miro

Segurança e Conformidade na Miro

Proteção de nível empresarial em que você pode confiar

miro

Índice

Visão geral

As organizações corporativas precisam inovar para sobreviver, e é exatamente isso que a Miro ajuda a fazer. Consolidada como o principal espaço de trabalho visual para inovação, a Miro conta com a confiança de mais de 180.000 organizações inovadoras de sucesso, incluindo 99% das empresas listadas na Fortune 100, como Google, Cigna, Nike, Ikea, Deloitte e Cisco.

Com a Miro, essas empresas podem criar estratégias, planejar e projetar produtos e serviços centrados no cliente e muito mais. No entanto, conectar times e funcionários globais requer uma plataforma segura e confiável para colaborar com informações confidenciais. Além disso, todos na organização precisam do acesso adequado quando necessário.

Neste informe técnico, resumiremos como a Miro ajuda as organizações a inovar, tendo como prioridade a **segurança de infraestrutura de nível empresarial, conformidade, controles de segurança de produtos** e **privacidade.**

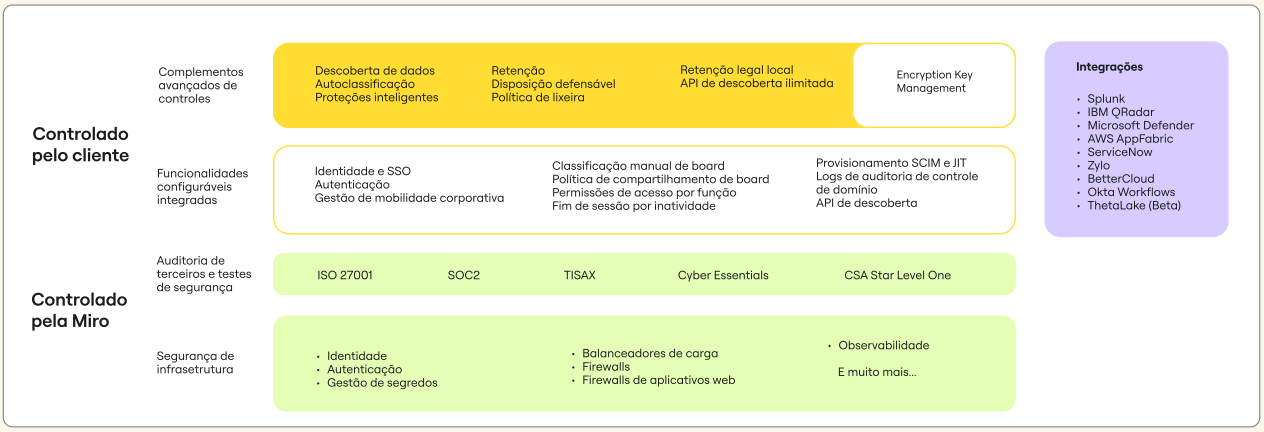
Nossa responsabilidade compartilhada

O objetivo deste informe é explicar nossas áreas de responsabilidade e apresentar todas as opções disponíveis, para reforçar ainda mais a postura de segurança da sua organização ao
usar a Miro.

Este diagrama resume como abordamos a segurança. As duas categorias inferiores representam o que a Miro controla, para garantir a segurança das informações e respaldar nossas obrigações de conformidade. As duas categorias superiores representam os recursos que criamos e que você pode configurar com base em suas necessidades de segurança e conformidade.

Analisaremos esses recursos detalhadamente neste informe.

Arquitetura de segurança e conformidade da Miro



Segurança da infraestrutura

Por ser uma plataforma de Software como um Serviço (SaaS) de nível empresarial, proteger as informações é uma parte fundamental de nossa postura geral de segurança, e inclui ativos de tecnologia físicos, como computadores e sistemas de rede, bem como recursos de nuvem. Manter esses ativos seguros ajuda a proteger não somente contra os tradicionais ataques de segurança cibernética, mas também contra as ameaças físicas, como roubo presencial e desastres naturais. Desse modo, protegemos as informações de nossos clientes.

Data centers

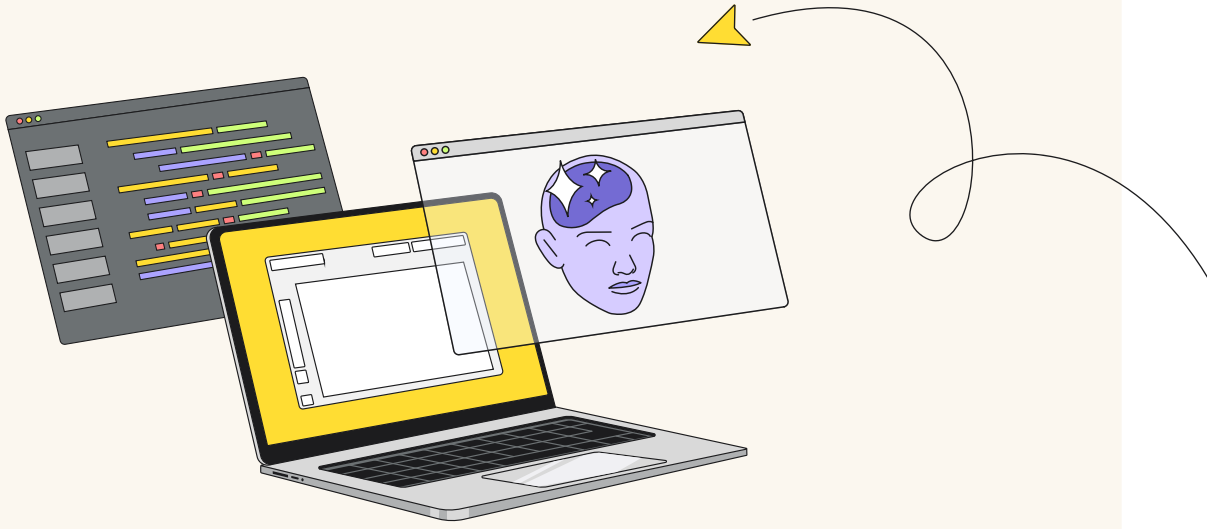
A Miro usa principalmente a Amazon Web Services (AWS) para sua infraestrutura de computação em nuvem e aproveita os recursos de segurança da AWS para proteger os dados e cargas de trabalho hospedados. A computação em nuvem se baseia em um modelo de responsabilidade compartilhada.

A AWS implementa medidas de segurança rigorosas, que incluem uma variedade de controles físicos dos data centers, garantias de privacidade de dados e controles robustos de seus serviços. Os ambientes de computação da AWS são continuamente auditados, com certificações de organismos de credenciamento em todas as regiões geográficas e verticais, incluindo SOC 1/SSAE 16/ISAE 3402 (anteriormente SAS 70), SOC 2, ISO 9001 / ISO 27001, FedRAMP, DoD SRG e PCI DSS Nível 1.

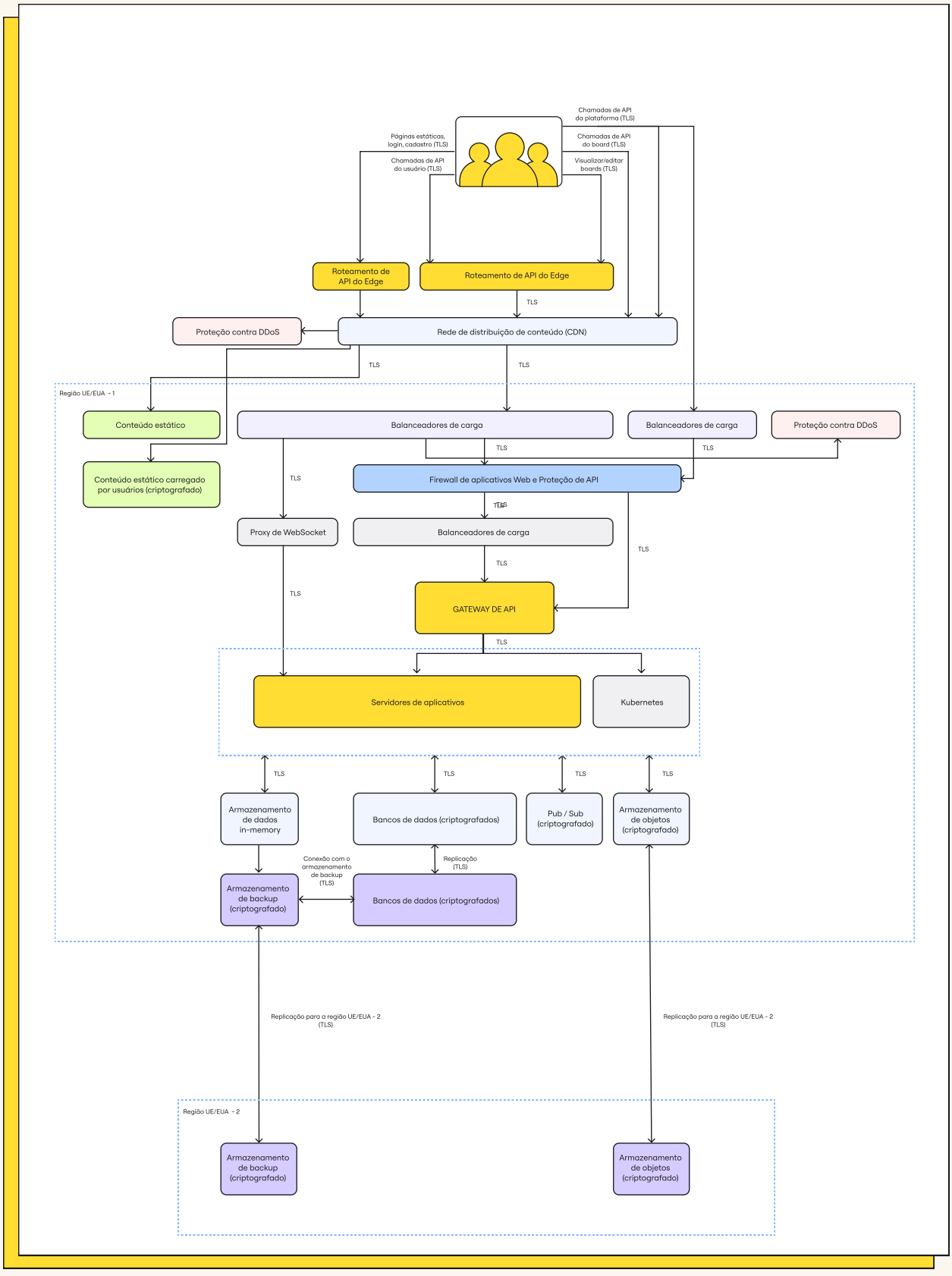
Os principais sistemas de produção da Miro estão hospedados em data centers da AWS localizados na UE (Irlanda) e nos EUA (Ohio). Além disso, os data centers da AWS localizados na UE (Frankfurt) e nos EUA (Virgínia) são usados para armazenar backups e podem ser operacionalizados de acordo com o plano de recuperação de desastres.

Dentro da infraestrutura de nuvem da AWS, a Miro é responsável por configurar a segurança lógica, de rede e de aplicativos da infraestrutura de nuvem, de acordo com as práticas recomendadas do setor e a estrutura bem projetada da AWS. As medidas de proteção são implementadas em uma abordagem em camadas, com o princípio do privilégio mínimo e negação por padrão, a menos que seja explicitamente permitido. O gerenciamento e o acesso são estritamente limitados a funcionários específicos e exigem autenticação multifator (MFA) e acesso de dispositivos gerenciados por meio de rede virtual privada (VPN).

Para obter mais informações, consulte o Modelo de responsabilidade compartilhada da AWS.



Fluxo de dados na UE e nos EUA

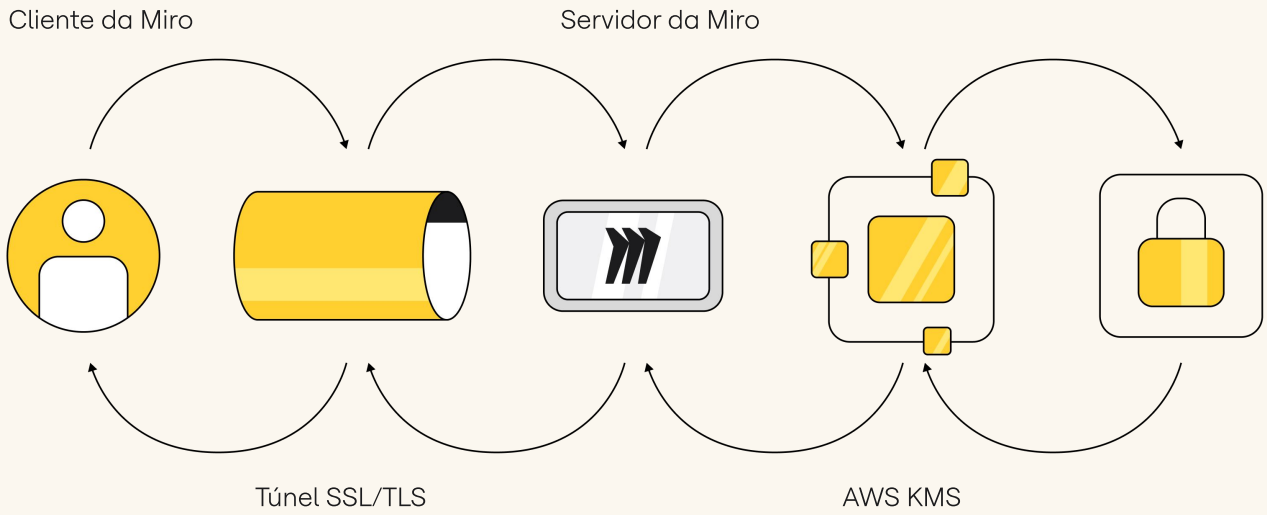


Criptografia de dados

Para proteger os dados do usuário, a Miro harmoniza a segurança dos dados com os requisitos técnicos de nossos clientes corporativos, empregando uma variedade de métodos de criptografia.

A Miro adere aos mais recentes padrões de criptografia para proteção de dados em repouso e em trânsito. Isso significa que a Miro suporta a **criptografia AES (Advanced Encryption Standard) de 256 bits** em repouso e **TLS (Transport Layer Security) 1.3**, além da 1.2, para dados em trânsito. Juntos, eles ajudam a garantir a criptografia de ponta a ponta em todo o ciclo de vida dos dados.

Criptografia na Miro



Para obter mais informações, baixe nosso informe técnico sobre criptografia.

Gerenciamento de chaves de criptografia

A infraestrutura de gerenciamento de chaves da Miro foi projetada pensando nos controles de segurança operacionais, técnicos e processuais, com acesso direto às chaves muito limitado. A geração, a troca e o armazenamento de chaves de criptografia são distribuídos para processamento descentralizado. A Miro oferece suporte a gerenciamento de chaves com uma chave hospedada na sua conta da AWS por meio do AWS KMS (Key Management System).

- **Chaves de criptografia de arquivo:** as chaves de criptografia de arquivo são criadas, armazenadas e protegidas por controles de segurança e políticas de segurança da infraestrutura do sistema de produção.
- **Chaves SSH internas:** o acesso aos sistemas de produção é restrito, com pares de chaves SSH exclusivos. Um sistema interno gerencia o processo seguro de troca de chaves públicas, e as chaves privadas são armazenadas com segurança.
- **Distribuição de chaves:** a Miro automatiza o gerenciamento e a distribuição de chaves confidenciais apenas para os sistemas necessários para as operações. O sistema de distribuição de chaves é baseado no AWS KMS.

Gerenciamento de segredos

Dados confidenciais como senhas, chaves de API, credenciais de banco de dados e certificados são armazenados com segurança em nossos sistemas de gerenciamento de segredos. O acesso aos nossos sistemas de gerenciamento de segredos é autorizado apenas para os serviços que requerem esses segredos e é limitado a um pequeno número de nossos engenheiros de operações.

Controle de acesso e autenticação

Os controles técnicos de acesso e as políticas internas da Miro proíbem os funcionários de acessar arbitrariamente boards de usuários e outras informações sobre as contas dos usuários. Apenas um pequeno número de engenheiros responsáveis pelo desenvolvimento de serviços fundamentais da Miro tem acesso limitado a tarefas de solução de problemas e apenas com o consentimento explícito dos usuários. A equipe de suporte da Miro não tem acesso ao conteúdo do board, a menos que seja explicitamente convidada pelo cliente e, quando um funcionário deixa a empresa, perde todo o acesso imediatamente.

Segurança de rede

A Miro mantém a segurança da rede de backend com vários níveis de proteção e defesa, incluindo grupos de segurança, proxies, monitoramento e teste de segurança de rede, sistemas de detecção de invasão e auditoria.

O acesso à rede interna do ambiente de produção é restrito apenas a grupos de usuários autorizados via VPN, com uso de logon único (SSO) e MFA, além da autenticação de chave requerida em todos os sistemas.

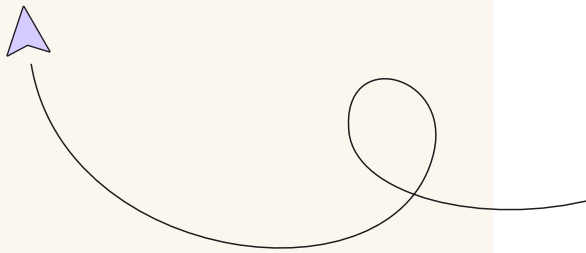
Gerenciamento de vulnerabilidades

A equipe de segurança da Miro realiza regularmente testes de segurança automatizados e manuais de aplicativos e infraestrutura, para identificar e corrigir possíveis vulnerabilidades de segurança. Também são usados prestadores de serviços independentes para realizar testes de penetração externa anuais e os problemas identificados são prontamente corrigidos. Nosso programa público de recompensa por bugs também incentiva os pesquisadores de segurança a enviar as vulnerabilidades descobertas em nossos produtos e serviços.

Gerenciamento de alterações

A Miro tem uma política formal de gerenciamento de alterações, que garante que todas as alterações do aplicativo sejam autorizadas antes da implementação no ambiente de produção e que todos os requisitos de segurança sejam atendidos. As alterações no ambiente de produção da Miro são restritas ao pessoal autorizado, enquanto a equipe de segurança garante que o servidor, o firewall e outras configurações relacionadas à segurança sejam mantidos atualizados com os padrões do setor.

Ao utilizar o gerenciamento de postura de segurança na nuvem, podemos identificar as ameaças mais relevantes em nosso ambiente de nuvem e ser alertados sobre vulnerabilidades ou atualizações que são necessárias em nossa infraestrutura de nuvem.



Políticas de segurança

> Na Miro, avaliamos o risco e melhoramos continuamente a segurança, a confidencialidade, a integridade e a disponibilidade do serviço. Revisamos e aprovamos nossas políticas de segurança (segurança da informação, ciclo de vida de desenvolvimento seguro de software, resposta a incidentes, acesso lógico e gerenciamento de alterações) ao menos uma vez por ano. Além disso, monitoramos a conformidade com essas políticas, executamos testes de segurança de aplicativos e redes e realizamos avaliações de riscos internos e externos.

Política e acesso de funcionários

Quando as leis locais permitem, os funcionários da Miro passam por verificações de antecedentes criminais, assinam um reconhecimento da política de segurança, comprometem-se com a confidencialidade e realizam treinamentos de segurança obrigatórios, para ajudar a garantir que as práticas recomendadas sejam seguidas, visando a proteção dos dados dos clientes.

O acesso entre redes é estritamente limitado ao número mínimo de funcionários e serviços, e a configuração do firewall é rigorosamente controlada e limitada a um pequeno número de administradores. O acesso a outros recursos é concedido mediante aprovação explícita de pessoas apropriadas e um registro do pedido de acesso e a justificativa são registrados pela gerência.

Segurança física

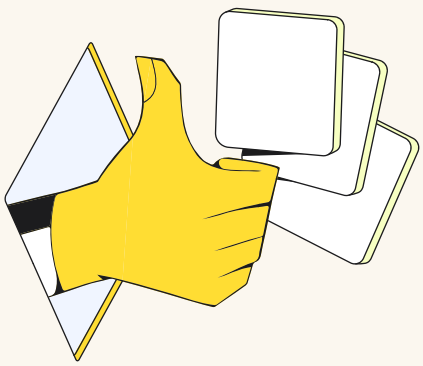
A Miro usa um provedor terceirizado profissional para aplicar sua política de segurança física e supervisionar a segurança de escritórios corporativos. O acesso físico às instalações corporativas é restrito ao pessoal autorizado da Miro por meio de um sistema de acesso com cartão, e um sistema de cartão de visitante ajuda a garantir que apenas pessoas autorizadas tenham acesso às instalações corporativas. O acesso às áreas que contêm servidores corporativos é restrito ao pessoal autorizado por meio de funções hierárquicas elevadas, concedidas usando o sistema de acesso com cartão. As listas de pessoas autorizadas aprovadas para o acesso físico aos ambientes corporativo e de produção são revisados pelo menos trimestralmente.

Confiabilidade

A infraestrutura de servidores da Miro fornece armazenamento de dados seguro e alta disponibilidade. Todos os serviços de aplicativos são executados em vários servidores, com um sistema de balanceamento de carga/tolerância a falhas para aumentar a redundância. As topologias de cluster são classificadas pelo nível N+1 de alta disponibilidade. Os dados do usuário são replicados para várias regiões de disponibilidade para proteção e são criptografados e submetidos a backup regularmente. Além disso, os backups diários do banco de dados são armazenados separadamente do data center principal.

Resposta a incidentes

A equipe de resposta a incidentes da Miro está preparada para responder a qualquer incidente 24 horas por dia, sete dias por semana. As políticas de tratamento de incidentes abrangem problemas de disponibilidade, integridade, segurança, privacidade e confidencialidade do serviço. Os procedimentos incluem resposta imediata a incidentes, avaliação de gravidade, medidas de contenção, comunicação com as partes interessadas e atualizações de status em status.miro.com.



Recuperação de desastres

No caso de uma crise ou desastre que afete as operações de negócios da Miro, nossa equipe de infraestrutura segue um plano de recuperação de desastres (DRP, na sigla em inglês), para atender aos requisitos de segurança da informação. As descobertas são documentadas e acompanhadas até a resolução. A equipe revisa e testa esse plano, incluindo a medição do tempo real de recuperação (RTA, na sigla em inglês), ao menos uma vez por ano.

O DRP abrange desastres de durabilidade e disponibilidade. O desastre de durabilidade é definido como uma perda completa ou permanente de data centers primários ou uma perda da capacidade de se comunicar ou servir dados de data centers.

O objetivo de tempo de recuperação (RTO, na sigla em inglês) é a duração do tempo e um nível de serviço no qual um processo de negócios ou serviço deve ser restaurado após um desastre. O objetivo de ponto de recuperação (RPO, na sigla em inglês) é o período máximo tolerável no qual os dados podem ser perdidos devido a uma interrupção do serviço.

Os planos de resposta a incidentes e de recuperação de desastres da Miro estão sujeitos a testes em intervalos planejados e em caso de mudanças organizacionais ou ambientais significativas.

Conformidade, auditoria e certificações

De acordo com o relatório de 2023 do Instituto Ponemon sobre o custo de uma violação de dados, a não conformidade com as normas de segurança é um dos maiores fatores que contribuem para violações de dados. É por isso que, na Miro, levamos a conformidade a sério. Temos um departamento de segurança dedicado liderado por um diretor de segurança da informação, que inclui várias equipes de segurança dedicadas à conformidade e governança. O diretor de privacidade de dados da Miro gerencia e supervisiona a privacidade de dados, para ajudar a garantir a conformidade com as normas de privacidade. Uma função de auditoria interna e independente está em vigor para reforçar a garantia objetiva e a revisão da governança.

Sempre em conformidade

A Miro está sempre em conformidade com os requisitos legais das regiões específicas onde operamos. Também somos transparentes sobre nossos padrões de segurança e privacidade de dados que protegem os dados dos clientes contra acessos não autorizados, violações e ameaças.

A auditoria e o atestado dessas certificações e dos padrões estabelecidos nos permitem avaliar nossa conformidade e a eficácia operacional dos controles ao longo do período de auditoria, como no relatório de garantia independente SOC 2 Tipo II.

Isso inclui:

- **Normas de segurança da informação**, como SOC 2 Tipo II e ISO/IEC 27001
- **Normas de transferência de dados** geridas por uma solução de residência de dados da UE líder da categoria e o uso de cláusulas contratuais padrão, para fornecer um nível adequado de proteção de dados fora da UE e do Reino Unido, que permita a adesão à Lei Geral de Proteção de Dados (LGPD)
- **Certificações regionais e setoriais**, como Cloud Security Alliance, Cyber Essentials e TISAX
- **Auditorias recorrentes de terceiros** conduzidas pelas melhores empresas do setor, como o British Standard Institute (BSI)
- **Diretrizes de acessibilidade** e um Relatório de Conformidade de Acessibilidade (ACR, na sigla em inglês) baseado no modelo voluntário de acessibilidade de produtos (VPA, na sigla em inglês)

Como a Miro protege os dados pessoais dos clientes

As leis e regulamentos de privacidade e proteção de dados, como a LGPD na Europa, tornaram-se cada vez mais rígidos, impondo obrigações rigorosas sobre como as organizações coletam, processam, transferem e armazenam dados do usuário. O não cumprimento desses regulamentos pode resultar em multas pesadas, investigação regulatória e perda de confiança do cliente, possivelmente inviabilizando um negócio de SaaS.

A Miro centraliza seu programa de privacidade e proteção de dados em torno de práticas estabelecidas do setor, com um grande foco na proteção de dados pessoais de clientes por meio da conduta dos funcionários e do design do produto. Os funcionários devem aderir aos padrões de proteção de dados, se comprometer com a confidencialidade e estão sujeitos a limitações técnicas (consulte a política e acesso de funcionários). Os processos de design do produto da Miro incluem verificações regulatórias e revisões jurídicas, e as equipes de produto e de engenharia recebem treinamentos periódicos sobre padrões de design.

A política de privacidade da Miro estabelece, de maneira explícita e transparente, as categorias de dados pessoais processados pela Miro na qualidade de controladora de dados, junto com os objetivos de negócio estabelecidos. Ela também define as categorias de terceiros utilizados pela Miro para processar os dados pessoais, indica como as pessoas podem exercer seus direitos segundo a lei de proteção de dados e os mecanismos de transferência de dados utilizados pela Miro, para transferir dados pessoais fora da UE.

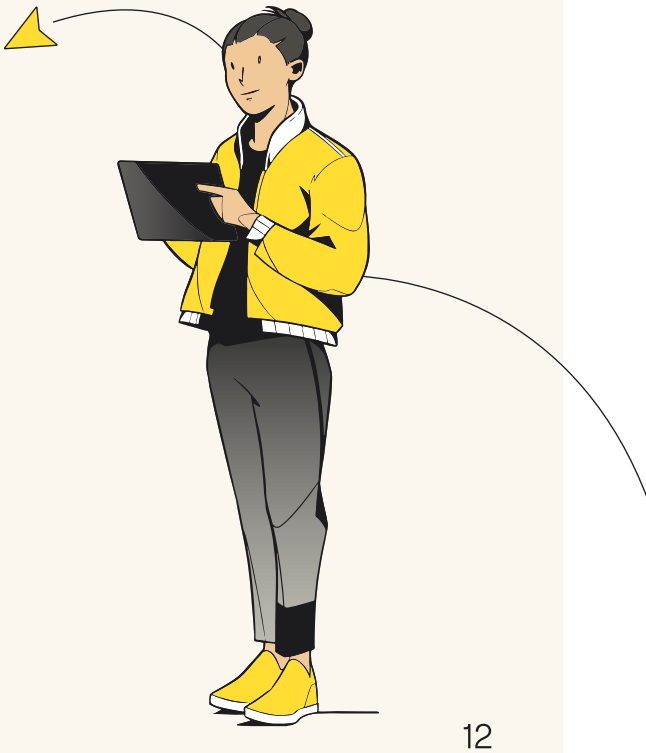
Quando a Miro processa dados pessoais em nome de seu cliente ou transfere dados pessoais de clientes fora da UE, concordamos em estabelecer as condições apropriadas, por exemplo, por meio de nosso Adendo de Processamento de Dados (DPA, na sigla em inglês), que inclui compromissos contratuais exigidos pela LGPD, pela Lei de Privacidade do Consumidor da Califórnia (juntamente com sua modificação por meio da Lei de Direitos de Privacidade da Califórnia) e outras leis de privacidade e proteção de dados dos EUA e do mundo.

Processamento de dados por terceiros

À medida que a Miro envolve terceiros para processar dados pessoais de clientes, exigimos um processo de aquisição rigoroso, que inclui verificações jurídicas e de segurança, e concordância com as condições adequadas de processamento e transferência de dados. A Miro fornece a lista desses terceiros online, disponível por meio de um link em seu DPA, e informa os clientes de sua intenção de alterar ou adicionar qualquer terceiro relevante a essa lista, de acordo com o processo estabelecido no DPA.

Segurança do produto

Sendo uma plataforma baseada em nuvem, a Miro pode ser acessada de um navegador da Web em dispositivos desktop e móveis, ou por meio de aplicativos dedicados para ambas as plataformas. Devido a esses pontos de contato e à natureza da colaboração remota e distribuída por meio de uma plataforma como a Miro, devemos ajudar os clientes a abordarem uma Arquitetura de Confiança Zero (ZTA, na sigla em inglês). Isso significa não apenas capacitar nossos clientes a ter as soluções de segurança certas, mas também ajudar a garantir que elas sejam implantadas corretamente.



miro

Arquitetura de Confiança Zero

Diferentemente dos modelos de segurança tradicionais que concedem amplo acesso com base na localização de um usuário ou no ponto de entrada da rede, a arquitetura de confiança zero pressupõe que as ameaças podem se originar de qualquer lugar, até mesmo de dentro da organização. Isso tem se tornado cada vez mais importante no ambiente de trabalho moderno, no qual os funcionários acessam recursos corporativos de vários locais e dispositivos. A arquitetura de confiança zero preconiza a verificação contínua da identidade, a segurança do dispositivo e a adesão às políticas de segurança em todas as interações do usuário com dados e recursos.

A Miro ajuda as organizações empresariais a abordar a arquitetura de confiança zero capacitando os admins para definir as políticas certas, com permissões e controles individuais, sem comprometer a capacidade de colaboração dos times. Esses controles de segurança incluem:

- **Logon único (SSO):** com o logon único baseado em SAML, os usuários podem acessar a Miro por meio de um provedor de identidade (IdP) de sua escolha, incluindo Okta, Azure AD, AuthO, Google SSO e outros. Assim, os usuários não precisam inserir repetidamente suas credenciais para cada aplicativo, economizando tempo e reduzindo o número de superfícies de ataque.

- **Autenticação em dois fatores (2FA):** a autenticação em dois fatores funciona na Miro sem exigir SSO e adiciona um nível extra de proteção quando os usuários acessam a conta da organização na Miro. A 2FA é válida para qualquer usuário que efetue login com seu e-mail e senha (colaboradores externos para empresas com SSO ou todos os usuários para organizações que não têm SSO configurado). Os usuários podem configurá-la em seus perfis ou os admins da empresa podem habilitar a 2FA para toda a organização. A Miro aplica a 2FA com um aplicativo de senha única baseada no tempo (TOTP, na sigla em inglês), como o Microsoft Authenticator, o Google Authenticator e o Authy.

- **Tempo limite da sessão inativa:** define os limites de tempo que os usuários podem ficar inativos antes de serem desconectados automaticamente. Esse limite minimiza o intervalo de tempo no qual um invasor pode tentar roubar e usar uma sessão atual do usuário (remota ou pessoalmente por meio de uma estação de trabalho sem supervisão).

- **Acesso baseado em função para admins:** há várias funções de admin que podem ser atribuídas aos usuários para executar fluxos de trabalho (por exemplo, admin da empresa, admin de usuário, admin de conteúdo), cada uma com níveis específicos de privilégios, definições e configurações de acesso. Isso distribui com segurança a carga de trabalho de administração, evitando que os admins tenham privilégios desnecessários ou acesso a informações confidenciais.

- **Políticas de compartilhamento:** decida quando e como o conteúdo da sua organização deve ser acessado, definindo políticas para:
  - Restringir o compartilhamento fora dos domínios permitidos
  - Restringir o compartilhamento por meio de link público
  - Exigir senhas para boards públicos (nível da empresa)
  - Restringir o compartilhamento em todos os times e em toda a empresa (nível de time)
  - Restringir a capacidade de mover boards para outros times (nível de time)
  - Restringir o compartilhamento de templates de clientes em toda a empresa

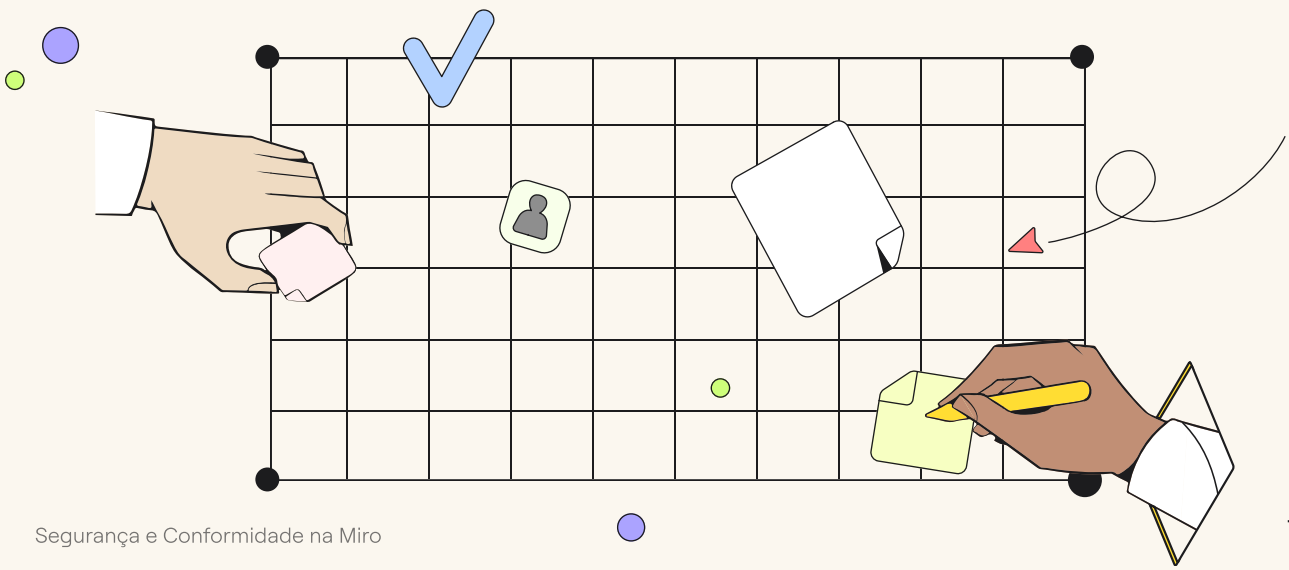
- **Gestão de mobilidade corporativa:** gerencie com segurança o acesso à Miro de dispositivos corporativos ou pessoais com integrações de ferramentas de gestão de mobilidade corporativa (EMM), como o Microsoft Intune e o VMware Workspace ONE, ambos com suporte para Android e iOS.

- **Logs de auditoria:** os admins da empresa podem visualizar todas as atividades dentro de sua organização. Os logs ajudam na solução de problemas ou quando é necessário um relatório detalhado de eventos importantes, como alterações nas definições de segurança globais, convites de novos usuários ou a criação de novos boards.

- **Classificação:** os usuários do plano Enterprise podem atribuir etiquetas de classificação aos seus boards para indicar o nível de confidencialidade. As etiquetas padrão podem ser configuradas no nível da empresa ou do time, e os usuários podem usá-las para filtrar boards no painel.

- **Gestão do ciclo de vida do conteúdo:** a Miro permite que os usuários filtrem por empresa, para gerenciar com eficiência o ciclo de vida dos boards no nível da empresa. Além disso, um menu de lixeira global é acessado facilmente, para restaurar ou excluir os boards permanentemente.

- **Administração:** a automação desempenha um papel crítico na prevenção de erros e economiza tempo ao lidar com centenas de milhares de boards e usuários. A otimização do provisionamento SCIM ou JIT automatiza o acesso do usuário e simplifica o gerenciamento do ciclo de vida do usuário.



Inteligência artificial

A inteligência artificial na Miro é tratada com o mesmo cuidado e atenção à segurança com que tratamos todo o produto. Nossos princípios e práticas orientadores em relação à IA demonstram nosso compromisso com o desenvolvimento ético e responsável da IA, para mantermos a confiança de clientes, usuários e parceiros.

Isso inclui a prestação de contas por meio de modelos transparentes de IA. Usamos dados apenas conforme descrito em nossa Política de Privacidade ou conforme explicitamente acordado entre a Miro e o cliente. Os clientes mantêm controle total sobre seu conteúdo. Também permitimos que os clientes preservem o controle ao aceitar ou recusar os serviços de IA. Mais informações em nosso informe técnico.

Integrações do ecossistema Enterprise

Os clientes do plano Enterprise podem beneficiar-se de uma variedade de integrações de segurança e conformidade, incluindo soluções de gerenciamento de eventos e informações de segurança (SIEM), agentes de segurança de acesso à nuvem (CASB), gestão de mobilidade corporativa (EMM), plataformas de integração, ferramentas de gerenciamento de ativos de software (SAM) e automação de fluxo de trabalho. As empresas também podem desenvolver suas próprias integrações personalizadas.

Integrações de nível empresarial

miro | ENTERPRISE GUARD

Miro Enterprise Guard: complemento de segurança avançada de dados e de governança

O trabalho realizado na Miro costuma ser estratégico e requer governança. Os clientes usam cada vez mais a Miro para criar e armazenar dados confidenciais e proprietários, e os dados confidenciais podem aparecer onde você menos espera, apesar das políticas da empresa. Além disso, observamos que a quantidade de conteúdo nos boards da Miro de nossos maiores clientes cresce a uma taxa de 2,5x por ano, aumentando ainda mais a superfície de risco para a segurança e governança de dados.

Os principais recursos de segurança de aplicativos SaaS de nível empresarial, como autenticação e SSO, bem como controles de acesso individuais, proporcionam à maioria dos clientes controle suficiente sobre quando e como eles protegem seus dados. No entanto, alguns clientes desejam níveis adicionais de proteção além de nossas medidas de segurança padrão devido à dimensão estratégica da Miro para seus negócios ou por causa dos requisitos de conformidade regulatória de seu setor, ou uma combinação de ambos.

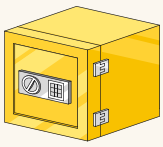
Pensando nisso, desenvolvemos o Miro Enterprise Guard, um complemento avançado de segurança e governança de dados.

---

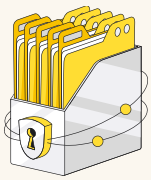
[1] Crescimento acumulado de boards em mais de mil organizações com plano Enterprise, de 2017 a 2023.

Gerencie o ciclo de vida do conteúdo de acordo com as suas necessidades

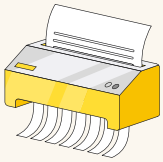
O Enterprise Guard automatiza o processo de gerenciamento do ciclo de vida de seus boards, ajudando a cumprir os requisitos de conformidade ou da política organizacional.
Com os recursos, você pode:



Reter os boards de acordo com a política, com uma trilha de auditoria completa



Excluir os boards de acordo com a política, com uma trilha de auditoria completa



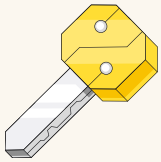
Definir a política de lixeira no nível organizacional, para maior controle sobre a exclusão e retenção permanentes justificáveis de seus boards da Miro

Gerenciamento de chaves

O pacote de complementos do Enterprise Guard também inclui a opção de habilitar o **Gerenciamento de chaves de criptografia (EKM)**, oferecendo controle total e independente sobre suas chaves de criptografia por meio do AWS KMS.

Você também obtém maior visibilidade de auditoria e maior controle de acesso dos dados, como nomes de contas, nomes de projetos e conteúdo gerado pelo usuário, incluindo widgets, comentários e arquivos carregados.

Além disso, quando os clientes trazem sua própria chave (BYOK, na sigla em inglês), eles podem auditar o uso das chaves, acessando os logs de todas as chamadas de API recebidas, para ajudar a atender os requisitos de conformidade e regulatórios



Gerenciamento de chaves de criptografia (EKM)

Conclusão

A maioria dos executivos está insatisfeita com a capacidade de inovação e competitividade de sua organização. Na verdade, 82% dos líderes afirmam que uma empresa desaparecerá no prazo de cinco anos se não conseguir inovar. Alguns dos maiores entraves à inovação são os desafios tecnológicos, como ferramentas desatualizadas e obsoletas. Os líderes e trabalhadores da informação concordam que a tecnologia legada sufoca a criatividade e dificulta a produtividade. É por isso que muitas organizações se apressaram em implementar ferramentas de colaboração, sem considerar totalmente as implicações de segurança.

Com um espaço de trabalho de colaboração visual como a Miro, a inovação torna-se fácil e segura. A Miro tem o compromisso de garantir a segurança e proteger os dados de nossos clientes. Por isso, mais de 60 milhões de usuários em todo o mundo, incluindo 99% das empresas da Fortune 100, confiaram a nós o seu bem mais valioso: suas informações. Junte-se a essas empresas líderes e inove em um espaço de trabalho colaborativo, sabendo que, durante todo o processo, você tem a certeza de que seus dados estão seguros e protegidos.

Entre em contato com nossa equipe de vendas para saber mais.

Recursos

Miro Trust Center
Informe técnico sobre criptografia
Residência de dados na Miro
Perguntas frequentes sobre segurança e conformidade (Central de ajuda)
Relatório anual de transparência
Política de Privacidade
Termos de Serviço
Miro Enterprise
Diretrizes de acessibilidade

A Miro é um espaço de trabalho visual voltado à inovação, no qual os times distribuídos de todos os tamanhos podem criar a próxima grande ideia. Com os canvas infinitos da plataforma, os times podem realizar workshops e reuniões, desenhar produtos, fazer brainstorming de ideias e muito mais. A Miro possui sedes em São Francisco e Amsterdã e atende a mais de 60 milhões de usuários em todo o mundo, incluindo 99% das empresas da Fortune 100. Fundada em 2011, a Miro atualmente possui mais de 1.800 funcionários em 12 escritórios pelo mundo.

miro

Para saber mais, acesse miro.com

Plano Enterprise da Miro
https://miro.com/enterprise/

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

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

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