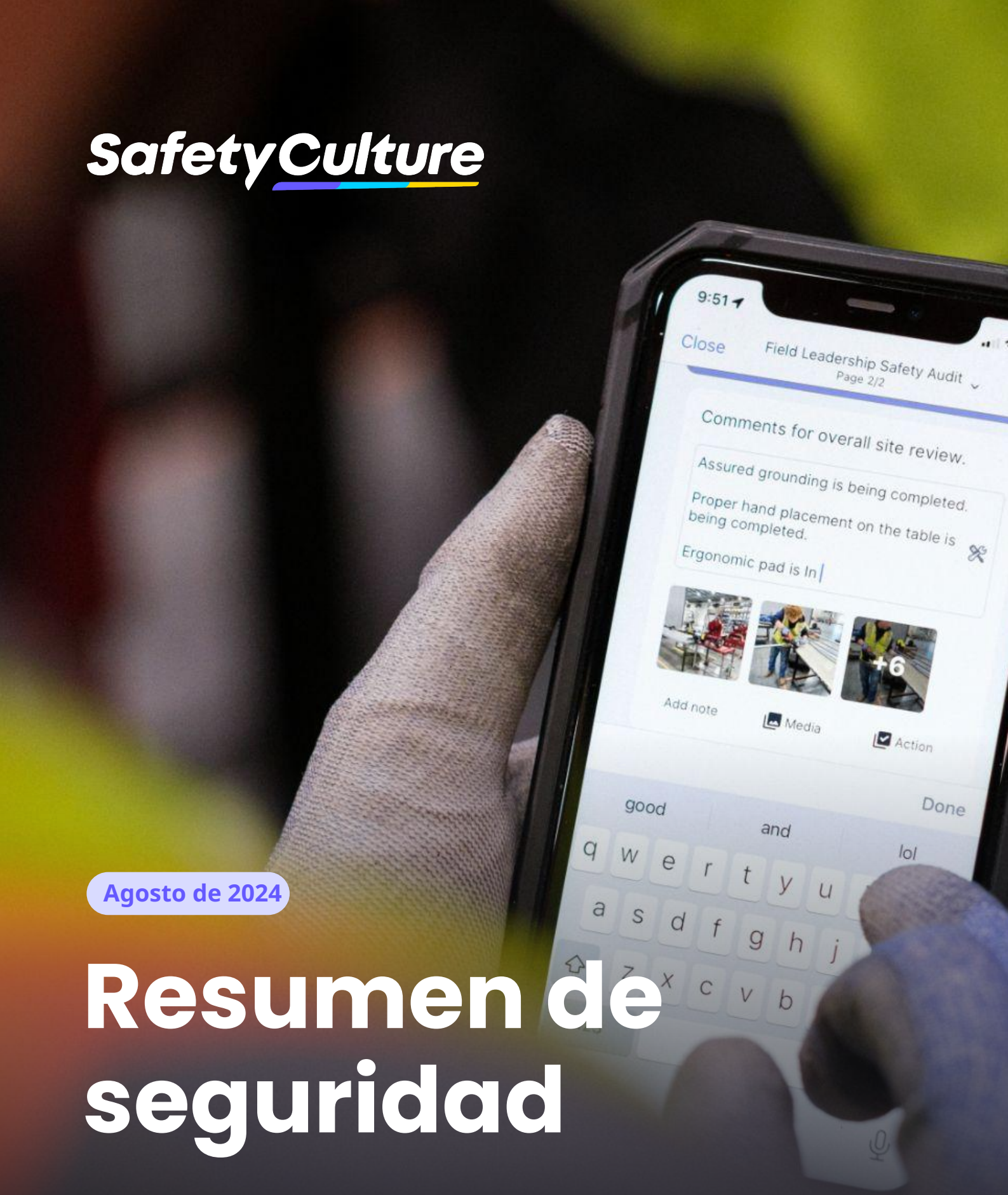
SafetyCulture



Agosto de 2024

Resumen de seguridad

Descubra la ciberseguridad de SafetyCulture

Índice

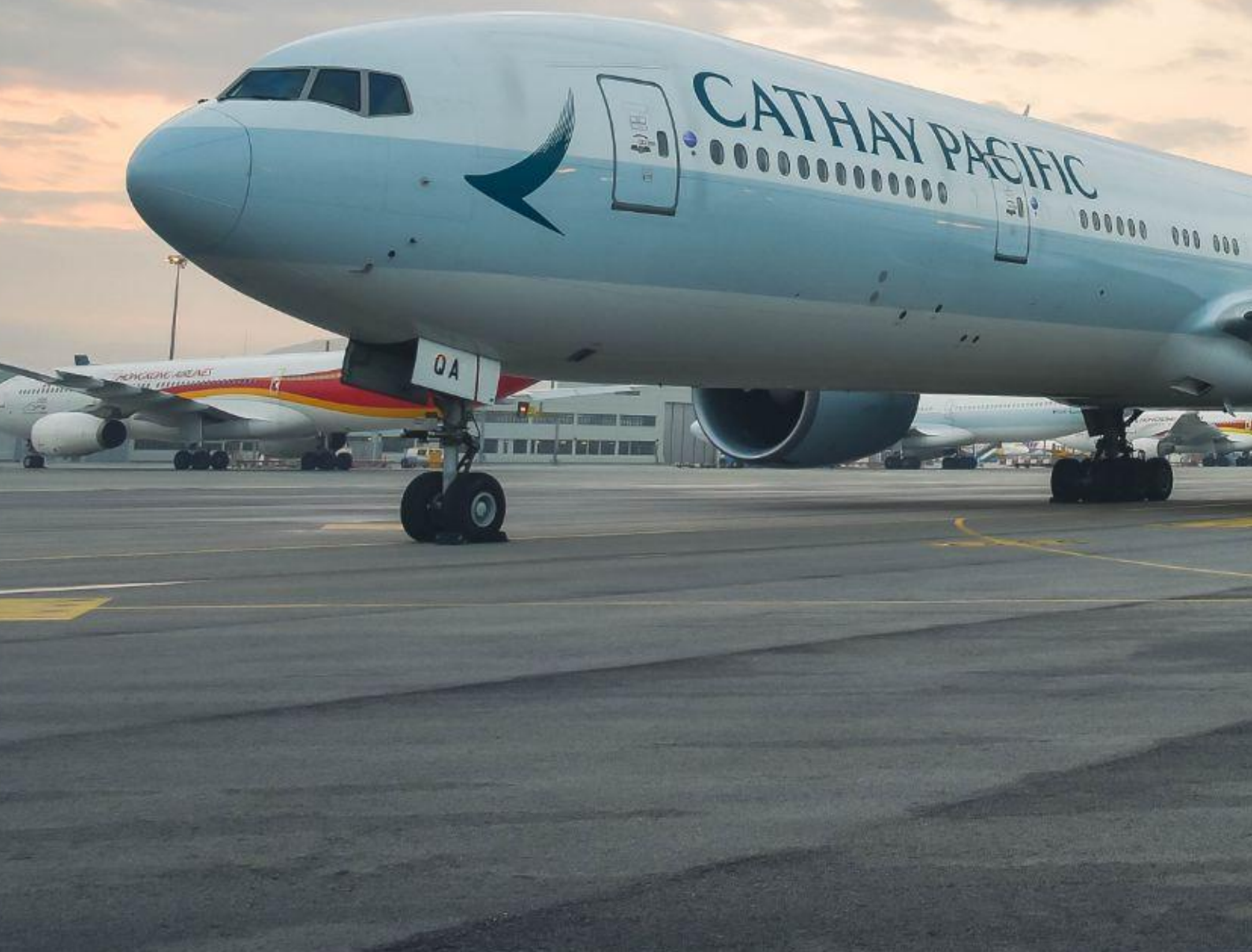
SafetyCulture

“Antes de SafetyCulture, necesitábamos que alguien introdujera todos los datos de la lista de verificación una vez que regresara a la oficina, luego debía ejecutar un análisis de Excel sobre los datos y finalmente compartirlos con el equipo. Estadísticas nos proporciona datos más completos en un área que podemos compartir”.

Deaky Wong

Ingeniero de mantenimiento superior

Cathay Pacific



Nuestra misión

La misión de SafetyCulture 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.

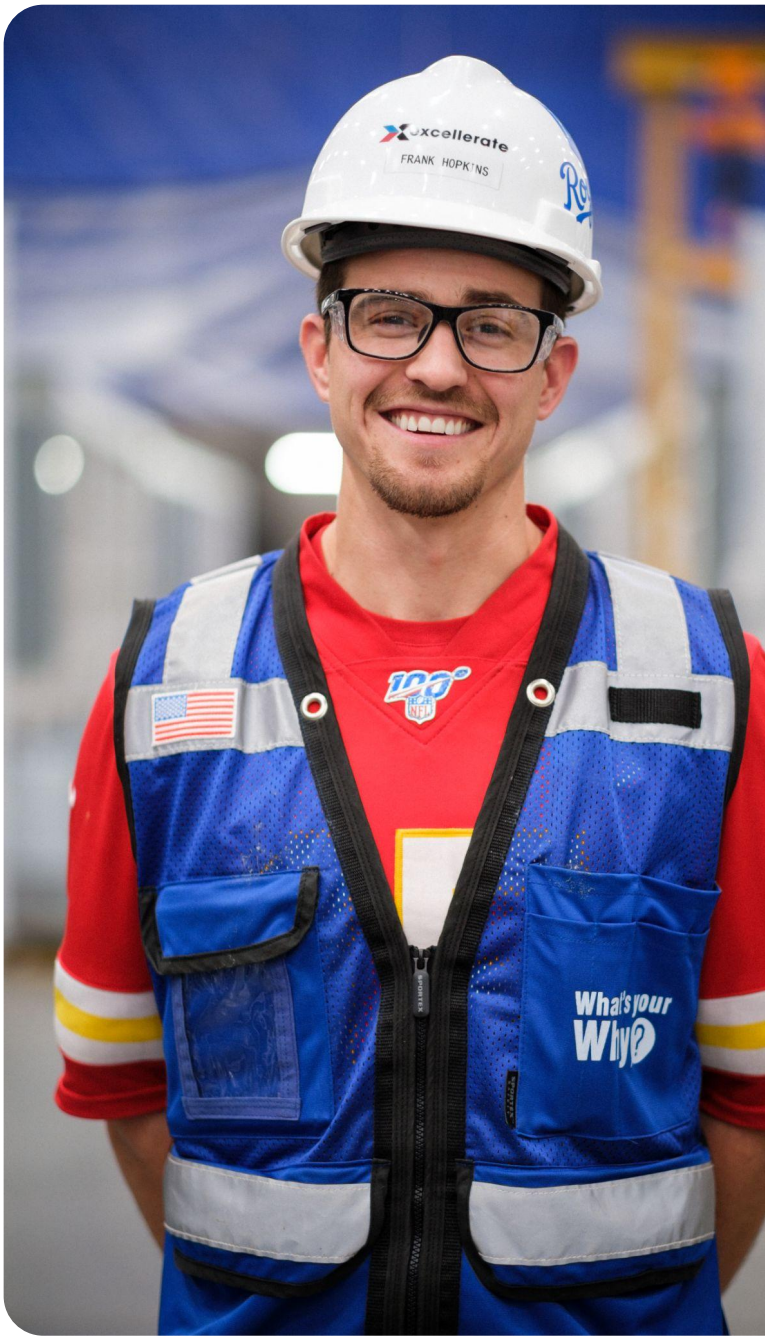
Cumplimos con nuestra misión a través de nuestros productos de software como servicio (SaaS).

Nuestros productos son utilizados por más de 27.000 empresas en todo el mundo en una gran cantidad de industrias y para una variedad de casos de uso.

Nos enorgullece que SafetyCulture 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.

SafetyCulture 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.



Resumen

Programa de seguridad cibernética

SafetyCulture 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 SafetyCulture 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).

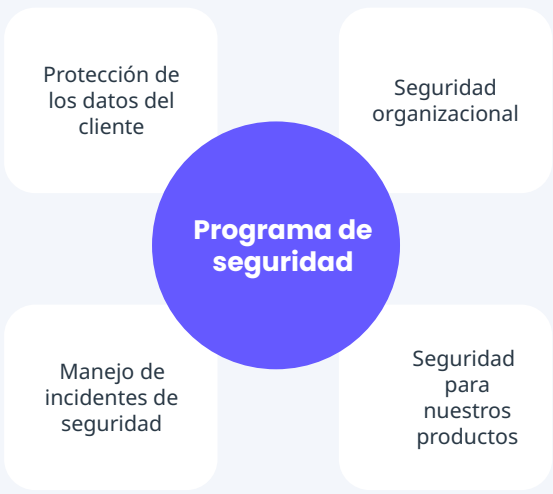
Las características clave incluyen:

- 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 aquello básico correctamente, reconociendo que los fundamentos de la seguridad siguen siendo los más críticos. Esto incluye:

  ➔ Formar a nuestra fuerza laboral 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 SafetyCulture y los datos de los clientes se controlen cuidadosamente.
  ➔ Cifrar los datos de los clientes que tenemos (tanto en tránsito como en reposo) utilizando mecanismos de cifrado robustos.
  ➔ 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

SafetyCulture 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 materiales) 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, contamos con un foro de gestión de seguridad de la información creado con las partes interesadas clave de todo SafetyCulture que se reúnen periódicamente para revisar y abordar asuntos relacionados con la seguridad y tomar decisiones que influyen en nuestro enfoque para la seguridad cibernética.

SafetyCulture 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 requieren específicamente 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 acceso a sistemas y servicios a los empleados que se van de la empresa.

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, SafetyCulture utiliza varios socios (Chargify, 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 SafetyCulture están protegidas con firewalls, así como con un sistema de detección de intrusiones (IDS) y tecnología de sistema de prevención de intrusiones (IPS) en el perímetro, provistos de dispositivos de seguridad de red dedicados para que podamos detectar y proteger 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 de Cloudflare (WAF) y la protección de denegación de servicio distribuida (DDoS) para evitar ataques web y de denegación de servicio contra nuestros productos.

Separamos nuestros entornos de desarrollo, prueba y producción.

Registro y supervisión

SafetyCulture 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 registros de Amazon Elastic Load Balancing (ELB) para rastrear las solicitudes de acceso al servicio (exitosas o no). 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 SafetyCulture 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 a nuestro entorno de TI es una de las medidas más importantes que tomamos para mantenernos seguros frente a posibles violaciones de seguridad. Para lograr esto:

- 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 implementamos parches para las vulnerabilidades más críticas, y los parches se implementan en nuestro entorno no productivo para realizar pruebas iniciales antes de propagarse rápidamente por todo el entorno de TI.

Nuestro foco de atención

Protección de datos del cliente

SafetyCulture 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.

Protecting customer data

Restringir el acceso a datos

SafetyCulture toma varias medidas para ayudar a proteger los datos de los clientes del acceso o uso inapropiado 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 SafetyCulture 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 SafetyCulture que se encuentra aquí: https://safetyculture.com/es/legal/politica-de-privacidad/.

Cuando los empleados de soporte de SafetyCulture necesiten acceder a datos específicos de un cliente (para resolución de problemas o con fines de soporte), SafetyCulture siempre requerirá el consentimiento del cliente antes de acceder a estos datos.

No guardamos ni almacenamos en caché los datos financieros de los clientes utilizados para la facturación a través de la plataforma de SafetyCulture 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 una infraestructura proporcionada por Amazon Web Services, que mantiene la seguridad de sus sitios utilizando controles de buenas prácticas de la industria, como se describe en su sitio web de seguridad y cumplimiento que se encuentra aquí: https://aws.amazon.com/architecture/security-identity-compliance/.

No se almacenan datos de clientes en nuestras oficinas físicas.

Cifrado de datos

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

En reposo, todos los datos de los clientes almacenados en los sistemas se cifran mediante AES-256 con claves administradas 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, SafetyCulture 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 SafetyCulture se guardan a intervalos regulares en distintas soluciones de almacenamiento de datos cifrados proporcionadas por Amazon Web Services. Las copias de seguridad se replican en varias instalaciones de AWS dentro de la región del cliente (APAC, EE. UU. o UE).

El acceso a las copias de seguridad de datos está restringido únicamente a aquellos empleados específicos de SafetyCulture para los que ese acceso es necesario como parte de los requisitos de su función. Las copias de seguridad están cifradas y se almacenan en modo de solo lectura.

Borrado y eliminación de datos

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

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

Asegurar nuestros productos

Sabemos que para la mayoría de los clientes, su principal experiencia con SafetyCulture 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 SafetyCulture 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.

SafetyCulture 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, SafetyCulture 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.

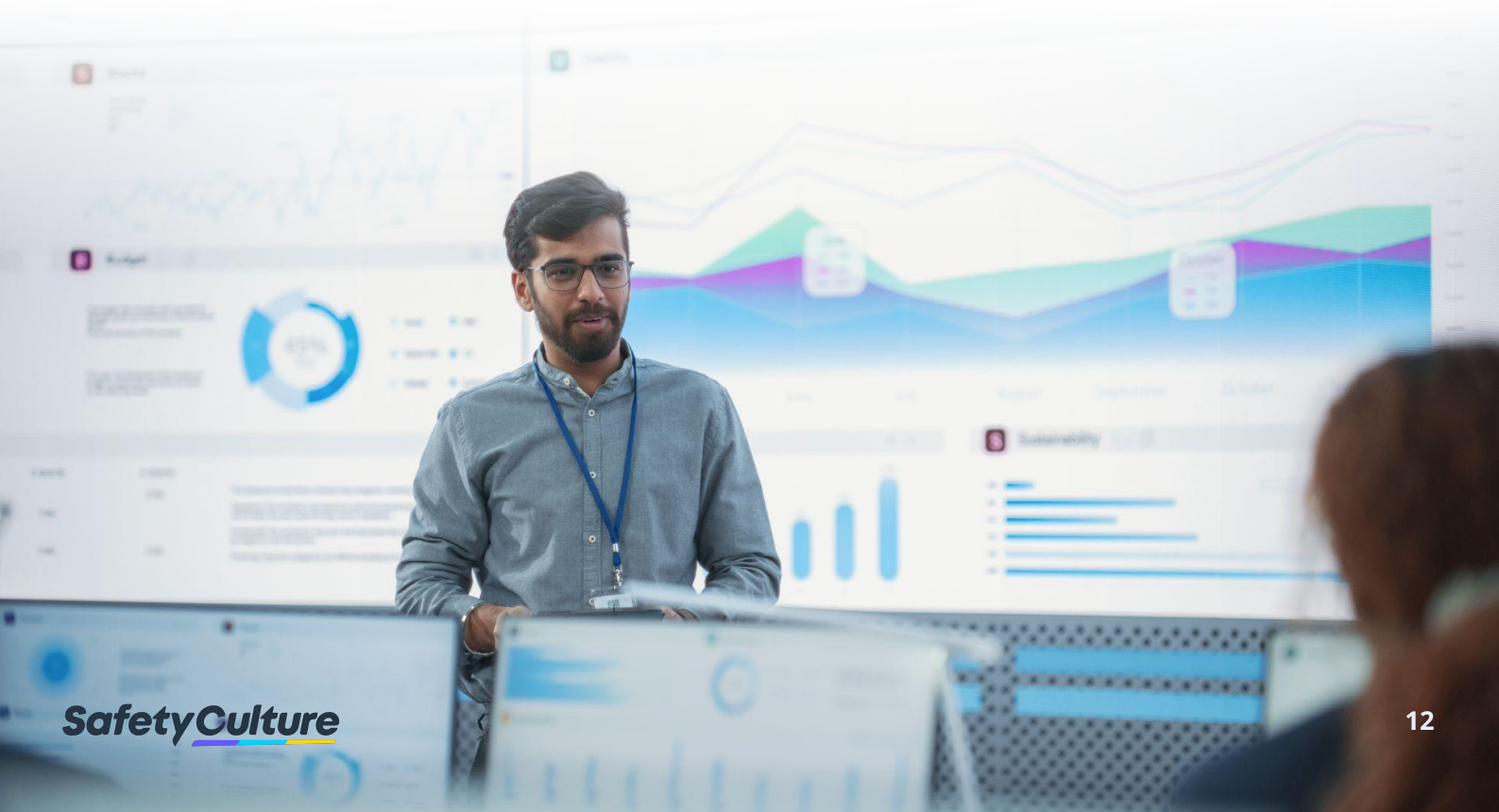
Manejo de incidentes de seguridad

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 SafetyCulture.

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.

SafetyCulture alerta de inmediato a los clientes afectados sobre los principales incidentes que afecten a la disponibilidad de los datos o servicios de SafetyCulture y sobre cualquier incidente que afecte a la confidencialidad e integridad de sus datos según la Política de Privacidad de SafetyCulture se aquí presente: https://safetyculture.com/es/legal/politica-de-privacidad/

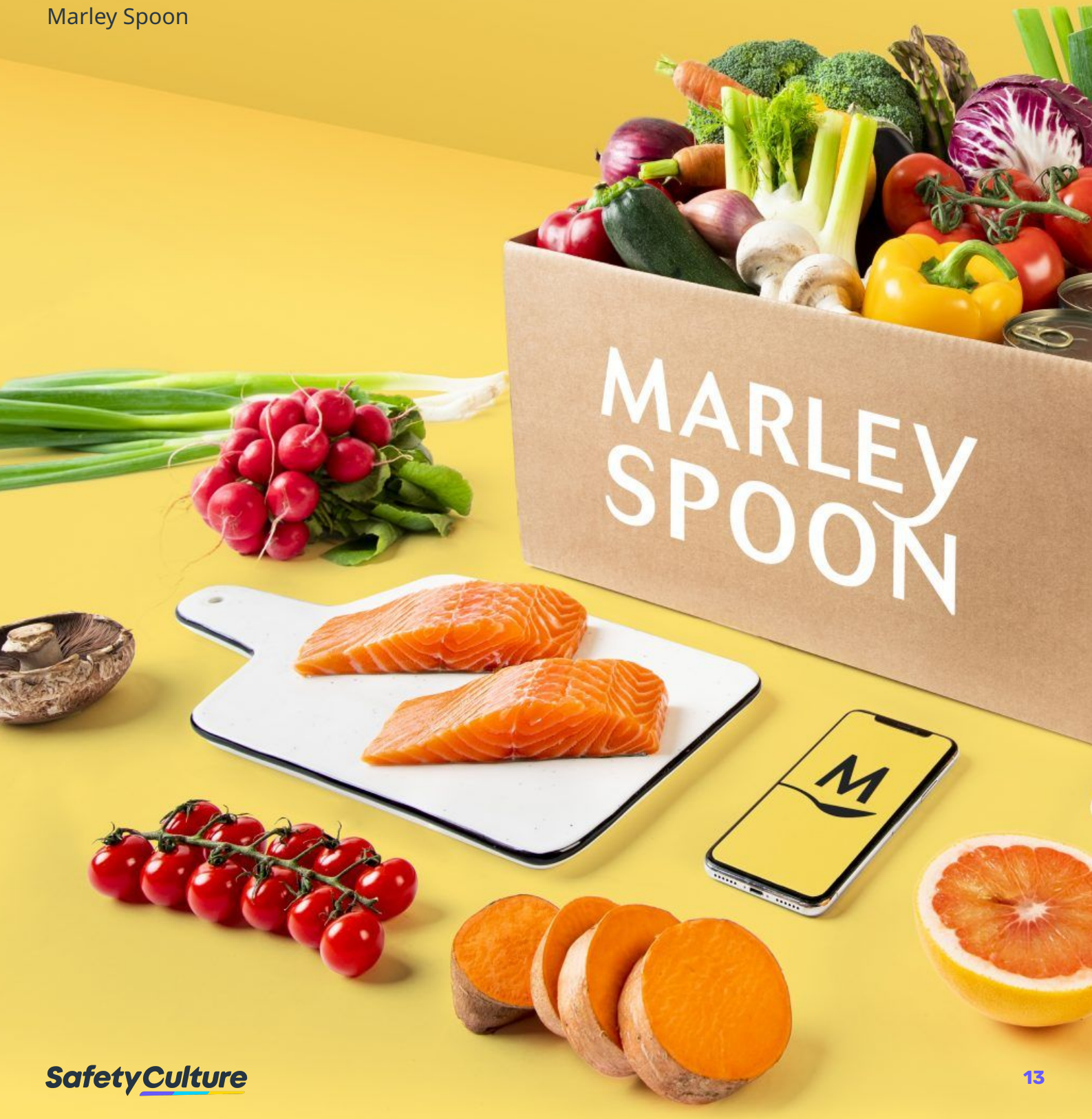


“Tenemos visibilidad sobre todo lo que hacemos gracias a los datos que capturamos con SafetyCulture. Si hay una excepción en un umbral o un proceso que necesita mejorarse, todo lo que tenemos que hacer es profundizar en ello y lo encontraremos”.

Sofia Dias

Gerente de Garantía de Calidad y Seguridad Alimentaria

Marley Spoon



Reflexiones finales

SafetyCulture 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, seguridad o privacidad, contáctenos a través de los siguientes datos.

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

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

Más lecturas

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

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

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