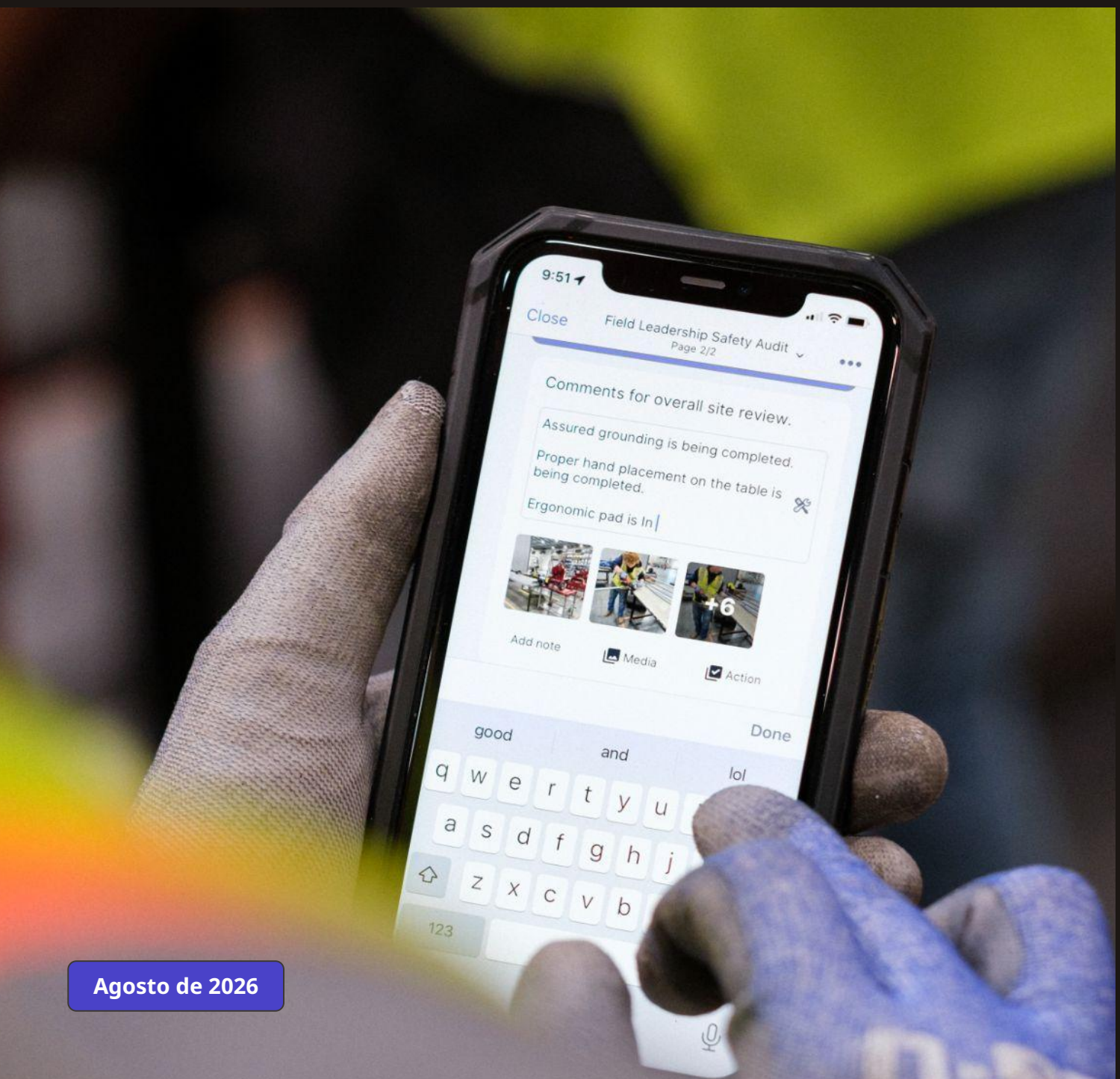
Mitti
by SafetyCulture

Resumen de seguridad

Descubra la ciberseguridad de Mitti



Agosto de 2026

Tabla de Contenido

“Antes de Mitti, necesitábamos que alguien ingresara todos los datos de la lista de verificación una vez que regresara a la oficina, luego ejecutara estadísticas en Excel y, finalmente, los compartiera con el equipo. Estadísticas nos proporciona datos más completos en un área que podemos compartir.”

Deaky Wong

Ingeniero de mantenimiento de conductos, Cathay Pacific

Nuestra misión

La misión de Mitti es ayudar a las empresas a lograr lugares de trabajo más seguros y de mayor calidad en todo el mundo a través de productos innovadores y de bajo costo para dispositivos móviles.

Cumplimos con nuestra misión a través de nuestros productos de software como servicio (SaaS).

Nuestros productos son utilizados por más de 85.000 empresas de todo el mundo en muchas industrias en diversos casos de uso.

Nos enorgullece que Mitti sea visto como un líder mundial en productos que promueven la seguridad y la calidad, y sabemos lo importante que es para ayudar a nuestros clientes a mejorar sus operaciones diarias.

Consideramos nuestro enfoque en la seguridad cibernética como un pilar clave para mantener nuestro estatus como un líder en este espacio y este contenido proporciona un resumen de cómo abordamos la ciberseguridad como organización.

Mitti cuenta con la certificación ISO 27001:2024 y seguimos los criterios de servicios de confianza de la AICPA, lo que demuestra nuestro compromiso con la seguridad de los clientes.

A-LIGN ISO 27001 CERTIFIED

A-LIGN SOC 2

STAR LEVEL ONE: SELF-ASSESSMENT
STAR LEVEL ONE
SECURITY TRUST ASSURANCE & RISK

Introducción

Programa de seguridad cibernética

Mitti cuenta con un programa de seguridad cibernética activo, sólido y en constante mejora para garantizar que nuestra organización y los productos que ofrecemos sean seguros. El programa de seguridad cibernética de Mitti emplea una serie de controles a nivel técnico y operativo para garantizar que tengamos un enfoque eficaz y totalmente defensivo para protegernos de los ataques cibernéticos y asegurar los datos manejados por nuestros productos con software como servicio (SaaS).

Las funciones clave incluyen:

Un programa de seguridad alineado con los estándares de mejores prácticas de la industria, incluido el uso de plataformas en la nube que cumplen con los fiables puntos de referencia de seguridad, incluidos ISO 27001 y SOC 2.

Un enfoque en hacer lo básico correctamente, reconociendo que los fundamentos de la seguridad siguen siendo los más importantes.

Esto incluye:

- Formar a nuestro personal sobre la importancia de la seguridad.
- Contar con un equipo de seguridad dedicado que sea responsable de mantener nuestra organización segura frente a amenazas reales e inminentes para nuestro negocio y los datos que los clientes nos confían.
- Emplear mecanismos resilientes para garantizar que el acceso a los sistemas de Mitti y los datos de los clientes se controlen cuidadosamente.
- Cifrar los datos de los clientes que tenemos (tanto en tránsito como en reposo).
- Asegurarnos de que aplicamos parches dentro de nuestro entorno de TI y a nuestros productos lo más rápido posible para minimizar la oportunidad de que los atacantes cibernéticos exploten las vulnerabilidades.
- Supervisar y probar activamente nuestro entorno de TI y nuestros productos en busca de vulnerabilidades y remediarlas lo más rápido posible.
- Contar con un proceso definido para brindar soporte y respuesta efectivos en caso de un incidente de seguridad.

Aplicar la debida diligencia para garantizar que nuestros proveedores de servicios cumplan con los estándares de la industria en lo que respecta a seguridad: sabemos que la seguridad de nuestros socios nos afecta directamente a nosotros y a nuestros clientes, por lo que elegimos con mucho cuidado con quién trabajamos.

El resto de este documento proporciona un resumen de las diversas partes de nuestro programa de seguridad.

Prácticas de seguridad organizacional

Nuestro enfoque para la seguridad como empresa se centra en alinearnos con las mejores prácticas recomendadas en estándares reconocidos como NIST, ISO 27001 y SOC.

Gobernanza de seguridad

Mitti tiene un conjunto documentado de políticas, estándares y procedimientos que definen nuestro enfoque para la seguridad como organización. Estas políticas y procedimientos se comparten con todo el personal y se revisan y actualizan al menos una vez al año (y con mayor frecuencia cuando se requieren cambios importantes) para garantizar que nuestro enfoque de seguridad se mantenga actualizado
.
Nos centramos en garantizar la rendición de cuentas para la seguridad en toda nuestra empresa. Con este fin, hemos establecido un foro de gestión de seguridad de la información con partes interesadas clave de toda Mitti que se reúnen periódicamente para revisar y analizar asuntos relacionados con la seguridad, y tomar las decisiones que influyen en nuestro enfoque de ciberseguridad.

Mitti cuenta con la certificación ISO 27001:2024 y seguimos los criterios de servicios de confianza de la AICPA, lo que demuestra nuestro compromiso con la seguridad de los clientes.

Controles de acceso

Nos aseguramos de que el acceso a los sistemas de nuestro entorno de TI, incluidas las plataformas en la nube que utilizamos, esté restringido a los empleados que específicamente requieren este acceso para su trabajo.

Todo acceso de administrador requiere una autenticación multifactor y los empleados que acceden a nuestro entorno deben utilizar una solución VPN aprobada.

Los permisos de acceso a nuestros sistemas se revisan periódicamente, empleado por empleado, y se modifican sin demora. Como parte de nuestro proceso de baja, se revoca todo el acceso a los sistemas y servicios de los empleados que se marchan de la empresa.

Prácticas de seguridad organizacional

Seguridad de terceros

Revisamos cuidadosamente las prácticas de seguridad de terceros con los que colaboramos, inicial y activamente para garantizar que sus prácticas cumplan con los estándares de la industria y con nuestras propias políticas y procedimientos de privacidad y seguridad. Si un tercero requiere acceso a nuestros sistemas, nos aseguramos de que el acceso se limite específicamente al propósito para el cual se ha contratado.

Como Amazon Web Services (AWS) es uno de nuestros principales proveedores, nos relacionamos con ellos utilizando el modelo de responsabilidad compartida para la seguridad y el cumplimiento, garantizando que haya una definición clara de quién asume la responsabilidad de qué en materia de seguridad. AWS está acreditado y cumple con muchos de los últimos estándares de la industria; puede encontrar más información aquí: https://aws.amazon.com/artifact.

Para el procesamiento de datos financieros y de tarjetas de crédito, Mitti utiliza varios socios (Zuora, eWay y Stripe) cuyas prácticas de seguridad cumplen con el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI-DSS).

Seguridad de la red

Las redes corporativas de Mitti están protegidas con firewalls, así como con tecnología de sistema de detección de intrusiones (IDS) y sistema de prevención de intrusiones (IPS) en el perímetro, proporcionados por dispositivos de seguridad de red dedicados, para que podamos detectar y protegernos contra cualquier tráfico malicioso.

Para nuestras plataformas basadas en la nube, utilizamos principalmente Amazon Web Services (AWS), que proporciona una estrategia de capas múltiples para defendernos de ataques externos. A nivel de infraestructura, AWS emplea estrategias como el control de acceso a dispositivos de red, segregación de datos mediante firewalls y nubes privadas virtuales para filtrar el tráfico malicioso y hacer uso de registros y control extensos para prevenir ataques basados en la red. A nivel de aplicación, aprovechamos el Firewall de Aplicaciones Web (WAF) y la protección contra Ataques de Denegación de Servicio Distribuido (DDoS) de Cloudflare para prevenir ataques basados en la web y ataques de denegación de servicio contra nuestros productos.

Separamos nuestros entornos de desarrollo, prueba y producción.

Prácticas de seguridad organizacional

Registro y supervisión

Mitti utiliza un sistema de registro centralizado, que incluye eventos de auditoría de acceso a las aplicaciones. Estos registros se conservan durante 90 días. También utilizamos los registros de Amazon Elastic Load Balancing (ELB) para rastrear las solicitudes de acceso al servicio. Los registros almacenados en AWS no se pueden modificar y el acceso está restringido a quienes lo requieran para cumplir con los requisitos de su función.

Reconocemos la importancia de revisar los registros periódicamente para identificar la actividad maliciosa de los usuarios e identificar posibles vulnerabilidades en nuestros productos; contamos con una supervisión automatizada que nos alerta sobre tipos específicos de eventos potencialmente maliciosos dentro de nuestra infraestructura global.

Formación en concienciación sobre seguridad

Todo el personal de Mitti recibe formación periódica en concienciación sobre seguridad para funciones técnicas y no técnicas. Se proporciona material adicional de formación en seguridad al personal individual cuando sea necesario para garantizar que estén equipados para manejar los desafíos específicos de su función orientados a la seguridad.

Gestión de parches y vulnerabilidades

La aplicación de parches en nuestro entorno de TI es una de las medidas más importantes que tomamos para mantenernos seguros ante una posible brecha de seguridad. Para lograrlo:

- Utilizamos AWS System Manager para implementar parches periódicamente en nuestra infraestructura basada en la nube.
- Utilizamos soluciones de gestión de dispositivos móviles para garantizar que los parches importantes se instalen de manera rápida y eficiente.
- Nuestros dispositivos están protegidos con tecnologías de seguridad de terminales para detectar y prevenir amenazas en la seguridad, incluidos virus y ataques de malware, y supervisar actividades maliciosas.
- Primero aplicamos los parches para las vulnerabilidades más críticas; estos se instalan primero en nuestro entorno de pruebas para realizar las pruebas iniciales antes de extenderse rápidamente por todo el entorno informático.

Protección de datos de clientes

Mitti se toma muy en serio la seguridad de los datos de nuestros clientes. Tomamos una serie de medidas para garantizar que los datos de los clientes estén cuidadosamente protegidos.

Protección de los datos del cliente

Restricción del acceso a los datos

Mitti implementa controles técnicos y organizacionales para ayudar a proteger los datos de los clientes contra el acceso o uso inadecuado por parte de personas no autorizadas (ya sean externas o internas). Los datos de los clientes solo se almacenan en nuestro entorno de producción, y el acceso a esos datos por parte de los empleados de Mitti está limitado únicamente a los empleados que requieran acceso para realizar sus tareas básicas. El acceso a los datos de los clientes se gestiona mediante herramientas de autenticación y control de acceso (incluido el uso de autenticación de dos factores) proporcionadas por Amazon Web Services y nuestros otros socios en la nube.

Los datos de los clientes sólo se utilizan para fines compatibles con la prestación de los servicios contratados, como la resolución de problemas en solicitudes de soporte técnico. Para obtener más detalles, consulte la Política de privacidad de Mitti que se encuentra aquí: https://mitti.com/es/legal/politica-de-privacidad/.

Cuando los empleados de soporte técnico de Mitti necesitan acceder a datos específicos de un cliente (con fines de resolución de problemas o soporte técnico), Mitti siempre requerirá el consentimiento del cliente antes de acceder a dichos datos.

No guardamos ni almacenamos en caché los datos financieros de los clientes utilizados para la facturación a través de la plataforma de Mitti y nuestros empleados no tienen acceso directo a los datos de facturación.

Acceso físico a los datos

Los datos de los clientes están alojados en infraestructura proporcionada por Amazon Web Services, que mantiene la seguridad de sus sitios mediante controles de mejores prácticas de la industria, tal como se describe en su sitio web de seguridad y cumplimiento, disponible aquí: https://aws.amazon.com/architecture/security-identity-compliance/.

No se almacenan datos de clientes en nuestras oficinas físicas.

Cifrado de datos

Mitti cuenta con mecanismos para garantizar que los datos de nuestros clientes estén siempre protegidos.

Cuando están en reposo, todos los datos de los clientes almacenados en los sistemas se cifran mediante AES-256 con claves gestionadas a través del Servicio de gestión de claves de Amazon Web Services. Todos los datos se almacenan de forma segura y están sujetos a las políticas y procedimientos de seguridad de AWS.

Para proteger los datos en tránsito, Mitti utiliza Transport Layer Security (TLS) y aplica un estándar mínimo de TLS v1.2 utilizando claves de cifrado de 128 bits. Somos compatibles con conexiones con claves de cifrado de hasta 256 bits para usar con un cifrado AES.

Copias de seguridad de datos

Los datos de Mitti se respaldan diariamente en soluciones de almacenamiento de datos cifrados y dispersos proporcionadas por Amazon Web Services. Las copias de seguridad se replican en varias instalaciones de AWS y se conservan durante al menos 30 días.

El acceso a las copias de seguridad de los datos está restringido únicamente a aquellos empleados concretos de Mitti que lo necesiten para desempeñar sus funciones. Las copias de seguridad están cifradas y se almacenan en modo de solo lectura.

Eliminación y disposición de datos

Los datos de nuestros clientes se almacenan en los sistemas de Amazon Web Services y están sujetos a sus procedimientos de eliminación y disposición. Estos procedimientos incluyen un proceso para borrar los archivos multimedia retirados seguros. Luego se inspeccionan los archivos multimedia borrados para garantizar la destrucción exitosa de los datos.

Cualquier hardware propiedad de Mitti que contenga datos confidenciales (incluidas las copias de seguridad de Mitti) está sujeto a la destrucción de datos lógica estándar de la industria antes de su reciclaje.

Seguridad de nuestros productos

Sabemos que para la mayoría de los clientes, su principal experiencia con Mitti será a través de nuestros productos. La seguridad es una parte importante en la forma en que se desarrollan y operan nuestros productos.

Prácticas seguras de desarrollo de software

Como parte de nuestro proceso de desarrollo de productos, cada cambio en el código e infraestructura se almacena en un sistema de control de código fuente, versionado, revisado y evaluado en su impacto antes del lanzamiento del cambio para la producción. Esta revisión incluye la observación de las mejores prácticas de seguridad. También separamos nuestros entornos de desarrollo, prueba y producción, y no utilizamos los datos de los clientes en nuestros entornos que no son de producción.

Control de cambios

Todos los cambios en los productos de Mitti se prueban activamente durante su desarrollo para garantizar que el impacto en los usuarios finales se evalúe antes de la implementación, y cualquier cambio significativo se incluye en las notas de la versión de producción.

Mitti emplea sistemas de seguimiento de cambios y control de versiones para supervisar y gestionar activamente los cambios en la base de código o la configuración de nuestros productos. Utilizamos un proceso automatizado para implementar cambios en nuestros entornos y podemos revertir los cambios según sea necesario. Usamos Amazon CloudTrail para rastrear cualquier cambio de configuración subyacente en la plataforma en nube en la que operan nuestros productos.

Identificación de vulnerabilidades y desarrollo de parches

Trabajamos arduamente para minimizar la cantidad de vulnerabilidades que surgen en nuestros productos y sabemos que es importante tomar medidas proactivas para asegurarnos de abordar cualquier vulnerabilidad lo más rápido posible. Con ese fin, Mitti realiza pruebas de penetración anuales, y prueba y supervisa activamente las vulnerabilidades en nuestras aplicaciones. Ejecutamos un programa privado de recompensas en busca de errores sabiendo que una comunidad de investigadores independientes en seguridad incentivados para probar nuestros productos de forma continua e identificar cualquier posible contratiempo servirá para fortalecer la seguridad de nuestros productos.

Cuando se identifica una vulnerabilidad (interna o externamente), el contratiempo se rastrea y se prioriza de acuerdo con la gravedad potencial del impacto para nuestros clientes. Los asuntos de gravedad crítica pueden implicar el trabajo de nuestros desarrolladores las 24 horas del día hasta que ello se resuelva.

Los parches para contratiempos se desarrollan y publican en el entorno de producción a través de un proceso de integración continua (métodos CI/CD) y se aplican lo antes posible.

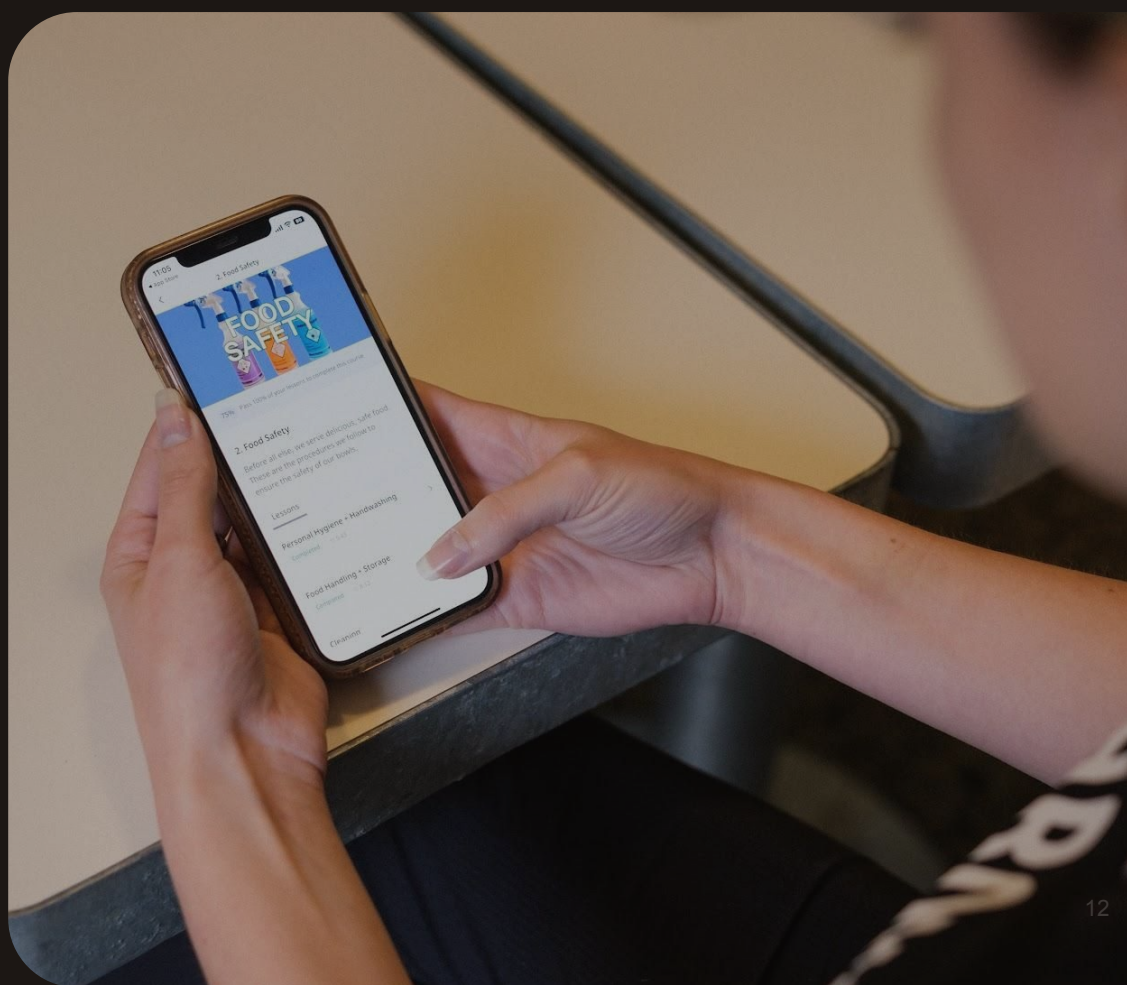
Gestión de incidentes de seguridad

Si bien hacemos todo lo posible para evitar cualquier incidente de seguridad, sabemos que también debemos estar preparados para manejar estos incidentes en caso de que surjan y minimizar el impacto potencial para nuestros clientes y Mitti.

Contamos con una serie de medidas que incluyen:

- Un procedimiento de gestión de incidentes documentado que define nuestro proceso para manejar la confidencialidad, integridad y disponibilidad de nuestro entorno y productos de TI.
- Contar con una organización global para proporcionar soporte técnico durante un incidente.
- Planes de recuperación ante desastres y estrategias de contingencia establecidos que se pueden ejecutar para ayudarnos a mantener la continuidad de las operaciones durante un incidente. Esto incluye el uso de múltiples zonas geográficas de disponibilidad proporcionadas por Amazon Web Services y la replicación de datos en múltiples sistemas en cada zona. Esto asegura el acceso continuo a los datos durante incidentes que afecten a la disponibilidad del sistema y proporciona redundancia de datos en caso de fallos en el sistema o en el almacenamiento de datos.

Mitti notifica de forma inmediata a los clientes afectados sobre incidentes importantes que afecten la disponibilidad de los servicios o datos de Mitti, así como sobre cualquier incidente que afecte la confidencialidad e integridad de sus datos.



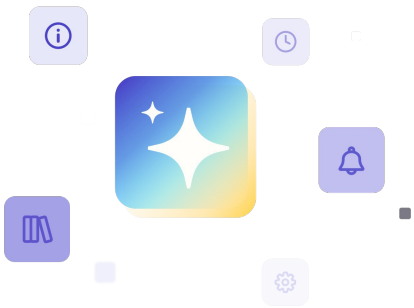
«Tenemos una visibilidad clara de todo lo que hacemos gracias a los datos que recopilamos con Mitti. Si hay un umbral de excepción o un proceso que necesita mejorarse, todo lo que debemos hacer es profundizar en ello y lo encontraremos».

Sofia Dias
Gerente de garantía de calidad y seguridad alimentaria

Marley Spoon

Mitti e IA

Mitti innova continuamente y ofrece a nuestros clientes nuevas funciones y tecnologías de forma segura y confiable. Esto incluye funciones de Inteligencia Artificial (IA). En Mitti, queremos ser transparentes con nuestros clientes sobre cómo usamos la IA para desarrollar nuestros productos y cómo la usamos para mejorar la experiencia de nuestros usuarios.



Cómo Mitti usa la IA

La IA permite a Mitti acelerar el desarrollo de funciones, automatizar trabajos manuales, mejorar las herramientas y lograr mejores resultados para los clientes.

Utilizamos infraestructura de IA propia y proveedores de IA de terceros.

Funciones de IA en Mitti

Dentro de Mitti, contamos con IA que puede ayudar a los usuarios a hacer preguntas sobre sus datos, generar resúmenes, crear contenido, traducir, encontrar información clave y obtener recomendaciones.

Proveedores de IA y seguridad

Mitti utiliza modelos de lenguaje de gran tamaño (LLM) alojados por Mitti y organizaciones de terceros como Anthropic, Google y AWS.

Evaluamos continuamente los proveedores de LLM y sus modelos para ofrecer la experiencia de mayor calidad a nuestros usuarios. Los terceros que procesan datos de clientes, incluidos los servicios de IA de terceros, se publican en nuestra página de subprocesadores disponible aquí: https://mitti.com/legal/privacy-sub-processors

Acceso y controles

Las funciones de IA tienen en cuenta los permisos y respetan las estructuras de permisos existentes, de modo que los usuarios solo acceden al contenido que están autorizados a ver. Solo los usuarios autorizados, como los administradores, pueden actualizar permisos, otorgar o eliminar el acceso de un usuario a las funciones de IA.

Datos de clientes y modelos de entrenamiento

Los clientes determinan qué datos se envían a los proveedores de IA y cómo utilizar los resultados del procesamiento de IA.

Mitti no permite que servicios de terceros utilicen datos de clientes para entrenar los modelos que usamos.

Recursos adicionales

Mitti se dedica a ser transparente con nuestros clientes sobre nuestros productos y cómo usamos la IA para mejorar la experiencia de nuestros usuarios. Si le interesa, aquí encontrará recursos adicionales:

- IA en Mitti
- Sus datos en Mitti
- Subprocesadores de sus datos

Reflexiones finales

Mitti considera que la seguridad cibernética es una parte fundamental de nuestro negocio y de los servicios que proporcionamos a empresas de todo el mundo. Si bien los controles y las medidas que implementamos se extienden significativamente más allá de lo que se aborda aquí, este contenido sirve para brindar una comprensión general del enfoque multifacético que adoptamos y nuestro compromiso con la seguridad.

Si tiene alguna pregunta sobre este contenido o necesita más información sobre nuestro enfoque en el soporte técnico, seguridad o privacidad, contáctenos a través de los siguientes datos.

- **Soporte técnico:** support@mitti.com
- **Privacidad:** privacy@mitti.com

Para informar sobre problemas de seguridad, escríbanos a security@mitti.com

Más lecturas

Nuestra página de seguridad: https://www.mitti.com/es/seguridad/

Nuestro portal de privacidad: https://mitti.com/es/legal/portal-de-privacidad/

Nuestra página de estados de los servicios: https://status.mitti.com/