridad de la red backend con varias capas de protección y defensa, que incluyen grupos de seguridad, proxies, supervisión y comprobación de la seguridad de la red, sistemas de detección de intrusos y auditoría.

El acceso a la red interna del entorno de producción está restringido únicamente a los grupos de usuarios autorizados a través de una VPN mediante el inicio de sesión único (SSO) y MFA, además, se requiere la autenticación de claves en todos los sistemas.

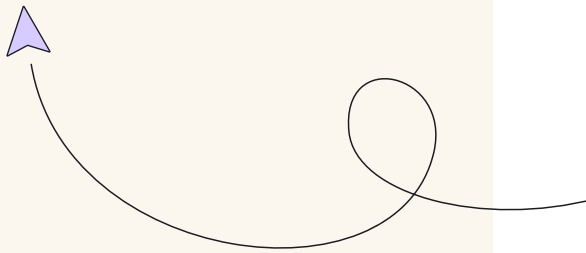
Gestión de vulnerabilidades

El equipo de seguridad de Miro realiza regularmente pruebas de seguridad automatizadas y manuales de las aplicaciones y las infraestructuras para identificar y solucionar posibles vulnerabilidades de seguridad. También se recurre a proveedores de servicios independientes para realizar pruebas de penetración externas anuales, y los problemas identificados se solucionan rápidamente. Nuestro programa público de recompensas por fallos también incentiva a los investigadores de seguridad a enviar cualquier vulnerabilidad que descubran en nuestros productos y servicios.

Gestión de cambios

Miro cuenta con una política formal de gestión de cambios que garantiza que todos los cambios en las aplicaciones se
autoricen antes de su implementación en el entorno de producción y que se cumplan todos los requisitos de seguridad. Los cambios en el entorno de producción de Miro están restringidos al personal autorizado, mientras que el equipo de seguridad se asegura de que las configuraciones del servidor, el firewall y otras relacionadas con la seguridad se mantengan actualizadas según los estándares del sector.

La gestión de la seguridad en la nube nos permite estar al tanto de las amenazas más relevantes en nuestro entorno en la nube y recibir alertas sobre vulnerabilidades o actualizaciones necesarias en nuestra infraestructura en la nube.



Políticas de seguridad

> En Miro, evaluamos los riesgos y mejoramos continuamente la seguridad, confidencialidad, integridad y disponibilidad del servicio. Al menos una vez al año, revisamos y aprobamos nuestras políticas de seguridad (seguridad de la información, ciclo de vida seguro en el desarrollo de software, respuesta a incidentes, acceso lógico y gestión de cambios). Supervisamos también el cumplimiento de dichas políticas, realizamos pruebas de seguridad de las aplicaciones y de la red, y llevamos a cabo evaluaciones de riesgos internas y externas.

Política de empleados y acceso

Cuando las leyes locales lo permiten, los empleados de Miro se someten a una revisión de sus antecedentes penales, firman un reconocimiento de la política de seguridad, se comprometen a respetar la confidencialidad y realizan cursos de formación obligatorios en materia de seguridad para garantizar que se sigan las prácticas recomendadas para salvaguardar los datos de los clientes.

El acceso entre redes está estrictamente limitado al número mínimo de empleados y servicios, y la configuración del firewall está estrictamente controlada y limitada a un pequeño número de administradores. El acceso a otros recursos se concede mediante la aprobación explícita por parte de las personas apropiadas, y los responsables dejan constancia de la solicitud de acceso y su justificación.

Seguridad física

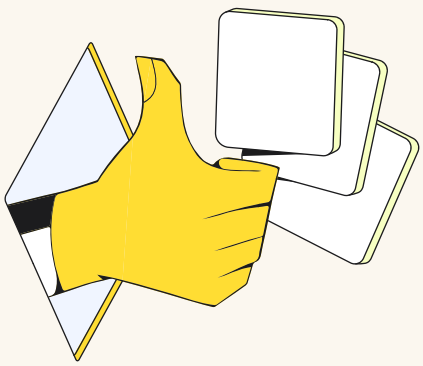
Miro cuenta con un proveedor profesional externo para aplicar su política de seguridad física y supervisar la seguridad de las oficinas corporativas. El acceso físico a las instalaciones corporativas está restringido al personal autorizado de Miro mediante un sistema de acceso con tarjeta de identificación, y un sistema de tarjetas de identificación para visitantes ayuda a garantizar que solo las personas autorizadas puedan acceder a las instalaciones corporativas. El acceso a las áreas que contienen los servidores corporativos está restringido al personal autorizado al que se conceden privilegios elevados a través del sistema de acceso mediante tarjeta de identificación. Las listas de personas autorizadas aprobadas para el acceso físico a la empresa y los entornos de producción se revisan al menos trimestralmente.

Fiabilidad

La infraestructura de servidores de Miro proporciona un almacenamiento de datos seguro y alta disponibilidad. Todos los servicios de aplicación se ejecutan en varios servidores que cuentan con un sistema de balanceo de carga y tolerancia a errores para aumentar la redundancia. Las topologías de clúster se clasifican según el nivel N+1 de alta disponibilidad. Los datos de los usuarios se replican en varias regiones de disponibilidad para su protección, y se cifran y se hacen copias de seguridad de ellos con regularidad. Además, las copias de seguridad diarias de las bases de datos se almacenan separadas del centro de datos principal.

Respuesta a incidentes

El equipo de respuesta a incidentes de Miro está preparado para responder a cualquier incidente de forma ininterrumpida. Las políticas de gestión de incidentes resuelven cuestiones de disponibilidad, integridad, seguridad, privacidad y confidencialidad del servicio. Los procedimientos incluyen respuesta rápida a los incidentes, evaluación de la gravedad, medidas de contención, comunicación con las partes interesadas y actualización del estado en status.miro.com.



Recuperación ante desastres

En caso de crisis o desastre que afecte las operaciones comerciales de Miro, nuestro equipo de infraestructuras sigue un plan de recuperación ante desastres (DRP) que aborda los requisitos de seguridad de la información. Los hallazgos se documentan y se lleva a cabo un seguimiento hasta su resolución. Al menos una vez al año, el equipo revisa y prueba este plan, lo cual incluye la medición del tiempo de recuperación real (RTA).

El plan de recuperación ante desastres resuelve los desastres de durabilidad y disponibilidad. Un desastre de durabilidad se define como una pérdida completa o permanente de los centros de datos primarios, o una pérdida de la capacidad de comunicar o servir datos desde los centros de datos.

El objetivo de tiempo de recuperación (RTO) es el período máximo de recuperación y el nivel de servicio al que un proceso de negocio o servicio se debe restaurar después de un desastre. Un objetivo de punto de recuperación (RPO) es el periodo máximo tolerable en el que podrían perderse datos debido a una interrupción del servicio.

Los planes de Miro para la respuesta a incidentes y recuperación ante desastres se someten a pruebas en intervalos planificados, y en caso de cambios organizativos o de entorno importantes.

Cumplimiento, auditoría y certificaciones

Según el informe sobre el costo de una filtración de datos en 2023 del Ponemon Institute, el incumplimiento de las normas de seguridad es uno de los principales factores que contribuyen a las filtraciones de datos. Por eso, en Miro tomamos muy en serio el cumplimiento de las normas. Miro cuenta con un departamento de seguridad específico dirigido por un responsable de seguridad de la información, que incluye varios equipos de seguridad dedicados al cumplimiento y la gobernanza. El responsable de privacidad de los datos de Miro gestiona y supervisa la privacidad de los datos para ayudar a garantizar el cumplimiento de las normas en cuestiones de privacidad. Asimismo, hay una función de auditoría interna independiente para controlar el cumplimiento de los objetivos y revisar la gobernanza.

Cómo cumple Miro las normas

Miro cumple los requisitos legales de las regiones específicas en las que opera. También somos transparentes sobre las normas de seguridad y privacidad de los datos que seguimos y que protegen los datos de los clientes frente a accesos no autorizados, filtraciones y amenazas.

La auditoría y confirmación de estas certificaciones y normas establecidas nos permiten evaluar nuestro cumplimiento y la eficacia operativa de los controles durante el periodo de auditoría, como el informe de control independiente SOC 2 Tipo II.

Esto incluye:

- **Normas de seguridad de la información** como SOC 2 Tipo II e ISO/IEC 27001.
- **Normas de transferencia de datos,** basadas en una solución de residencia de datos en la UE líder en su categoría, y en el uso de cláusulas contractuales estándar para proporcionar un nivel adecuado de protección de los datos fuera de la UE y el Reino Unido que respalde la adhesión al Reglamento General de Protección de Datos (RGPD).
- **Certificaciones regionales y específicas del sector,** como Cloud Security Alliance, Cyber Essentials y TISAX.
- **Auditorías externas periódicas** realizadas por las mejores empresas del sector, como el Instituto Británico de Normalización (BSI).
- **Lineamientos de accesibilidad** y un informe de conformidad de accesibilidad (ACR) basado en VPAT.

Cómo protege Miro los datos personales de los clientes

Las leyes y normas sobre privacidad y protección de los datos, como el RGPD en Europa, cada vez son más estrictas e imponen obligaciones rigurosas sobre la manera en que las organizaciones recopilan, procesan, transfieren y almacenan los datos de los usuarios. El incumplimiento de estas normas puede acarrear cuantiosas multas, el escrutinio de los organismos reguladores y la pérdida de confianza de los clientes, lo que podría paralizar un negocio de SaaS.

El programa de privacidad y protección de datos de Miro gira en torno a las prácticas establecidas del sector y se centra especialmente en proteger los datos personales de los clientes mediante la conducta de los empleados y el diseño de los productos. Los empleados deben cumplir las normas de protección de los datos, comprometerse a la confidencialidad y están sujetos a limitaciones técnicas (consulta la Política de empleados y acceso). Los procesos de diseño de los productos de Miro incluyen puntos de control normativos y revisiones legales, y los equipos de producto e ingeniería reciben formación periódica sobre los estándares de diseño.

La Política de Privacidad de Miro establece de forma explícita y transparente las categorías de datos personales que Miro trata como responsable del tratamiento, junto con la finalidad comercial establecida. También describe las categorías de terceros que Miro contrata para tratar los datos personales y explica los procedimientos que los particulares pueden seguir para ejercer sus derechos, según lo que establece la ley de protección de los datos y el mecanismo de transferencia de datos en el que Miro se basa para transferir datos personales fuera de la UE.

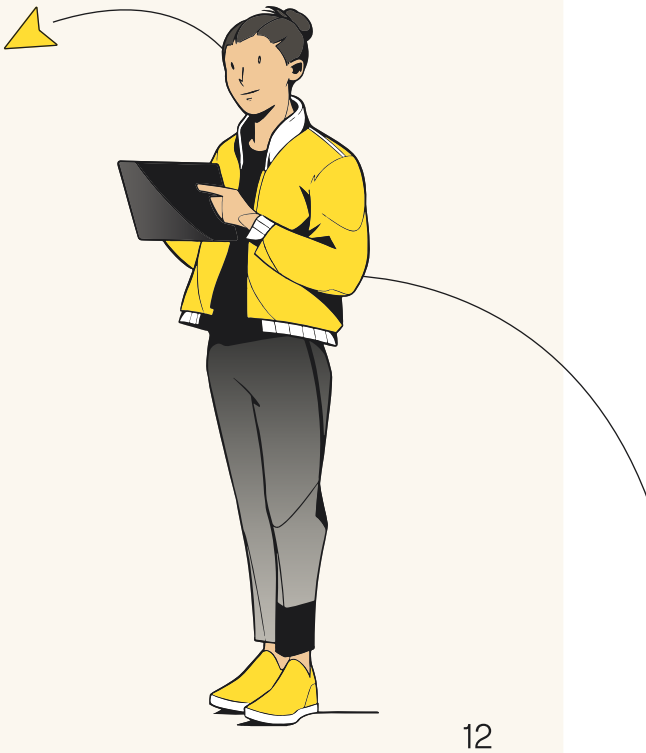
Cuando Miro procesa datos personales en nombre de su cliente o transfiere datos personales de clientes fuera de la UE, aceptamos establecer los términos adecuados, por ejemplo, en nuestro Anexo de Tratamiento de los Datos (DPA), que incluye los compromisos contractuales exigidos por el RGPD, la Ley de Privacidad del Consumidor de California (junto con su modificación a través de la Ley de Derechos de Privacidad de California) y otras leyes de privacidad y protección de los datos estadounidenses y mundiales.

Tratamiento de los datos por parte de terceros

En la medida en que Miro contrate a terceros para tratar los datos personales de los clientes, exigimos un estricto proceso de contratación que incluya comprobaciones legales y de seguridad, y un acuerdo con las condiciones adecuadas de tratamiento y transferencia de los datos. En su anexo de tratamiento de los datos (DPA), Miro incluye un enlace a la lista de dichos terceros disponible online, e informa a los clientes sobre su intención de cambiar o añadir terceros relevantes a dicha lista según el proceso establecido en el DPA.

Seguridad del producto

Miro es una plataforma en la nube a la que se puede acceder desde un navegador web, tanto en ordenadores como en dispositivos móviles, o mediante aplicaciones específicas para ambas plataformas. Debido a estos puntos de contacto y a la naturaleza de la colaboración remota y distribuida a través de una plataforma como Miro, debemos ayudar a los clientes a trabajar con una arquitectura de confianza cero (ZTA). Esto significa no solo capacitar a nuestros clientes para que cuenten con las soluciones de seguridad adecuadas, sino también ayudarlos a garantizar que se implementen correctamente.



Arquitectura de confianza cero

A diferencia de los modelos de seguridad tradicionales, que conceden un acceso amplio según la ubicación del usuario o el punto de entrada a la red, la ZTA asume que las amenazas pueden originarse en cualquier lugar, incluso dentro de la organización. Esto es cada vez más importante en el entorno laboral moderno, en el que los empleados acceden a los recursos corporativos desde distintos lugares y dispositivos. La ZTA aboga por la verificación continua de la identidad, la seguridad de los dispositivos y el cumplimiento de las políticas de seguridad en cada interacción del usuario con los datos y los recursos.

Miro ayuda a las organizaciones empresariales a abordar la ZTA y proporciona a los administradores las herramientas que necesitan para establecer las políticas adecuadas con permisos y controles detallados, sin comprometer la capacidad de colaboración de los equipos. Estos controles de seguridad incluyen:

- **SSO:** con el Inicio de Sesión Único (SSO) basado en SAML, los usuarios pueden acceder a Miro mediante un proveedor de identidad (IdP) de su elección, como Okta, Azure AD, AuthO o Google SSO, entre otros. De esta manera, los usuarios no tienen que introducir repetidamente sus credenciales para cada aplicación, lo cual les ahorra tiempo y reduce el número de superficies de ataque.

- **2FA:** la Autenticación de Doble Factor (2FA) funciona en Miro sin necesidad de SSO y añade una capa extra de protección cuando los usuarios acceden a la suscripción a Miro de su organización. La 2FA se aplica a todos los usuarios que inicien sesión con su correo electrónico y contraseña (colaboradores externos para empresas con SSO o todos los usuarios en organizaciones que no tengan configurado SSO). Los usuarios pueden configurarlo en su perfil, o los administradores de la empresa pueden habilitar la 2FA para toda una organización. Miro aplica la 2FA mediante la aplicación de una contraseña temporal de un solo uso (TOTP), como Microsoft Authenticator, Google Authenticator y Authy.

- **Tiempo de espera de la sesión inactiva:** establece el tiempo máximo que los usuarios pueden estar inactivos antes de la sesión se cierre automáticamente. Este límite reduce al mínimo el periodo de tiempo en que un atacante puede intentar robar y utilizar la sesión de un usuario existente (ya sea de forma remota o en persona en una estación de trabajo desatendida).

- **Acceso basado en roles para administradores:** hay varios roles de administradores que pueden asignarse a los usuarios para llevar a cabo sus flujos de trabajo (por ejemplo, administrador de empresa, administrador de usuarios, administrador de contenidos), cada uno con niveles específicos de privilegios de acceso, ajustes y configuraciones. De esta manera, la carga de trabajo de administración se distribuye de forma segura y se evita que los administradores tengan privilegios innecesarios o acceso a información sensible.

- **Políticas sobre el uso compartido:** decide cuándo y cómo debe accederse al contenido de tu organización y establece políticas para:
  - Restringir el uso compartido fuera de los dominios permitidos.
  - Restringir el uso compartido mediante enlaces públicos.
  - Exigir contraseñas para los tableros públicos (a nivel de empresa).
  - Restringir el uso compartido con todos los equipos y con toda la empresa (a nivel de equipo).
  - Restringir la capacidad de mover tableros a otros equipos (a nivel de equipo).
  - Restringir el uso compartido de plantillas de clientes con toda la empresa.

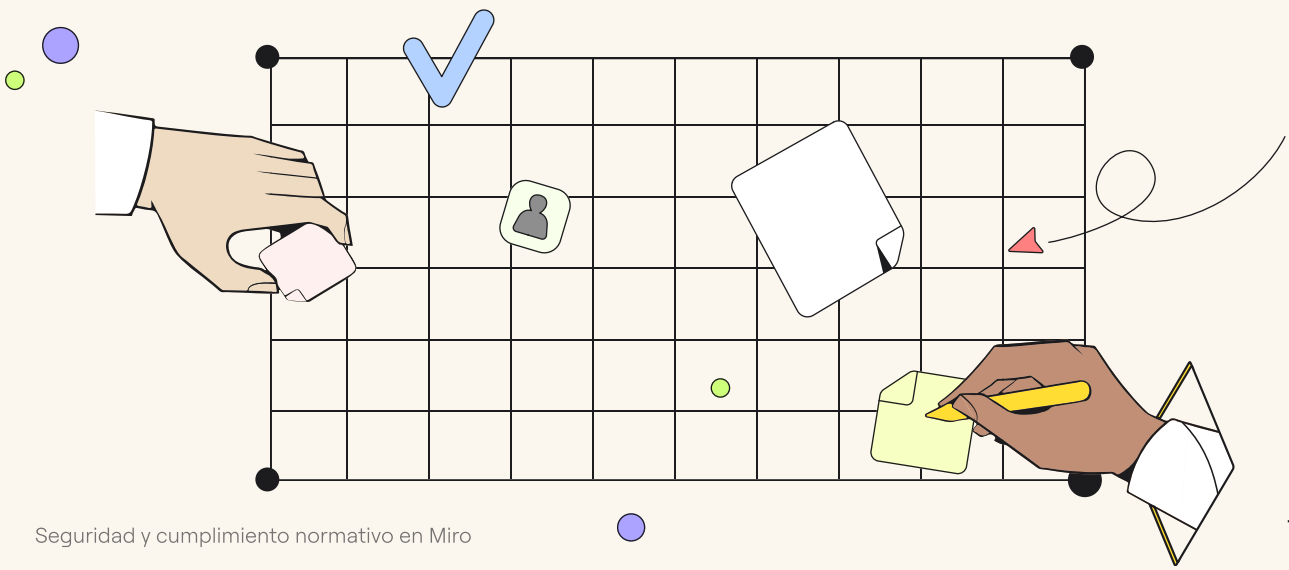
- **Gestión de la movilidad empresarial:** os administradores de la empresa pueden ver toda la actividad de su organización. Los registros ayudan a solucionar problemas y a generar informes detallados de los eventos importantes, como cambios en la configuración global de seguridad, invitaciones de nuevos usuarios o creación de nuevos tableros.

- **Registros de auditoría:** Unternehmens-Admins können alle Aktivitäten innerhalb ihrer Organisation einsehen. Protokolle helfen bei der Fehlerbehebung oder wenn ein detaillierter Bericht über wichtige Ereignisse erforderlich ist, z. B. Änderungen an globalen Sicherheitseinstellungen, Einladungen neuer Nutzer oder die Erstellung von neuen Boards.

- **Clasificación:** los usuarios del plan Enterprise pueden asignar etiquetas de clasificación al contenido de su tablero para indicar el nivel de confidencialidad. Las etiquetas predeterminadas pueden configurarse por empresa o por equipo, y los usuarios pueden utilizarlas para filtrar los tableros en su panel.

- **Gestión del ciclo de vida del contenido:** en Miro, los usuarios pueden filtrar por empresa para facilitar la gestión del ciclo de vida de los tableros de las empresas. Además, se puede acceder fácilmente a un menú de papelera global donde se pueden recuperar o borrar permanentemente los tableros eliminados.

- **Administración:** la automatización desempeña un papel fundamental en la prevención de errores y ahorra tiempo cuando se trabaja con cientos de miles de tableros y usuarios. El aprovisionamiento SCIM o JIT automatiza el acceso de los usuarios y agiliza la gestión de su ciclo de vida.



Inteligencia artificial

La IA en Miro se trata con el mismo cuidado y atención a la seguridad que en el resto del producto. Los principios y las prácticas que guían nuestra aproximación a la IA demuestran nuestro compromiso con el desarrollo ético y responsable de la IA, con el fin de mantener la confianza de clientes, usuarios y colaboradores.

Esto incluye la responsabilidad mediante modelos transparentes de IA. Utilizamos los datos únicamente como se indica en nuestra Política de Privacidad o como se acuerde expresamente entre Miro y el cliente. Los clientes mantienen el control total sobre sus contenidos. Para ello, les permitimos decidir si desean participar o no en los servicios de IA. Obtén más información en nuestro documento técnico.

Integraciones del ecosistema Enterprise

Los clientes del plan Enterprise pueden aprovechar diversas integraciones de seguridad y cumplimiento normativo, como soluciones de administración de información y eventos de seguridad (SIEM), agentes de seguridad de acceso a la nube (CASB), EMM, plataformas de integración, herramientas de gestión de recursos de software (SAM) y automatización del flujo de trabajo. Las empresas también pueden desarrollar sus propias integraciones.

Integraciones de nivel empresarial

miro | ENTERPRISE GUARD

Miro Enterprise Guard: Complemento avanzado de seguridad y gobernanza de datos

El trabajo que se lleva a cabo en Miro suele ser estratégico y requiere gobernanza. Los clientes utilizan cada vez más Miro para crear y almacenar datos confidenciales y privados, y a pesar de las políticas de la empresa, la información sensible puede aparecer donde menos lo esperas. Además, la cantidad de contenido de nuestros mayores clientes en los tableros de Miro se multiplica por 2,5 cada año, lo que aumenta aún más la superficie de riesgo para la seguridad y la gobernanza de los datos.

Las principales funciones de seguridad de las aplicaciones SaaS empresariales, como la autenticación y el SSO, así como los controles de acceso detallados, dan a la mayoría de los clientes control suficiente sobre cómo y cuándo se protegen sus datos. Sin embargo, debido al carácter estratégico de Miro para su negocio o a los requisitos de cumplimiento normativo de su sector, o a una combinación de ambas cosas, algunos clientes quieren capas de protección adicionales a nuestras medidas de seguridad estándar.

Ahí es donde entra Miro Enterprise Guard, un complemento avanzado de seguridad y gobernanza de datos.

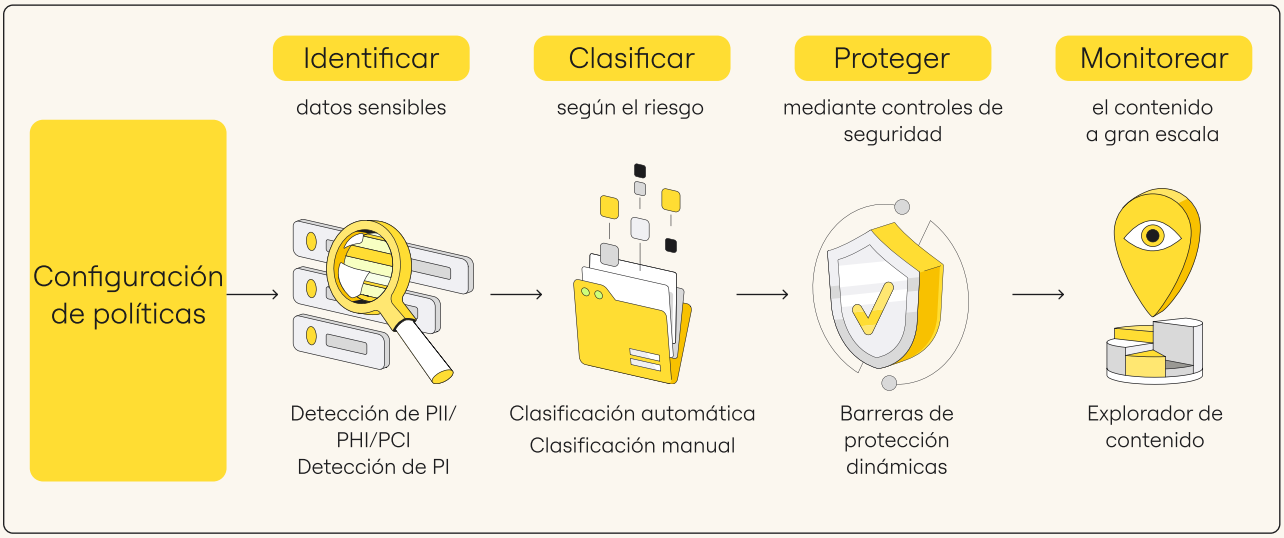
[1] Crecimiento acumulado de tableros en más de 1000 organizaciones suscritas al plan Enterprise entre 2017 y 2023

Identifica, clasifica y protege los datos sensibles

Enterprise Guard automatiza el proceso de búsqueda y clasificación de datos sensibles en Miro y ofrece mayores controles de seguridad de los datos. Enterprise Guard puede hacer lo siguiente:

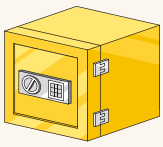
- Escanear tus tableros de Miro para **identificar y clasificar datos sensibles** como PII, PCI o PHI, así como información crítica para el negocio para que puedas conservarla, eliminarla o corregirla.
- Aplicar **etiquetas de clasificación automáticamente** a los datos que se encuentran, basándose en criterios predefinidos que puedes establecer en Miro o en otras herramientas de seguridad de datos mediante integración.
- Aplicar **barreras de protección inteligentes** de acuerdo con las etiquetas de clasificación del tablero. Las barreras de protección inteligentes son controles dinámicos que estableces según tu política, que pueden impedir determinadas acciones de los usuarios, como copiar y pegar, compartir públicamente y exportar tableros.
- También puedes consultar una vista unificada de todos los tableros de Miro con datos sensibles y las etiquetas de clasificación de cada tablero con el **explorador de contenido**. Te da más visibilidad sobre lo que se debe proteger y controles precisos para hacerlo, a la vez que apoyas la colaboración en toda tu organización.

Adaptar la seguridad al riesgo

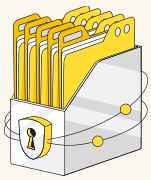


Gestionar el ciclo de vida del contenido a escala

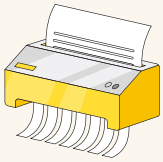
Enterprise Guard automatiza el proceso de gestión del ciclo de vida de tus tableros para ayudarte a satisfacer los requisitos de cumplimiento normativo o de las políticas de la organización.
Con estas funciones puedes hacer lo siguiente:



Conservar tableros según políticas específicas, con registros de auditoría completos.



Eliminar tableros según políticas específicas, con restauración de los registros de auditoría completos.



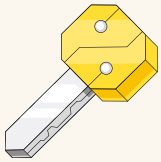
Definir la política de papelera de la organización para mejorar el control sobre el borrado y la retención permanentes y defendibles de tu tablero de Miro

Gestión de claves

Como parte del paquete adicional Enterprise Guard también se incluye la opción para habilitar la **gestión de claves de cifrado (EKM)**. Esto te proporciona un control completo e independiente sobre tus claves de cifrado gracias a AWS KMS.

Asimismo, se obtiene más visibilidad de auditoría y un mayor control del acceso a datos tales como nombres de cuenta, nombres de proyecto y contenido generado por el usuario, incluidos widgets, comentarios y archivos cargados.

Además, los clientes que aportan su propia clave ("BYOK") pueden auditar el uso de las claves con los registros de todas las llamadas a la API que se hicieron relacionadas con ellas para ayudar a satisfacer los requisitos de cumplimiento y normativos.



Gestión de claves de cifrado (EKM)

Conclusión

La mayoría de los directivos están descontentos con la capacidad de su organización para innovar y competir. De hecho, el 82% de ellos cree que una empresa se extinguirá en cinco años si no logra innovar. Algunos de los mayores obstáculos a la innovación son los retos tecnológicos, como las herramientas anticuadas y heredadas. Tanto los ejecutivos como los trabajadores de la industria están de acuerdo en que la tecnología heredada ahoga la creatividad e impide la productividad. Por eso, muchas organizaciones se han apresurado a implementar herramientas de colaboración sin tener plenamente en cuenta las implicaciones para la seguridad.

Con un espacio de trabajo de colaboración visual como Miro, innovar es fácil y seguro. Nos hemos comprometido a proteger la seguridad y los datos de nuestros clientes, los más de 60 millones de usuarios en todo el mundo, incluido el 99% de la lista Fortune 100, quienes confían a Miro su activo más valioso: su información. Únete a estas empresas líderes y aprovecha las ventajas que ofrece un espacio de trabajo de innovación colaborativa, sabiendo que puedes confiar en todo momento en que tus datos estarán seguros y protegidos.

Comunícate con nuestro equipo de Ventas para obtener más información.

Ressources

Miro Trust Center
Documento técnico sobre cifrado
Residencia de datos en Miro
Preguntas frecuentes sobre seguridad y cumplimiento normativo (Centro de ayuda)
Informe anual de transparencia
Política de Privacidad
Condiciones del Servicio
Plan Enterprise de Miro
Lineamientos de accesibilidad

Miro es un espacio de trabajo visual que ofrece a equipos de cualquier tamaño y en ubicaciones diversas la posibilidad de hacer realidad su próxima gran idea. La plataforma ofrece un lienzo infinito que permite a los equipos organizar talleres y reuniones interesantes, diseñar productos, crear lluvias de ideas y mucho más. Miro, con sedes conjuntas en San Francisco y Ámsterdam, presta servicio a más de 60 millones de usuarios en todo el mundo, incluido el 99% de empresas de la lista Fortune 100. Miro se fundó en 2011 y actualmente cuenta con más de 1800 empleados en 12 centros repartidos por todo el mundo.

miro

Para obtener más información, visita miro.com.

Plan Enterprise de Miro
https://miro.com/enterprise/

Blog de Miro
https://miro.com/blog/

LinkedIn
https://www.linkedin.com/company/mirohq/

X (antes Twitter)
https://twitter.com/MiroHQ