aircall

Información general sobre seguridad

Qué contiene este documento

Introducción

Aircall se toma muy en serio la seguridad de la información y el cumplimiento de sus normas. El propósito de este documento es asegurar a nuestros clientes que sus datos se tratan de acuerdo con sus exigencias en cuanto a protección de datos y cumplimiento de normas, así como ofrecer una total transparencia y garantizar a los clientes de Aircall que su información está en buenas manos.

Nuestros controles y mecanismos de seguridad se basan en la normativa ISO 27001 para la seguridad de la información y los estándares del NIST (Instituto Nacional de Estándares y Tecnología estadounidense), que incluyen programas sobre políticas y procedimientos, control de acceso, continuidad operativa, seguridad de RR. HH., seguridad de la infraestructura de redes, seguridad de terceros, gestión de vulnerabilidades y respuesta a incidentes.

Organización de la seguridad

Aircall tiene un equipo dedicado a la seguridad de la información que se encarga de todos los temas relativos a la seguridad de la empresa.

Este equipo cuenta con diversas certificaciones y credenciales que acreditan sus competencias en el campo.

Seguridad en recursos humanos

Verificación de antecedentes y contratos de confidencialidad

Los empleados de Aircall se someten a una verificación de antecedentes llevada a cabo por terceros antes de recibir una oferta formal de trabajo, siempre que las leyes y las normativas laborales del país en el que estén ubicados lo permitan. Asimismo, todos los empleados de Aircall están obligados a firmar contratos de confidencialidad antes de que se les dé acceso a los sistemas o a los datos de la empresa.

Concienciación y formación

La formación es la base de un programa de seguridad de la información efectivo y, sin ella, los controles técnicos no servirán para proteger los datos de los clientes y demás información confidencial.

Todos los empleados nuevos están obligados a asistir a una sesión de formación durante su proceso de incorporación. Esta sesión tiene como objetivo precisar cuáles son sus responsabilidades, especialmente respecto a la protección contra amenazas internas, ransomware e ingeniería social, así como al uso correcto de los recursos y otros temas relacionados.

Tras este proceso inicial, su formación continúa con, al menos, actualizaciones bimensuales, notificaciones y comunicaciones internas.

Identificación y gestión del acceso

Aircall sigue un proceso formal para autorizar o revocar el acceso a sus recursos. El acceso al sistema se basa en los conceptos de «dar la menor cantidad de privilegios posible» y «qué se necesita» para garantizar que el acceso autorizado sea coherente con las responsabilidades definidas. Además, todos los empleados están obligados a usar una identificación única para acceder a los sistemas de la empresa.

Aircall también aplica una política estándar sobre las contraseñas de la empresa, la cual obliga a cambiarlas en su totalidad cada 90 días siguiendo determinados criterios: un mínimo de diez caracteres y el uso de caracteres especiales, mayúsculas, minúsculas y números. Asimismo, se exige la autenticación por factores múltiples (mediante, por ejemplo, llaves físicas) y las soluciones de inicio de sesión único.

Los permisos se revisan periódicamente (al menos una vez por trimestre) para garantizar su adecuación a las responsabilidades de los empleados.

Proceso de terminación

Aircall ha establecido un proceso de terminación documentado en el que se determinan las responsabilidades para obtener registros y revocar los permisos de acceso de los empleados que dejen la empresa.

Infraestructura de producto de Aircall

Física y del entorno

Amazon Web Services (AWS) es nuestro proveedor de la infraestructura en la nube. AWS sigue un programa de seguridad auditado que incluye las normativas PCI, ISO 27000 y SOC2. Los controles que han implementado son los siguientes:

- Circuito cerrado de televisión (CCTV)
- Guardias de seguridad
- Suministro eléctrico de emergencia
- Control de la temperatura y la humedad
- Detectores de humo
- Detectores de fugas

Aircall no aloja los sistemas de los productos en sus oficinas.

Seguridad de la red

Aircall divide su sistema en redes independientes para proteger mejor la información confidencial y para separar los servicios públicos de los internos. La información de los clientes que se comparte con Aircall solo está disponible en la red de producción. Asimismo, usamos una combinación de grupos de seguridad, firewalls, detección de intrusiones, sistemas de prevención (IDS/IPS) y firewalls de aplicaciones web para proteger los datos de los clientes.

Tenemos un enfoque de «infraestructura como código» en lo que se refiere a la seguridad de la red y a las reglas de los cortafuegos; contamos además con alertas que identifican diferencias entre la configuración aprobada y los ajustes de producción.

Continuidad operativa y recuperación en caso de desastre

Aircall tiene un proceso de continuidad operativa y recuperación en caso de desastre. Nuestro servicio usa diferentes zonas de disponibilidad de AWS en distintas ubicaciones geográficas para poder seguir funcionando si algo falla en una ubicación. Además, nuestro plan de recuperación se actualiza todos los años.

El objetivo es identificar y aislar de forma rápida y transparente cualquier incidencia que afecte a los clientes. Contamos con una página en la que se puede hacer un seguimiento del funcionamiento de Aircall **(https://status.aircall.io/)** y que se actualiza constantemente hasta que se resuelve dicha incidencia.

Copias de seguridad y recuperación

Se realizan a diario copias de seguridad y se almacenan en el centro de datos de AWS usando el cifrado AES de 256 bits. Además, las pruebas de restauración de las copias de seguridad se hacen, como mínimo, una vez al año.

Cifrado

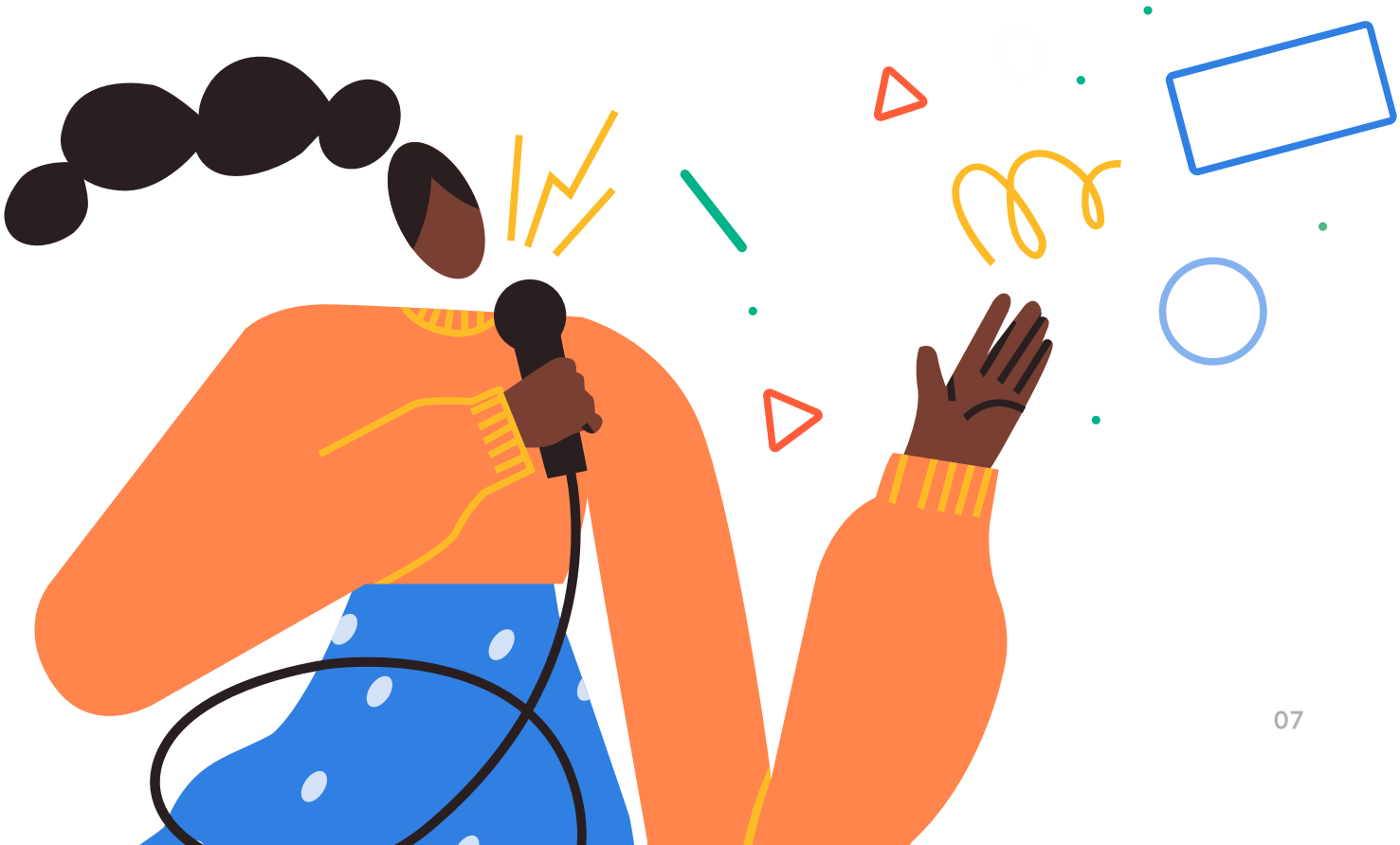
Aircall garantiza que toda la información confidencial de los clientes es cifrada tanto durante su transferencia como en su almacenamiento usando los estándares TLS 1.2 y AES de 256 bits respectivamente. Nuestro equipo de ingenieros usa AWS KMS (servicio de gestión de claves) y el equipo de seguridad gestiona todas las claves de manera centralizada.

Monitorización

Aircall ha incluido herramientas para la revisión de registros y monitorización con el fin de identificar anomalías o violaciones. Al detectarlas, el equipo adecuado se encargará de revisar, investigar y aplicar las correcciones pertinentes.

Nube multiusuario

Aircall es un servicio multiusuario basado en la nube. Los datos de los clientes se dividen de forma lógica, lo que significa que Aircall verifica si el usuario tiene el permiso para hacer las solicitudes. Esto se hace comprobando que la empresa del usuario es la misma que la de los datos solicitados.



Seguridad de aplicaciones

Vulnerabilidad y gestión de parches

Aircall ha implementado procesos para hacer búsquedas periódicas de posibles puntos débiles en sus sistemas de TI. Los resultados se ingresan en nuestro sistema de tickets, se evalúan para establecer el nivel de riesgo y de prioridad y se añaden a los casos pendientes de resolver. Todas las incidencias y los parches que se clasifican como de alto riesgo se resuelven en un plazo de 30 días.

Pruebas de penetración

Aircall hace pruebas de penetración a nivel de aplicación dos veces al año utilizando para ello actores externos independientes. Las amenazas de seguridad y los puntos débiles detectados tienen prioridad, se categorizan y se solucionan a la mayor brevedad. Mediante una petición y tras firmar acuerdos de confidencialidad, es posible obtener los informes.

Además, Aircall cuenta con un programa de recompensas por la identificación de bugs, con el que se recompensa a los investigadores independientes que participen en la identificación y la presentación de fallas de seguridad de los productos de Aircall.

Gestión de cambios

Aircall cuenta con un proceso formal que gestiona los cambios en el entorno de producción de los servicios, incluyendo cualquier cambio en el software, las aplicaciones y los sistemas subyacentes.

Todos los cambios en el código fuente de los sistemas de producción están sujetos a una revisión preliminar del código por parte de un ingeniero, en la que se incluye un análisis de la seguridad, el rendimiento y los riesgos potenciales.

Respuesta a incidentes

Aircall cuenta con procesos documentados para recibir informes sobre incidencias de seguridad. El equipo de seguridad de Aircall sigue un procedimiento documentado que incluye los siguientes pasos:

- Registro
- Categorización
- Investigación
- Control
- Conclusiones

A la hora de actuar frente a cualquier incidencia, primero evaluamos la exposición de la información y verificamos el origen del problema de seguridad, siempre que sea posible. Nos comunicamos con el principal involucrado (y cualquier otro cliente al que le haya afectado el problema) por correo electrónico o teléfono (en caso de que el contacto por correo electrónico no sea suficiente). Además, ofrecemos actualizaciones periódicas para asegurarnos de que la incidencia se resuelve de forma apropiada.

Si tienes cualquier duda sobre la seguridad o has detectado alguna incidencia, envía un mensaje a **report@aircall.io**.

Gestión de proveedores

Aircall cuenta con un programa de gestión de proveedores para garantizar que se hagan todos los controles de seguridad pertinentes. Aircall evalúa periódicamente a cada proveedor (se hace al menos una evaluación al año a los principales proveedores) teniendo en cuenta los estándares de seguridad y continuidad operativa de Aircall, incluyendo el tipo de acceso y la clasificación de los datos a los que se accede (si aplica), los controles necesarios para proteger la información y los requisitos legislativos o normativos.

Aircall firma acuerdos escritos con todos sus proveedores, que incluyen obligaciones de confidencialidad y seguridad que ofrecen el nivel de protección adecuado para todos los datos de clientes que estos proveedores puedan procesar.

Seguridad de endpoints

Todos los portátiles de Aircall se gestionan de forma centralizada y están completamente cifrados. Además, los usuarios no pueden desactivar los antivirus ni ninguna otra medida de seguridad.

Nuestro equipo de TI actualiza los dispositivos periódicamente para asegurarse de que se utilizan las últimas versiones del software instalado.

Privacidad y retención de datos

Aircall tiene un programa de privacidad. Para más información sobre la privacidad y la retención de datos, visita **(https://aircall.io/privacy-faqs/)**.