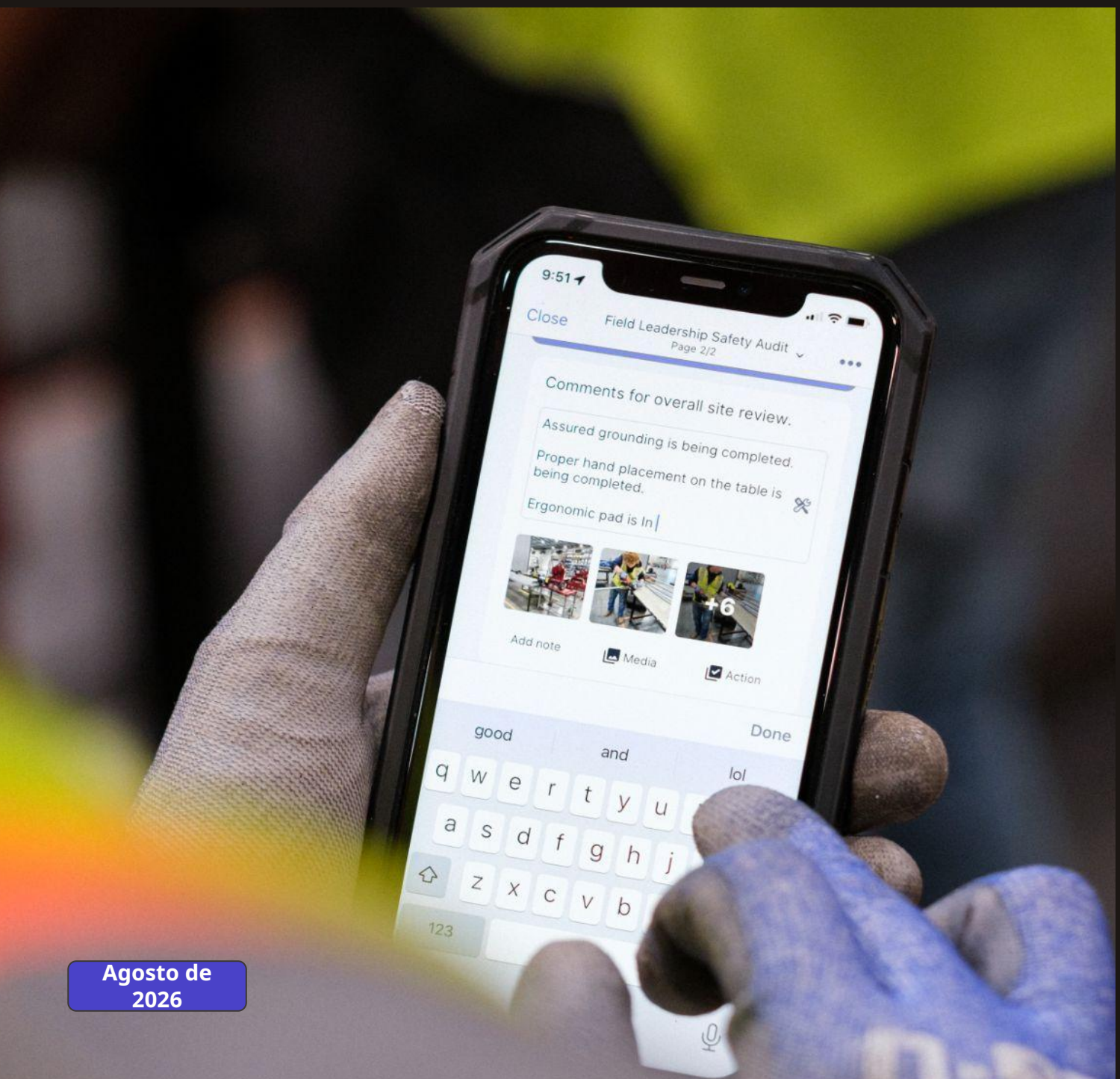
Mitti
by SafetyCulture

Visão geral da segurança

Entenda a segurança cibernética do Mitti



Agosto de 2026

Índice

“Antes do Mitti, precisávamos que alguém inserisse todos os dados do checklist assim que voltasse ao escritório, executasse análises do Excel e, por fim, compartilhasse com a equipe. A análise nos fornece dados mais abrangentes em uma área que podemos compartilhar.”

Deaky Wong

Engenheiro de manutenção de linha, Cathay Pacific

Nossa missão

A missão do Mitti é ajudar empresas a obter locais de trabalho mais seguros e de maior qualidade em todo o mundo através de produtos inovadores e de baixo custo que funcionam em dispositivos móveis.

Cumprimos nossa missão por meio de nossos produtos de Software-as-a-Service (SaaS).

Nossos produtos são usados por mais de 85.000 empresas em todo o mundo, em diversos setores e em uma variedade de casos de uso.

Temos orgulho da Mitti ser vista como líder mundial em produtos que promovem segurança e qualidade, e sabemos da importância de ajudar nossos clientes a melhorar suas operações diárias.

Vemos nossa abordagem de segurança cibernética como um pilar fundamental para manter nosso status como líder neste espaço, e este conteúdo resume como abordamos a segurança cibernética como empresa.

A Mitti possui a certificação ISO 27001:2022 e segue os Critérios de Serviços de Confiança da AICPA, reafirmando nossa dedicação à segurança do cliente.

Visão geral

Programa de segurança cibernética

A Mitti possui um programa de cibersegurança ativo, robusto e em contínua melhoria implementado para garantir que nossa empresa e os produtos que fornecemos sejam seguros. O programa de segurança cibernética da Mitti emprega vários controles em nível técnico e operacional para garantir que tenhamos uma abordagem eficaz de defesa em profundidade para proteção contra ataques cibernéticos e segurança dos dados tratados por nossos produtos Software-as-a-Service (SaaS).

As principais funcionalidades incluem:

Um programa de segurança alinhado com os padrões de melhores práticas do setor, incluindo o uso de plataformas de nuvem compatíveis com benchmarks de segurança confiáveis, incluindo ISO 27001 e SOC 2.

Um foco em acertar o básico, reconhecendo que os fundamentos da segurança continuam sendo os mais críticos.

Isso inclui:

- Treinamento da nossa força de trabalho sobre a importância da segurança.
- Ter uma equipe de segurança dedicada, responsável por manter nossa empresa segura contra ameaças reais e iminentes aos nossos negócios e aos dados que os clientes nos confiam.
- Empregar mecanismos robustos para garantir que o acesso aos sistemas e dados de clientes da Mitti seja cuidadosamente controlado.
- Criptografar os dados de clientes que mantemos (tanto em trânsito quanto em repouso).
- Garantir a aplicação de patches em nosso ambiente de TI e em nossos produtos o mais rápido possível para minimizar a oportunidade de exploração de vulnerabilidades por invasores cibernéticos.
- Monitorar e testar ativamente nosso ambiente de TI e nossos produtos em busca de vulnerabilidades, remediando-as como prioridade.
- Ter um processo definido implementado para fornecer suporte e resposta eficazes em caso de incidente de segurança.

Aplicar due diligence para garantir que nossos provedores de serviço estejam cumprindo os padrões do setor no que diz respeito à segurança. Sabemos que a segurança de nossos parceiros afeta diretamente a nós e aos nossos clientes, por isso escolhemos com quem trabalhamos com muito cuidado.

O restante deste documento fornece uma visão geral das várias partes do nosso programa de segurança.

Práticas de segurança organizacional

Nossa abordagem à segurança como empresa é focada no alinhamento com as melhores práticas recomendadas em padrões reconhecidos, como NIST, ISO 27001 e SOC.

Governança de segurança

A Mitti possui um conjunto documentado de políticas, padrões e procedimentos que define nossa abordagem de segurança como empresa. Essas políticas e procedimentos são compartilhados com toda a equipe e revisados e atualizados pelo menos anualmente (e com mais frequência quando alterações materiais são obrigatórias) para garantir que nossa abordagem à segurança permaneça atual.

Nosso foco é garantir a responsabilidade pela segurança em toda a nossa empresa. Para esse fim, temos um fórum de gestão de segurança da informação estabelecido com as principais partes interessadas de toda a Mitti, que se reúnem regularmente para revisar e discutir assuntos relacionados à segurança, e tomar quaisquer decisões que tenham uma influência em nossa abordagem de segurança cibernética.

A Mitti possui a certificação ISO 27001:2024 e segue os Critérios de Serviços de Confiança da AICPA, reafirmando nossa dedicação à segurança do cliente.

Controles de acesso

Garantimos que o acesso a sistemas em nosso ambiente de TI, incluindo as plataformas de nuvem que usamos, seja restrito a funcionários que especificamente requerem este acesso para seu trabalho.

Todo acesso de administrador requer autenticação multifator, e é obrigatório que os funcionários que acessam nosso ambiente usem uma solução de VPN aprovada.

As permissões de acesso aos nossos sistemas são revisadas regularmente por funcionário e alteradas prontamente. Como parte de nosso processo de desligamento, todo o acesso a sistemas e serviços para funcionários que estão saindo é revogado.

Segurança de terceiros

Revisamos cuidadosamente as práticas de segurança de terceiros que contratamos – inicial e ativamente, para garantir que suas práticas atendam aos padrões do setor e estejam em conformidade com nossas próprias políticas e procedimentos de privacidade e segurança. Se um terceiro requer acesso aos nossos sistemas, garantimos que o acesso seja limitado especificamente ao propósito para o qual foi contratado.

Como a Amazon Web Services (AWS) é uma de nossas principais provedoras, engajamos com ela usando o Modelo de Responsabilidade Compartilhada para segurança e conformidade, garantindo que haja uma definição clara de quem assume a responsabilidade pelo que em relação à segurança. A AWS é certificada e está em conformidade com muitos dos mais recentes padrões do setor – mais informações podem ser encontradas aqui:

Para o processamento de dados financeiros e de cartão de crédito, a Mitti usa vários parceiros (Zuora, eWay e Stripe) cujas práticas de segurança estão em conformidade com o Payment Card Industry Data Security Standard (PCI-DSS).

Segurança de rede

As redes corporativas da Mitti são protegidas por firewalls, bem como pela tecnologia de sistema de detecção de intrusão (IDS) e sistema de prevenção de intrusão (IPS) no perímetro, fornecidos por dispositivos dedicados de segurança de rede para que possamos detectar e nos proteger contra qualquer tráfego malicioso.

Para nossas plataformas baseadas em nuvem, usamos principalmente a Amazon Web Services (AWS), que fornece uma estratégia multicamadas para defender contra ataques externos. Em nível de infraestrutura, a AWS emprega estratégias como controle de acesso de dispositivo de rede, segregação de dados usando firewalls e nuvens privadas virtuais para filtrar tráfego malicioso e fazer uso de extensos registros e monitoramento para evitar ataques baseados em rede. Em nível de aplicativo, aproveitamos o Web Application Firewall (WAF) e a proteção Distributed Denial of Service (DDoS) da Cloudflare para prevenir ataques baseados na Web e de negação de serviço contra nossos produtos.

Nós segregamos nossos ambientes de desenvolvimento, teste e produção.

Práticas de segurança organizacional

Registro e monitoramento

A Mitti faz uso de um sistema de registro centralizado, que inclui eventos de auditoria de acesso a aplicativos. Esses registros são mantidos por 90 dias. Também usamos registros do Amazon Elastic Load Balancing (ELB) para rastrear solicitações de acesso a serviço. Os registros armazenados na AWS não podem ser modificados, e o acesso é restrito àqueles que requerem acesso para os requisitos de suas funções.

Reconhecemos a importância de revisar os registros regularmente para identificar atividades maliciosas de usuários e identificar possíveis vulnerabilidades em nossos produtos; temos monitoramento automatizado que nos alerta sobre tipos específicos de eventos potencialmente maliciosos em nossa infraestrutura global.

Treinamento de conscientização sobre segurança

Todo o pessoal da Mitti passa por treinamento regular de conscientização sobre segurança para funções técnicas e não técnicas. Material adicional de treinamento de segurança é fornecido aos funcionários individualmente quando obrigatório, para garantir que eles estejam preparados para lidar com os desafios específicos de sua função.

Correção e gerenciamento de vulnerabilidades

A correção do nosso ambiente de TI é uma das medidas mais importantes que tomamos para nos mantermos protegidos contra uma possível violação de segurança. Para alcançar isso:

- Usamos o AWS System Manager para implantar patches regularmente em nossa infraestrutura baseada em nuvem.
- Utilizamos soluções de gerenciamento de dispositivos móveis (MDM) para garantir que patches importantes sejam instalados da forma mais rápida e eficiente possível.
- Nossos dispositivos são protegidos com tecnologias de segurança de endpoint para detectar e prevenir ameaças à segurança, incluindo vírus, ataques de malware e monitorar atividades maliciosas.
- Implantamos patches para as vulnerabilidades mais críticas primeiro, com os patches sendo implantados em nosso ambiente de não produção para testes iniciais antes de serem propagados rapidamente por todo o ambiente de TI.

Protegendo dados do cliente

A Mitti leva a segurança dos dados de nossos clientes extremamente a sério. Tomamos várias medidas para garantir que os dados do cliente sejam cuidadosamente protegidos.

Protegendo nossos dados de clientes

Restringindo o acesso aos dados

A Mitti implementa controles técnicos e da empresa para ajudar a proteger os dados dos clientes contra acesso ou uso inadequado por pessoas não autorizadas (sejam externas ou internas). Os dados do cliente são armazenados apenas em nosso ambiente de produção, e o acesso a esses dados por funcionários da Mitti é limitado apenas aos funcionários que requerem acesso para realizar suas tarefas padrão. O acesso aos dados do cliente é gerenciado usando controle de acesso e ferramentas de autenticação (incluindo o uso de autenticação de dois fatores) fornecidos pela Amazon Web Services e por nossos outros parceiros de nuvem.

Os dados do cliente são usados apenas para fins compatíveis com a prestação dos serviços contratados, como a solução de solicitações de suporte técnico. Para obter todos os detalhes, consulte a Política de Privacidade da Mitti, encontrada aqui: https://mitti.com/pt-BR/juridico/portal-de-privacidade

Quando os funcionários de suporte da Mitti precisarem acessar dados específicos de um cliente (para fins de solução de problemas ou suporte), a Mitti sempre requererá o consentimento de um cliente antes de acessar esses dados.

Não armazenamos nem armazenamos em cache dados financeiros do cliente usados para cobrança por meio da plataforma Mitti, e nossos funcionários não têm acesso direto aos dados de cobrança.

Acesso físico aos dados

Os dados do cliente são hospedados na infraestrutura fornecida pela Amazon Web Services, que mantém a segurança de seus locais usando controles de melhores práticas do setor, conforme descrito em seu site de segurança e conformidade, encontrado aqui: https://aws.amazon.com/architecture/security-identity-compliance/.

Nenhum dado de cliente é armazenado nas localizações de nossos escritórios físicos.

Criptografia de dados

A Mitti tem mecanismos implementados para garantir que os dados de nossos clientes estejam sempre protegidos.

Em repouso, todos os dados de clientes armazenados nos sistemas são criptografados usando AES-256 com chaves gerenciadas pelo Key Management Service da Amazon Web Services. Todos os dados são armazenados com segurança e sujeitos às políticas e aos procedimentos de segurança da AWS.

Para proteger os dados em trânsito, a Mitti usa a Transport Layer Security (TLS) e impõe um padrão mínimo de TLS v1.2 usando chaves de criptografia de 128 bits. Damos suporte a conexões com chaves de cifra de até 256 bits para uso com uma cifra AES.

Backups de dados

Os dados da Mitti são copiados diariamente em soluções distintas de armazenamento de dados criptografados fornecidas pela Amazon Web Services. Os backups são replicados para várias instalações da AWS e mantidos por pelo menos 30 dias.

O acesso aos backups de dados é restrito apenas a funcionários específicos da Mitti, onde esse acesso é necessário como parte dos requisitos de suas funções. Os backups são criptografados e armazenados em modo somente leitura.

Exclusão e descarte de dados

Nossos dados de clientes são armazenados e estão sujeitos aos procedimentos de exclusão e descarte da Amazon Web Services. Esses procedimentos incluem um processo para apagar com segurança mídias descontinuadas. A mídia apagada é então inspecionada para garantir a destruição bem-sucedida dos dados.

Qualquer hardware de propriedade da Mitti que contenha dados confidenciais – incluindo backups da Mitti – está sujeito à destruição lógica de dados no padrão do setor antes da reciclagem.

Protegendo nossos produtos

Reconhecemos que, para os clientes em volume, sua experiência principal com a Mitti será através dos nossos produtos. A segurança é uma parte importante da maneira como nossos produtos são desenvolvidos e operam.

Práticas seguras de desenvolvimento de software

Como parte do nosso processo de desenvolvimento de produtos, todas as alterações de código e de infraestrutura são armazenadas em um sistema de controle de origem, versionadas, revisadas e avaliadas quanto ao impacto antes da liberação da alteração para produção. Esta revisão inclui a observância das melhores práticas de segurança. Nós também segregamos nossos ambientes de desenvolvimento, teste e produção, e não usamos dados de clientes em nossos ambientes de não produção.

Controle de alterações

Todas as alterações nos produtos Mitti são ativamente testadas durante seu desenvolvimento para garantir que o impacto sobre os usuários finais seja avaliado antes da implantação, e quaisquer alterações significativas são incluídas nas anotações de liberação da produção.

A Mitti emprega sistemas de rastreamento de alterações e controle de versão para monitorar e gerenciar ativamente as alterações na base de código ou na configuração de nossa infraestrutura. Usamos processos automatizados para implantar alterações em nossos ambientes e podemos reverter as alterações conforme necessário. Usamos o Amazon CloudTrail para rastrear quaisquer alterações de configuração subjacentes na plataforma de nuvem na qual nossos produtos operam.

Identificação de vulnerabilidades e desenvolvimento de patches

Trabalhamos intensamente para minimizar o número de vulnerabilidades que surgem em nossos produtos, e reconhecemos que é importante tomar medidas proativas para garantir que tratemos de quaisquer vulnerabilidades o mais rápido possível. Para esse fim, a Mitti realiza testes de penetração anuais e ativamente testa e monitora vulnerabilidades em nossos aplicativos. Executamos um programa privado de recompensas por bugs, porque uma comunidade de pesquisadores de segurança independentes, incentivados a testar ativamente nossos produtos para identificar quaisquer problemas potenciais, apenas fortalecerá a segurança de nossos produtos.

Onde uma vulnerabilidade é identificada (interna ou externamente), o problema é rastreado e priorizado de acordo com a gravidade potencial do impacto para nossos clientes. Para problemas de gravidade crítica, isso pode incluir o trabalho ininterrupto de nossos desenvolvedores até que seja resolvido.

Patches para problemas são desenvolvidos e lançados no ambiente de produção por meio de um processo de integração contínua (CI/CD) e aplicados o mais rápido possível.

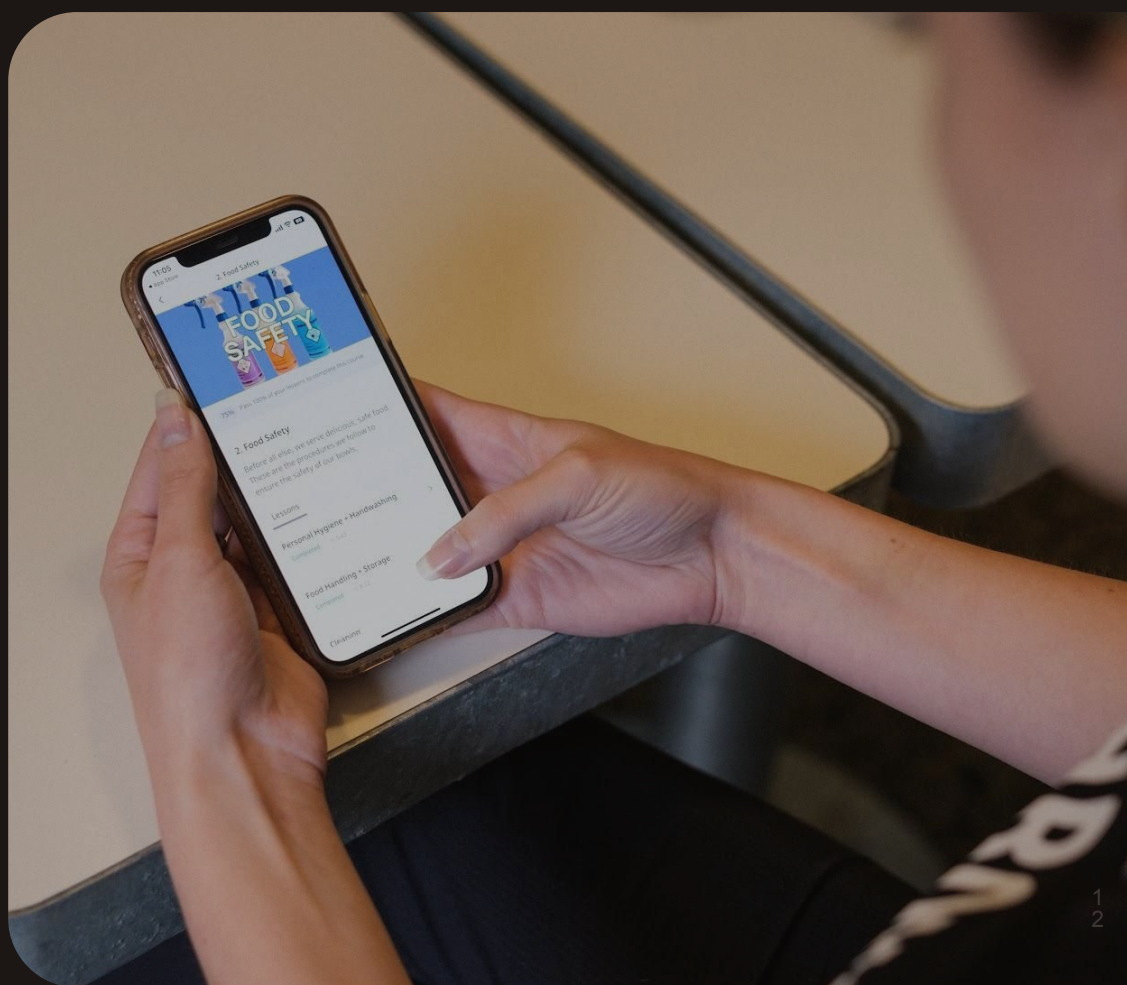
Tratamento de incidentes de segurança

Embora façamos o possível para evitar quaisquer incidentes de segurança, reconhecemos que também precisamos estar preparados para lidar com esses incidentes, caso surjam, para minimizar o impacto potencial sobre nossos clientes e sobre a Mitti.

Temos uma série de medidas em vigor, incluindo:

- Um Procedimento de Gerenciamento de Incidentes documentado que define nosso processo para lidar com a confidencialidade, integridade e disponibilidade de nosso ambiente de TI e produtos.
- Ter uma empresa global para fornecer suporte durante um incidente.
- Planos de recuperação de desastres e estratégias de contingência estabelecidos que podem ser executados para nos ajudar a manter a continuidade das operações durante um incidente. Isso inclui o uso de várias zonas de disponibilidade geográfica por meio da Amazon Web Services e a replicação de dados em vários sistemas em cada zona. Isso garante o acesso aos dados contínuo durante incidentes que afetam a disponibilidade do sistema e fornece redundância de dados em caso de falhas no sistema ou de armazenamento de dados.

A Mitti alerta prontamente os clientes afetados sobre incidentes importantes que impactem a disponibilidade dos serviços ou dados da Mitti e sobre quaisquer incidentes que afetem a confidencialidade e a integridade de seus dados.

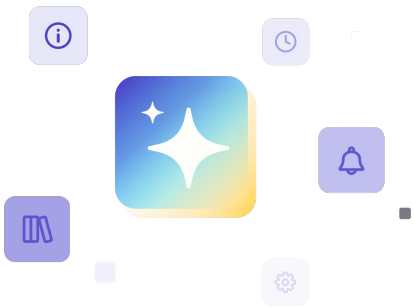


“Temos visibilidade de tudo o que fazemos devido aos dados que capturamos usando a Mitti. Se houver uma exceção de limite ou um processo que precise ser melhorado, tudo o que precisamos fazer é investigar, e nós encontraremos.”

Sofia Dias
Gerente de Segurança Alimentar e Garantia de Qualidade

Marley Spoon

Mitti e IA



A Mitti inova continuamente e traz novas funcionalidades e tecnologias para nossos clientes de forma segura e protegida. Isso inclui as funcionalidades de Inteligência Artificial (IA). Na Mitti, queremos ser transparentes com nossos clientes sobre como usamos a IA para criar nossos produtos e como usamos a IA para aprimorar a experiência de nossos usuários.

Como a Mitti usa a IA

A IA permite à Mitti acelerar o desenvolvimento de nossa funcionalidade, automatizar o trabalho manual, melhorar as ferramentas e possibilitar melhores resultados para os clientes.

Usamos infraestrutura de IA auto-hospedada e provedores de IA de terceiros.

Funcionalidades de IA na Mitti

Dentro da Mitti, temos uma IA que pode ajudar os usuários a fazer perguntas sobre seus dados, gerar resumos, criar conteúdo, traduzir, encontrar insights e obter recomendações.

Provedores de IA e segurança

A Mitti utiliza grandes modelos de linguagem (LLMs) hospedados pela Mitti e por empresas terceiras, como Anthropic, Google e AWS.

Avaliamos continuamente os provedores de LLM e seus modelos para fornecer a experiência da mais alta qualidade aos nossos usuários. Os terceiros que processam dados de clientes, incluindo serviços terceirizados de IA, estão publicados em nossa página de subprocessadores encontrada aqui: https://mitti.com/legal/privacy-sub-processors

Acesso e controles

As funcionalidades de IA reconhecem permissões e respeitam as estruturas de permissões existentes, portanto, os usuários acessam apenas o conteúdo que estão autorizados a ver. Somente usuários autorizados, como administradores, podem atualizar permissões, conceder ou retirar o acesso de um usuário às funcionalidades de IA.

Dados do cliente e modelos de treinamento

Os clientes determinam quais dados são passados para os provedores de IA e como usar os resultados do processamento de IA.

A Mitti não permite que serviços de terceiros usem dados de clientes para treinar os modelos que usamos.

Recursos adicionais

A Mitti se dedica a ser transparente com nossos clientes sobre nossos produtos e como usamos a IA para aprimorar a experiência de nossos usuários. Se houver interesse, aqui estão os recursos adicionais:

- IA na Mitti
- Seus dados na Mitti
- Subprocessadores de seus dados

Conclusão

A Mitti considera a segurança cibernética uma parte fundamental do nosso negócio e dos serviços que fornecemos às empresas em todo o mundo. Embora os controles e as medidas que temos em vigor se estendam significativamente além do que é abordado aqui, este conteúdo serve para fornecer uma compreensão geral da abordagem multifacetada que adotamos e de nosso compromisso com a segurança.

Se você tiver dúvidas sobre este conteúdo ou precisar de mais informações sobre nossa abordagem de suporte, segurança ou privacidade, entre em contato conosco pelos dados abaixo.

- **Suporte:** support@mitti.com
- **Privacidade:** privacy@mitti.com

Para relatar problemas de segurança, entre em contato conosco em

Leitura adicional

Nossa página de segurança: https://mitti.com/pt-BR/seguranca

Nosso portal de privacidade: https://www.mitti.com/pt-BR/juridico/portal-de-privacidade

Nossa página de status de serviço: https://status.mitti.com