jamf

Security 360:

Informe anual de tendencias

Dispositivos móviles

Índice

Introducción

Security 360 de Jamf ofrece un análisis detallado del panorama de amenazas en constante evolución; se basa en incidentes reales que fueron detectados en nuestra base de clientes, nuevos hallazgos hechos por nuestros investigadores de amenazas y observaciones de eventos a nivel mundial, nacional y del sector. Esta edición del informe se enfoca en explorar el panorama de las amenazas móviles para poner de relieve los riesgos a los que se enfrentan las organizaciones.

Analizamos los diversos y letales vectores de ataque que utilizan los atacantes para obtener acceso, desplazarse de un sistema a otro y, en última instancia, comprometer los datos o causar daños. Los atacantes aprovechan las vulnerabilidades de los dispositivos y el software, introducen código malicioso en las aplicaciones y las comunicaciones web, y amenazan a los usuarios —el eslabón más débil en las defensas de toda organización— todo ello con el fin de alcanzar sus objetivos.

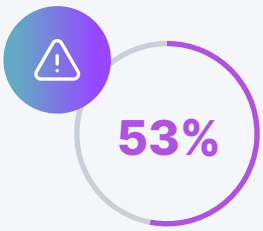
Además de analizar estas tendencias en materia de amenazas, el informe incluye la opinión del director de seguridad de la información (CISO) de Jamf, que ofrece información a los responsables de seguridad y a los profesionales de TI encargados de proteger las flotas de dispositivos móviles.

Metodología de la investigación

Para comprender y cuantificar el impacto real de las tendencias de seguridad identificadas en este informe, hemos analizado de forma anónima una muestra de más de 1.7 millones de dispositivos iOS y Android de nuestra base de clientes. Nuestro análisis se llevó a cabo a finales de 2025, revisando los 12 meses anteriores y abarcando múltiples países de todo el mundo.

Para mantener la privacidad y preservar los más altos estándares al recopilar y manipular datos, los metadatos analizados en nuestra investigación proceden de registros agregados que no contienen información personal o identificativa de la organización.

Aspectos clave



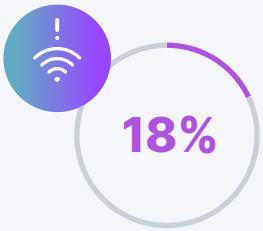
Porcentaje de organizaciones que tenían al menos un dispositivo con un sistema operativo muy desactualizado

Un sistema operativo desactualizado implica vulnerabilidades sin parchar y susceptibles de ser explotadas. Automatizar y aplicar las actualizaciones contribuye en gran medida a proteger sus dispositivos.

1 en 850

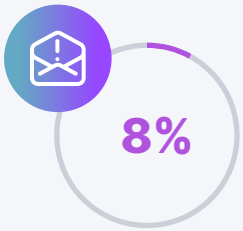
Número de dispositivos que se usan para trabajar, y que tienen jailbreak

Jamf detectó estos dispositivos; las políticas de acceso basadas en el contexto impidieron el acceso a los recursos de la empresa.



Porcentaje de organizaciones cuyos empleados se conectan a puntos de acceso riesgosos

Los puntos de acceso riesgosos abren la puerta a amenazas para la infraestructura, como puntos de acceso no autorizados o ataques por intermediarios, especialmente si los dispositivos no están configurados para hacer frente a este riesgo.



Porcentaje de dispositivos en que el usuario hizo clic en un enlace de phishing.

Los ataques de phishing siguen siendo una táctica muy utilizada por los atacantes para comprometer cuentas, sin grandes cambios año tras año. Sin protecciones adecuadas, las consecuencias pueden ser devastadoras.

Ataques de cero clics y ataques a navegadores

Métodos que siguen siendo populares y eficaces

Siguen apareciendo vulnerabilidades tanto en los sistemas operativos como en el software; estas se convierten en la clave que permite a los atacantes obtener información confidencial a través de múltiples familias de spyware. Este informe destaca la importancia de reducir estratégicamente los riesgos en sus dispositivos móviles.

Principales tendencias en la empresa

Los dispositivos móviles ayudan a los empleados a mantener su productividad independientemente del lugar en el que trabajen. La forma en que administramos y utilizamos estos dispositivos —y las amenazas a las que se enfrentan— determina cómo se protegen.

Su organización se esfuerza cada día por reducir la superficie de ataque de su dispositivo. Usted implementa controles y políticas, y equipa su infraestructura tecnológica con el mejor software de seguridad, pero los atacantes siguen evolucionando y no cejan en su empeño.

Hay muchos elementos que conforman su superficie de ataque. En este informe, hablaremos de los principales riesgos que las organizaciones tienen dificultades para controlar y que los atacantes suelen aprovechar, así como de cómo evitar consecuencias desastrosas.

1. Las vulnerabilidades del software y de los dispositivos forman parte del día a día de las empresas.

A pesar de todo el esmero que implica el desarrollo de los sistemas operativos de sus dispositivos móviles, la perfección es imposible. En 2025 se publicaron más de 48,000 registros de CVE. Son muchas vulnerabilidades que hay que identificar y resolver.

Pero los desarrolladores lo saben, y por eso lanzan parches de seguridad. Ahí es donde entran en juego sus equipos. ¿Está instalando estos parches? ¿Mantiene actualizados los sistemas operativos? ¿Siguiendo las mejores prácticas de seguridad? Es importante la forma en que configura sus dispositivos.

Los atacantes aprovechan las vulnerabilidades; la superficie de ataque aumenta.

2. Las apps móviles pueden ser una bendición o una pesadilla.

Las apps son una parte esencial del trabajo móvil. Es posible que su empresa realice la implementación de decenas —o incluso cientos— de apps en toda su flota. Cada app conlleva sus propios riesgos. El malware para dispositivos móviles es relativamente poco frecuente, pero la privacidad, las cadenas de suministro y el manejo de datos siguen siendo riesgos potenciales.

Sus apps también deben mantenerse actualizadas; sus desarrolladores igualmente corrigen vulnerabilidades. La administración del ciclo de vida de las apps es fundamental, al igual que garantiza un equilibrio entre la seguridad y la privacidad de sus empleados.

Las apps multiplican los riesgos potenciales; la superficie de ataque aumenta.

3. Las redes y los riesgos de Internet amenazan incluso a los dispositivos más seguros.

Proteger sus datos es fundamental, tanto si están almacenados como en tránsito. Para lograrlo, es necesario comprender su infraestructura de red y el comportamiento de los usuarios. Los empleados suelen conectarse a puntos de acceso sin protección que podrían estar expuestos a ataques por intermediarios (AitM). Si no se configura correctamente, sus datos quedan expuestos.

El phishing y otros riesgos en Internet siguen proliferando. Los atacantes se hacen pasar por sitios web populares de diversas categorías de contenido en línea: entretenimiento, negocios, servicios públicos y finanzas. Y los usuarios caen en la trampa todos los días, sobre todo ahora que la IA generativa ayuda a los atacantes a perfeccionar sus técnicas.

Los errores de los usuarios y las redes externas implican puntos de entrada sin control; la superficie de ataque aumenta.

4. Los riesgos se multiplican y dan lugar a amenazas sofisticadas.

Las vulnerabilidades de los dispositivos, las apps, la infraestructura de red y el comportamiento de los usuarios pueden crear brechas en su escudo cibernético. Cuanto mayor sea su superficie de ataque, más difícil será protegerla, y estos tres tipos de riesgos suelen ser objeto de ataques dirigidos.

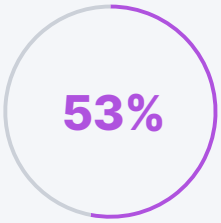
La proliferación de estos riesgos puede dar pie a ataques más dañinos, como las amenazas persistentes avanzadas (APT) y el spyware. En 2025, Jamf Threat Labs observó que seguían produciéndose ataques de cero clics y de un clic. Los principales objetivos fueron contra ejecutivos, políticos, activistas y periodistas.

Investigamos algunos de los ataques de cero clics y de un clic más perniciosos de 2025. Estos ataques tienen como objetivo sustraer información confidencial de inteligencia y aprovechar vulnerabilidades en múltiples componentes de un dispositivo. Más adelante en este informe, analizaremos nuestras conclusiones.

Vulnerabilidades de los dispositivos

Los sistemas operativos móviles brindan una base, que puede ser segura o no.

El código fuente del sistema operativo de su dispositivo es enorme y complejo. Y como los seres humanos somos falibles, es inevitable que se cuelen vulnerabilidades en el código. Los humanos también son astutos: los atacantes siempre están al acecho de posibles vulnerabilidades.



de las **organizaciones** al menos tiene un dispositivo con un sistema operativo muy desactualizado

¿Qué es un CVE?

El programa "Common Vulnerabilities and Exposures" (Vulnerabilidades y exposiciones comunes, CVE) funciona como una base de datos de vulnerabilidades descubiertas por la comunidad de ciberseguridad. Cada listado de CVE identifica el software o la biblioteca afectados, indica un nivel de gravedad y ofrece posibles métodos de explotación.

Veamos algunos ejemplos destacados de 2025, dos de los cuales se confirmó que fueron explotados en el mundo real. Estas vulnerabilidades y exposiciones comunes (CVE) se corrigieron en el iOS 18.4.1.

CVE-2025-31200

Puntuación de gravedad: 9.8 (crítica)

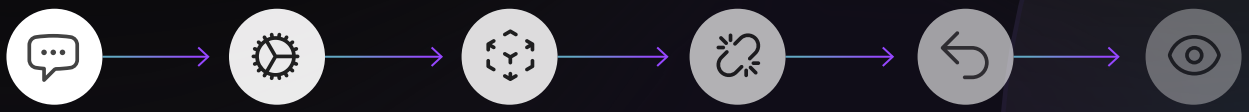
El procesamiento de un flujo de audio en un archivo multimedia creado con fines maliciosos podría dar lugar a la ejecución de código.

CVE-2025-31201

Puntuación de gravedad: 9.8 (crítica)

Un atacante con capacidad arbitraria de lectura y escritura podría eludir la autenticación de punteros.

Los atacantes pueden aprovechar vulnerabilidades como estas para robar sus datos e implementar programas espía. Imagine este escenario (muy simplificado):



Una persona de alto perfil recibe un mensaje cuidadosamente elaborado que contiene un archivo de audio malicioso.

Sin intervención humana, el dispositivo móvil procesa el mensaje de audio para su reproducción previa.

Una corrupción de la memoria durante el procesamiento permite realizar operaciones arbitrarias de lectura y escritura.

La evasión de la autenticación de punteros permite a los atacantes falsificar punteros de código válidos.

El atacante redirige la ejecución del código hacia una carga maliciosa.

El dispositivo ha sido comprometido y comienza la vigilancia.

¿Y qué significa esto?

- **Se trata de un ataque dirigido que no requiere ningún clic:** el usuario no tiene que hacer clic en nada para que su dispositivo quede comprometido. Probablemente los usuarios objetivo sean personas de alto perfil, como periodistas, políticos o ejecutivos.
- **Las vulnerabilidades se acumulan:** los atacantes buscan minuciosamente posibles vulnerabilidades y son muy hábiles para encontrarlas.
- **La importancia de las actualizaciones:** estas vulnerabilidades se corrigieron en iOS 18.4.1. Si sus dispositivos no están actualizados, sus datos no están protegidos.

Esperemos que esto ponga de relieve la importancia de contar con dispositivos actualizados. Eso no quiere decir que sea fácil de poner en práctica. Hay diversas razones por las que un usuario no desearía actualizar su dispositivo:

- Nuevas funciones o interfaz que no quieren usar
- Incompatibilidad de la app con la nueva versión del sistema operativo
- Interrupción del flujo de trabajo/limitaciones de recursos

Como hemos demostrado, es muy común el software desactualizado, y mantenerse al día es una tarea constante. Hacer cumplir los plazos de actualización y las versiones mínimas del sistema operativo protegerá su flota de dispositivos frente a vulnerabilidades graves, como las analizadas por Jamf Threat Labs en 2025.

Los atacantes aprovechan las vulnerabilidades para llevar a cabo vectores de ataque de cero clics, como el análisis de imágenes y archivos de audio, y ataques a navegadores con un solo clic.A pesar de los parches de seguridad y los esfuerzos de los proveedores, los atacantes aún pueden encontrar y aprovechar nuevas vulnerabilidades para desarrollar soluciones ofensivas, lo que propicia que las actualizaciones periódicas de los dispositivos móviles sean fundamentales para proteger a todos los usuarios frente a las vulnerabilidades. A continuación se presenta un resumen de las vulnerabilidades más impactantes de 2025.

Vulnerabilidades relevantes de iOS, 2025

CVE-2025-24201 | Gravedad: 10.0 (crítica)	CVE-2025-43300 | Gravedad: 10.0 (crítica)	CVE-2025-31201 | Gravedad: 9.8 (crítica)
DESCRIPCIÓN:		
Es posible que el contenido web creado con fines maliciosos logre escapar del entorno aislado de contenido web.	El procesamiento de un archivo de imagen malicioso puede provocar daños en la memoria.	Un atacante con capacidad de lectura y escritura arbitraria podría eludir la autenticación de punteros.
IMPACTO:		
Esta vulnerabilidad permite la escritura fuera de límites de datos más allá del final o antes del inicio del búfer previsto. Esto puede provocar una corrupción de la memoria o permitir que un atacante modifique datos para ejecutar código no previsto.	Esta vulnerabilidad también permite la escritura fuera de límites de datos más allá del final o antes del inicio del búfer previsto.	Esta vulnerabilidad se debe a controles de acceso inadecuados, lo que permite el acceso no autorizado a componentes críticos para la seguridad. Como resultado, los atacantes pueden modificar y leer la memoria, así como ejecutar código no autorizado.
SISTEMA OPERATIVO PARCHADO:		
iOS 18.3.2 y iPadOS 18.3.2	iOS 18.6.2 y iPadOS 18.6.2	iOS 18.4.1 y iPadOS 18.4.1

En la siguiente tabla se muestran otras vulnerabilidades que confirmamos que fueron explotadas en 2025.

iOS

VERSIÓN CORREGIDA DE IOS	FECHA	PUNTUACIÓN DE VULNERABILIDAD	COMPONENTE
18.3.1	Febrero de 2025	CVE-2025-24200 Puntuación CVSS: 6.1 | Gravedad: media	Accesibilidad
18.3.1	Febrero de 2025	CVE-2025-43200 Puntuación CVSS: 4.2 | Gravedad: media	Mensajes
18.4.1	Abril de 2025	CVE-2025-31200 Puntuación CVSS: 9.8 | Gravedad: crítica	CoreAudio
26.2	Diciembre de 2025	CVE-2025-43529 Puntuación CVSS: 8.8 | Gravedad: alta	WebKit
26.2	Diciembre de 2025	CVE-2025-14174 Puntuación CVSS: 8.8 | Gravedad: alta	WebKit

Vulnerabilidades relevantes de Android, 2025

CVE-2025-10585 | Gravedad: 9.8 (crítica)	CVE-2025-48543 | Gravedad: 8.8 (alta)	CVE-2024-53104 | Gravedad: 7.8 (alta)
DESCRIPCIÓN:		
Una confusión de tipos en V8 de Google Chrome permitía a un atacante remoto explotar potencialmente una corrupción de memoria dinámica mediante una página HTML diseñada de forma malintencionada.	En varios lugares, existe una posible forma de escapar del entorno aislado de Chrome para atacar el proceso `system_server` de Android debido a un fallo de "uso tras liberación". Esto podría fomentar una escalada de privilegios a nivel local sin que se requieran privilegios de ejecución adicionales. No se requiere la intervención del usuario para que se produzca la explotación.	media: uvcvideo: Omitir el análisis de tramas de tipo UVC_VS_UNDEFINED en uvc_parse_format. Esto puede provocar escrituras fuera de límites, ya que los fotogramas de este tipo no se tuvieron en cuenta al calcular el tamaño del búfer de fotogramas en uvc_parse_streaming.
IMPACTO:		
Se declara un puntero u otro recurso como un tipo determinado, pero después accede a un recurso de un tipo incompatible. Esto puede provocar reescrituras en la memoria, fallos del sistema y, posiblemente, la ejecución de código.	El uso de memoria que ya ha sido liberada puede dañar datos válidos. Si los atacantes introducen datos maliciosos antes de que se consolide la memoria, podrían llegar a ejecutar código arbitrario.	La escritura fuera de límites de datos más allá del final o antes del inicio del búfer previsto puede provocar una corrupción de la memoria o permitir que un atacante modifique los datos para ejecutar código inesperado.
SISTEMA OPERATIVO PARCHADO:		
Chrome 140.0.7339.155	Android 13, 14, 15, 16	Núcleo de Linux original, febrero de 2025

Android

VERSIÓN DE ANDROID PARCHADA	FECHA	PUNTUACIÓN DE VULNERABILIDAD	COMPONENTE
12, 12L, 13, 14, 15	Marzo de 2025	CVE-2024-43093 Puntuación CVSS: 7.3 | Gravedad: alta	Marco
Boletín de seguridad*	Marzo de 2025	CVE-2024-50302 Puntuación CVSS: 5.5 | Gravedad: media	Kernel
Boletín de seguridad	Septiembre de 2025	CVE-2025-38352 Puntuación CVSS: 7.4 | Gravedad: alta	Kernel

*Android no lanza versiones del sistema operativo para las actualizaciones del kernel. Consulte el boletín de seguridad de Android correspondiente para obtener más información.

Chrome

VERSIÓN PARCHADA DE CHROME	FECHA	PUNTUACIÓN DE VULNERABILIDAD
136.0.7103.125	Mayo de 2025	CVE-2025-4664 Puntuación CVSS: 4.3 | Gravedad: media
137.0.7151.72	Junio de 2025	CVE-2025-5419 Puntuación CVSS: 8.8 | Gravedad: alta
138.0.7204.63	Junio de 2025	CVE-2025-6554 Puntuación CVSS: 8.1 | Gravedad: alta
138.0.7204.157	Julio de 2025	CVE-2025-6558 Puntuación CVSS: 8.8 | Gravedad: alta
142.0.7444.175*	Diciembre de 2025	CVE-2025-13223 Puntuación CVSS: 8.8 | Gravedad: alta
143.0.7499.109	Diciembre de 2025	CVE-2025-14174 Puntuación CVSS: 8.8 | Gravedad: alta

*La versión indicada es para Chrome para computadoras de escritorio.

Es importante la forma en que configura sus dispositivos.

Los sistemas operativos móviles actuales ofrecen una amplia gama de potentes funciones, algunas de las cuales ni siquiera podíamos imaginar hace tan solo cinco años. Y ya sabe lo que se dice lo que conlleva tener un gran poder...

(Con suerte) usted inscribirá sus dispositivos en la administración de dispositivos móviles (MDM) para asegurarse de que estén correctamente configurados. Los dispositivos necesitan un equilibrio entre la facilidad de uso y la productividad, la seguridad y la privacidad del usuario, por lo que la configuración adecuada no siempre resulta evidente.

Aunque esto variará en función del perfil de riesgo y el sector de su organización, hay algunas funciones y configuraciones estándar que entrañan un gran riesgo y, por lo tanto, deben restringirse:

- Los dispositivos con jailbreak eluden las restricciones de seguridad de Apple y permiten al usuario modificar su dispositivo de formas inseguras o inestables. Cada dispositivo con jailbreak es una posible puerta trasera que permite a los atacantes acceder a su sistema.
- Las tiendas de apps alternativas permiten a los usuarios instalar aplicaciones fuera de la App Store o Google Play. Los marketplaces de apps alternativas no están sujetas a los mismos requisitos de seguridad y privacidad, lo que aumenta el riesgo de encontrar una app maliciosa o problemática.

SIN EMBARGO, A PESAR DE ESTOS RIESGOS, JAMF THREAT LABS DESCUBRIÓ QUE:

1 de cada 850
dispositivos utilizados para el trabajo tenía jailbreak

2%
de las organizaciones tenía dispositivos con apps de marketplaces alternativos.

Reflexiones de nuestro CISO

El enfoque integral que se describe a continuación mitiga las amenazas más comunes que afectan a los dispositivos móviles: spyware, aplicaciones comprometidas o maliciosas y aplicaciones sin parches, todas las cuales pueden exponer de forma silenciosa datos corporativos confidenciales sin que el usuario se percate de ello.

- **Asegúrese de que todos los dispositivos móviles estén inscritos en la MDM**, ejecuten versiones aprobadas del sistema operativo, cuenten con las actualizaciones correspondientes y cumplan con los requisitos mínimos de seguridad. Cualquier dispositivo que no esté en conformidad debe quedar aislado automáticamente de los recursos corporativos hasta que se encuentre la solución. Contar con un marco sólido para administrar los dispositivos y a los usuarios de dichos dispositivos es fundamental para detener posibles brotes de malware antes de que se produzcan.
- **Implemente una seguridad basada en agentes** que monitoree las fugas de privilegios, los comportamientos maliciosos y las amenazas a nivel del sistema operativo. Asegúrese de que los datos de telemetría se envíen a su SIEM para que su SOC tenga visibilidad de las amenazas móviles junto con el resto de su entorno.
- **Active el filtrado de DNS y la protección contra phishing** para todas las apps de todos los dispositivos, no solo para el correo electrónico. Esto debería incluir la detección de redes Wi-Fi no autorizadas y de ataques por intermediarios.

Riesgo en las aplicaciones

Las apps móviles son una parte fundamental del trabajo que realizan sus empleados. ¿Cuántas apps móviles implementa su organización? Estas apps, ya sean de terceros o desarrolladas internamente, actúan como puerta de entrada a sus datos confidenciales.

<1%

de las organizaciones se ven afectadas por el malware móvil.

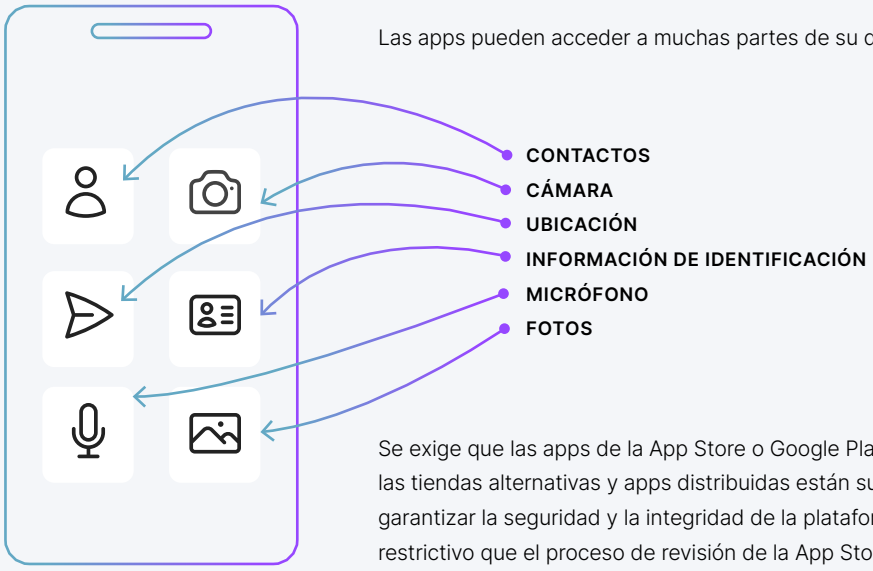
El malware para dispositivos móviles es poco común. Existe, pero no en la misma medida que en las computadoras. Esto se debe en gran medida a la arquitectura moderna que utilizan los principales sistemas operativos móviles, en los que el aislamiento de procesos y las tiendas de apps controladas reducen el riesgo de que el contenido malicioso llegue al dispositivo.

Aun así, las apps amplían su superficie de ataque. Considere:

- **Cómo administran las aplicaciones el almacenamiento y la transmisión de datos**
- **Qué datos recopilan las apps y cuáles son sus políticas de privacidad**
- **Importan las cadenas de suministro, como en qué bibliotecas se basa la app**

Los delincuentes aprovechan las vulnerabilidades de las apps para lanzar amenazas persistentes avanzadas y software espía, por lo que es fundamental conocer a fondo sus apps. Además, la forma en que las apps administran la transferencia de datos a través de las redes puede representar un riesgo; hablaremos de ello más adelante.

Las políticas de privacidad de las apps regulan el tratamiento de los datos.



Las apps pueden acceder a muchas partes de su dispositivo, algunas más sensibles que otras:

Se exige que las apps de la App Store o Google Play informen sobre los datos que recopilan. Todas las tiendas alternativas y apps distribuidas están sujetas al proceso de certificación de Apple para garantizar la seguridad y la integridad de la plataforma, aunque el proceso de aprobación es menos restrictivo que el proceso de revisión de la App Store oficial.

Es difícil encontrar un equilibrio entre la seguridad y la privacidad.

Tanto si usted proporciona dispositivos móviles a sus empleados como si les permite traer sus propios dispositivos, al permitirles el acceso a los recursos y datos de su empresa, debe dar prioridad a la seguridad y la privacidad. Seguridad, porque necesita proteger sus datos. Y la privacidad, porque hay que proteger al usuario.

Encontrar ese equilibrio puede ser todo un reto. Por ejemplo:

- Es **posible que su** sistema de prevención de pérdida de datos incurra en prácticas que violen la privacidad.
- **Bloquear un dispositivo** por motivos de seguridad puede afectar la productividad.
- Las **políticas inadecuadas** pueden dar lugar a la "TI en la sombra", en la que los usuarios descargan aplicaciones no autorizadas para realizar determinadas tareas laborales.

Para hacer frente a estos problemas, su organización puede:

- Exigir la inscripción en la **MDM** para acceder a los recursos corporativos
- Separar los datos personales de los de la empresa mediante contenedores o particiones reforzadas en los dispositivos BYOD para aplicar las políticas de prevención de pérdida de datos, protegiendo así la privacidad de los usuarios al impedir el acceso a los datos personales
- Enviar el tráfico de red de la empresa a través de túneles cifrados para garantizar la confidencialidad y la integridad de los datos
- Informar a los usuarios sobre las mejores prácticas y políticas de seguridad

Suplemento: análisis de la seguridad de las apps

Jamf se asoció con NowSecure para llevar a cabo un análisis exhaustivo de los riesgos de las apps móviles, especialmente en el contexto de las apps más utilizadas en implementaciones empresariales. Analizamos 135 de las aplicaciones móviles empresariales y personales más populares y con mayor difusión, utilizando el estándar OWASP como referencia para evaluar los riesgos de las apps móviles.

Todas las apps analizadas se encontraban en su versión más reciente al 31 de diciembre de 2025, lo que refleja la exposición real de las empresas a las versiones actuales de las apps.

NowSecure ayuda a las organizaciones a evitar que las vulnerabilidades de las apps móviles y las fugas de datos se conviertan en incidentes de seguridad, privacidad o conformidad. Al analizar continuamente tanto las aplicaciones móviles propias como las de terceros e integrar los resultados en los flujos de trabajo de seguridad, TI y administración de riesgos, NowSecure proporciona a los equipos la visibilidad, las pruebas y el control necesarios para controlar los riesgos móviles a gran escala.

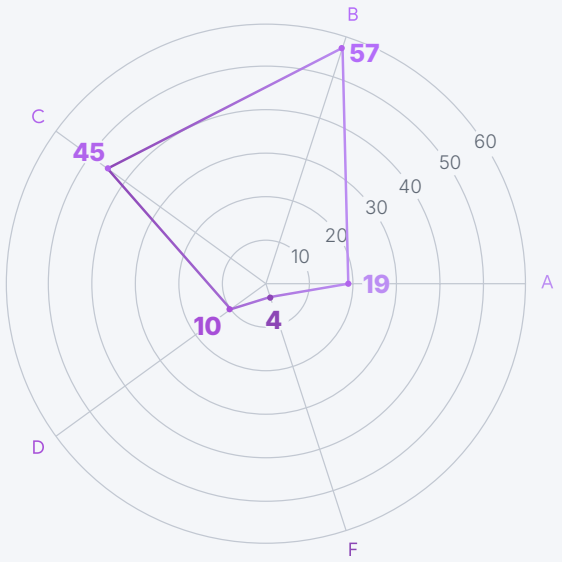
Más información sobre NowSecure.

Puntuación de seguridad de las apps

NowSecure es un proveedor que ofrece una puntuación de seguridad para apps móviles del 0 al 100 (cuanto más alta, mejor) y una calificación de riesgo de la **A** a la **F** (**A** = riesgo mínimo, **F** = riesgo considerable). Estas puntuaciones se basan en pruebas automatizadas que evalúan vulnerabilidades, fugas de datos, prácticas de programación inseguras, debilidades criptográficas y fallos de red.

Alrededor del **86%** de las 135 aplicaciones analizadas presentan fallos de seguridad conocidos, mientras que solo el **14%** se considera que entraña un riesgo mínimo. Esto significa que el riesgo está presente en las apps empresariales y personales más comunes que se utilizan a diario, incluso en las versiones más recientes.

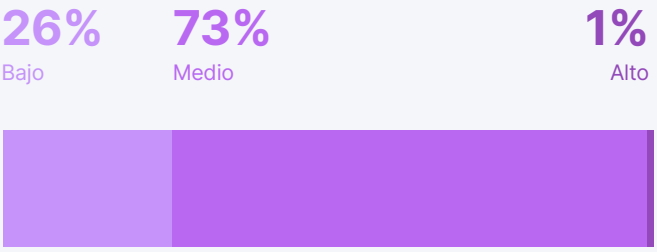
PUNTUACIONES DE SEGURIDAD DE LAS APPS MÁS POPULARES



A — F

Riesgo mínimo — Riesgo considerable

DISTRIBUCIÓN DE VULNERABILIDADES



De todas las vulnerabilidades detectadas en el análisis, la mayoría se clasificaron en la categoría de gravedad media. Como veremos más adelante, el número de vulnerabilidades supera el número de apps analizadas, lo que implica que se detectó que varias aplicaciones presentaban más de una vulnerabilidad.

Evaluación de la vulnerabilidad de las apps

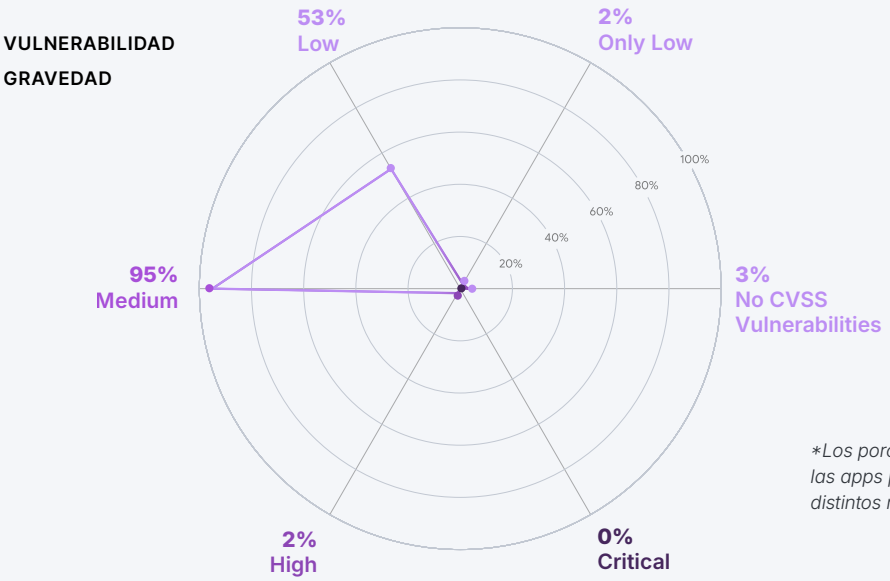
Es importante evaluar las implicaciones de riesgo que tienen las múltiples vulnerabilidades en una sola app. En el momento de la evaluación, el **95%** de las apps contenía al menos una vulnerabilidad de gravedad media, y el **2%** de las 135 aplicaciones presentaba vulnerabilidades de gravedad alta, lo que las hacía muy vulnerables a los ataques.

Si bien los fabricantes de software deben proporcionar la solución para las vulnerabilidades de sus aplicaciones, las empresas son responsables de evaluar su exposición al riesgo y de garantizar que se realicen a tiempo las actualizaciones. Existen diferentes recomendaciones en cuanto a los plazos de aplicación de parches (p. ej., la CISA recomienda proporcionar la solución para las vulnerabilidades de gravedad crítica en un plazo no mayor a 15 días naturales desde su detección inicial y para las de gravedad alta en un plazo no mayor a 30 días naturales desde su detección inicial), pero estos datos muestran que todas las organizaciones deberían contar con programas para mantener las apps actualizadas.

Como mencionamos anteriormente, NowSecure evaluó las apps en sus versiones actuales. Aun así, la mayoría presentaba múltiples vulnerabilidades. La administración de los riesgos de las apps es una tarea continua y en constante evolución que requiere monitoreo y control constantes.

Pero es manejable si usted:

1. Identifica vulnerabilidades continuamente así como problemas de privacidad
2. Prioriza la remediación en función del impacto en la empresa
3. Obliga la aplicación de políticas mediante controles de administración de dispositivos móviles
4. Monitorea el comportamiento de las apps de terceros a lo largo del tiempo

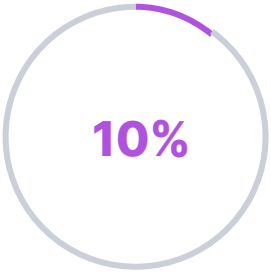


**Los porcentajes pueden superar el 100% porque las apps pueden contener vulnerabilidades de distintos niveles de gravedad.*

Cadena de suministro

Las apps móviles suelen depender de SDK y bibliotecas de terceros que entrañan riesgos ocultos.

Es posible que su app cuente con políticas de recopilación de datos y de privacidad adecuadas, pero que utilice kits de desarrollo de software (SDK) o bibliotecas de terceros que presenten fallos graves. Dado que las empresas siguen siendo responsables de la exposición de datos y del incumplimiento de la conformidad, deben tener una visión clara de los riesgos de la cadena de suministro de software.



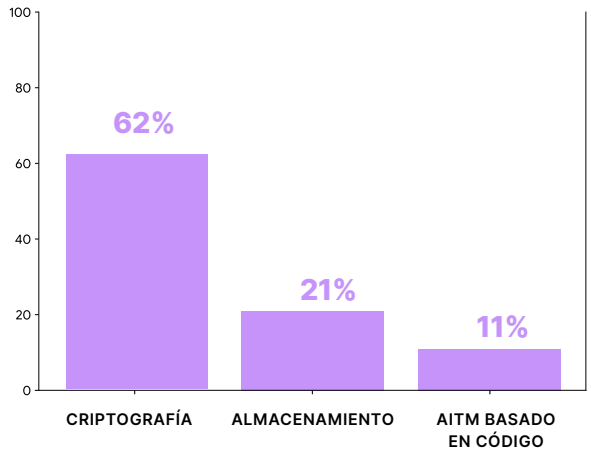
de las **apps** utilizaban
bibliotecas vulnerables

Seguridad de los datos

Los datos pueden filtrarse desde las apps de varias maneras.

- **Problemas relacionados con el cifrado:** Para los desarrolladores de aplicaciones, resulta complicado proteger los datos, asegurar las comunicaciones y verificar la identidad de los usuarios. Muchos dependen de bibliotecas de terceros. En todas las apps que analizaron, NowSecure identificó el uso de dos bibliotecas vulnerables ya conocidas: OpenSSL y libpng.
- **Almacenamiento inseguro:** La forma en que se administran los datos en reposo puede garantizar o comprometer la confidencialidad, integridad y disponibilidad de sus datos. Las medidas de protección de almacenamiento deficientes aumentan el riesgo de fuga de datos.
- **Riesgos de AitM:** También es importante cómo controlan las aplicaciones los datos en tránsito. Si las comunicaciones no están debidamente cifradas, por ejemplo, un atacante puede interceptar o manipular la información confidencial mientras se transmite.
- **Acceso a los datos:** Las aplicaciones móviles tienen acceso a los datos en la nube y a los datos corporativos que buscan los atacantes. La pérdida de datos es pérdida de datos, sin importar cómo se haya accedido a ellos.

TIPOS DE VULNERABILIDADES



Uso de la IA

La IA, especialmente la IA generativa, sigue siendo un tema candente en estos días. En un informe de enero de 2026, Deloitte señala que el acceso de los trabajadores a la IA autorizada aumentó un 50% en un año, y que el 60% de los empleados utiliza herramientas de IA en el trabajo.

Tiene sentido, ya que tanto la IA integrada en los dispositivos como la basada en la nube ofrecen una gran variedad de funciones muy prácticas. Por ejemplo, las apps móviles incorporan cada vez más ambas:

- **IA integrada en el dispositivo:** los modelos de lenguaje de gran escala (LLM) permiten a las aplicaciones realizar tareas de procesamiento del lenguaje natural, como la generación de texto y la escritura predictiva, mientras que los modelos de aprendizaje automático se utilizan para funciones como el reconocimiento de imágenes, la detección de objetos en tiempo real, los escáneres de códigos de barras y la realidad aumentada.
- **IA basada en la nube:** realiza diversas tareas avanzadas, recurriendo a una infraestructura externa para el procesamiento y el cálculo.

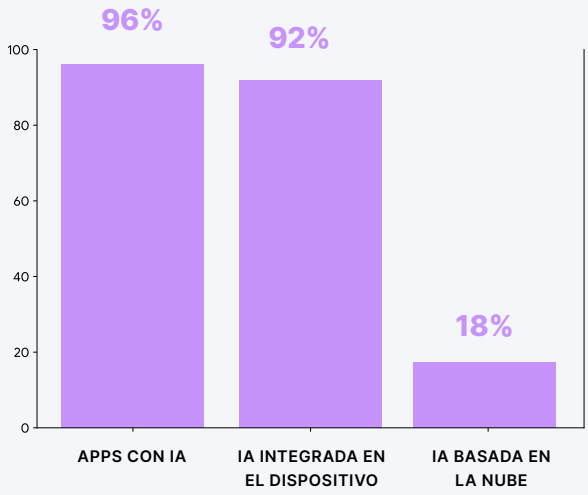
Los usuarios y las organizaciones no tardan en adoptar la IA generativa, pero a medida que la tecnología evoluciona, también lo hacen los riesgos.

Considere los riesgos:

- Los usuarios pueden recurrir a la "IA en la sombra", es decir, un acceso a la IA no autorizado y sin control que puede incluir **datos confidenciales de la empresa** e infringir las políticas. La dependencia de la IA basada en la nube de una infraestructura externa implica que es posible que su organización no tenga una visión clara de los **riesgos potenciales**, incluida la **exposición de datos**.
- Los usuarios pueden utilizar agentes de IA para **realizar acciones autónomas**, más allá de los controles previstos.

Resulta que muchas aplicaciones comunes utilizan la inteligencia artificial, a menudo sin que la empresa tenga un control claro sobre ello.

PRESENCIA DE FUNCIONES DE IA EN LAS APPS



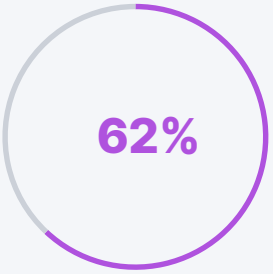
Privacidad

Llevamos nuestros dispositivos móviles a todas partes. Contienen una gran cantidad de información sobre nuestra vida personal y laboral, ya sean fotos, contactos, datos confidenciales, documentos financieros, información privada, etc.

Por este motivo, tanto los usuarios como los empleadores dan prioridad a la privacidad; además, es posible que usted esté sujeto a leyes de protección de datos.

Sin embargo, esto no siempre se refleja en nuestras aplicaciones, ya sea por decisión de los desarrolladores o por descuido. Las apps pueden solicitar permisos peligrosos que recopilan datos confidenciales, como el acceso a:

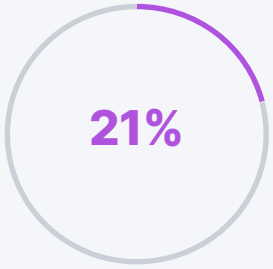
- Ubicación del dispositivo
- Micrófono
- Cámara
- Contactos



de las **apps** solicitaban **permisos peligrosos**

Más allá de solicitar información, ¿cómo la administran las apps? Algunos datos se recopilan porque la app los necesita para funcionar. Otros datos, no tanto. Ciertas funciones de las apps socavan la privacidad con problemas que la afectan, como:

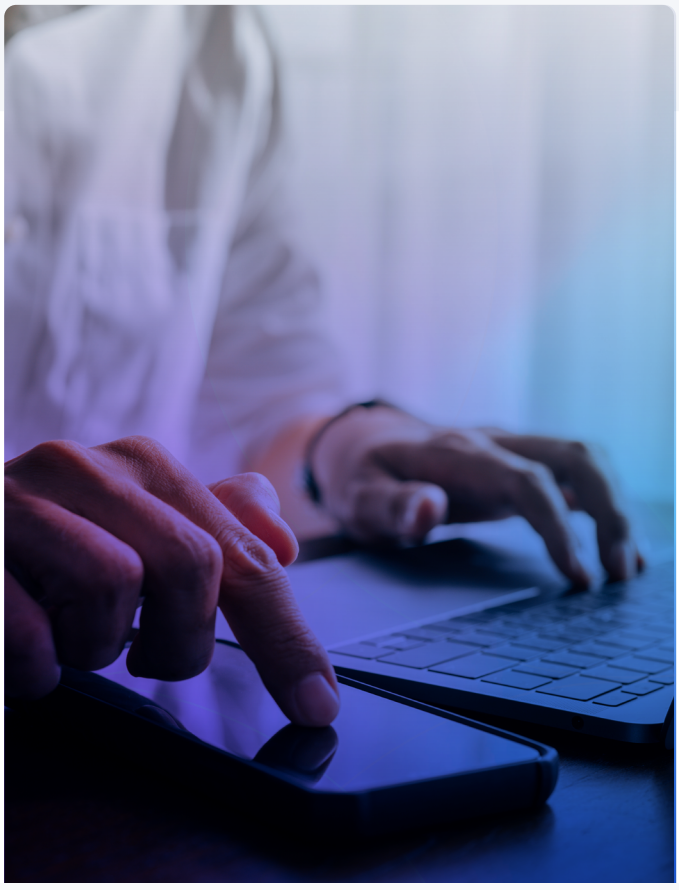
- Rastreo y elaboración de perfiles
- Compartir datos con terceros
- Recopilación de datos de contacto/publicidad dirigida



de las **apps** presentaban **comportamientos que afectaban a la privacidad**

Reflexiones de nuestro CISO

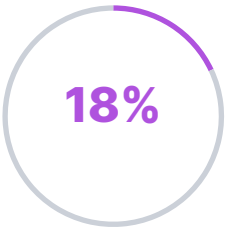
Las apps móviles son la puerta de entrada a los datos confidenciales de la empresa. Para manejar este riesgo, las organizaciones deben controlar qué apps se permiten en los dispositivos, proteger los datos mientras se transmiten por las redes y mantener una visión clara de las vulnerabilidades de las aplicaciones en toda la flota de dispositivos. Con el BYOD, el objetivo es la separación. Manteniendo los datos corporativos en contenedores y protegidos sin invadir la privacidad personal. El resultado es un enfoque equilibrado en el que los equipos de seguridad disponen de los controles que necesitan y los empleados tienen la seguridad de que sus datos personales se mantienen privados.



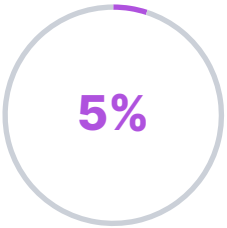
Riesgos de la red y de la web

Al igual que la muerte y los impuestos, una cosa es segura: los atacantes seguirán aprovechando el eslabón más débil de nuestra seguridad: las personas. Los atacantes son cada vez más eficaces y utilizan la IA generativa para diseñar ataques cada vez más convincentes. Los usuarios hacen clic en enlaces de phishing, se conectan a redes Wi-Fi y puntos de acceso de riesgo, y descuidan sus prácticas de seguridad cibernética.

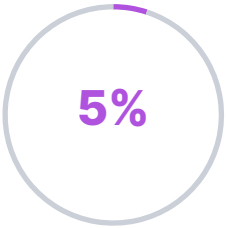
No todas las vulnerabilidades residen en un dispositivo; incluso los dispositivos perfectamente protegidos y con configuraciones ideales siguen siendo vulnerables a las amenazas que interceptan los datos en tránsito. Las redes son un medio muy utilizado para llevar a cabo ataques. Esto puede manifestarse de diversas formas:



de las **organizaciones** tiene usuarios que se conectan a **puntos de acceso riesgosos**



de las **organizaciones** tienen usuarios que han sido víctimas de **ataques AitM basados en la infraestructura**



de las **organizaciones** tienen dispositivos **afectados por criptojacking**

Infraestructura de red

Usted puede controlar las configuraciones de su propia red, pero no las de todas las redes de terceros —incluidas las redes celulares— a las que se conectan sus usuarios cuando están fuera del campus. Con suerte, estará aplicando el acceso condicional, segmentando su red y aplicando políticas de acceso a la red de confianza cero.

De lo contrario, sus datos corren peligro. Si un usuario se conecta a una red Wi-Fi pública no segura —que puede tener un cifrado débil o carecer de autenticación—, los atacantes pueden aprovecharse de ello para robar cookies de sesión, eludir la validación de certificados o emplear otras técnicas.

Los protocolos web regulan la forma en que los dispositivos, los navegadores y los servidores intercambian información. Son un componente fundamental de la seguridad de los datos. Los atacantes pueden forzar el uso de versiones anteriores y menos seguras de estos protocolos, lo que facilita el descifrado y el robo de los datos en tránsito. Esto expone a su organización a ataques por intermediarios.

Estos ataques AitM aprovechan vulnerabilidades en la infraestructura de red, a diferencia de las vulnerabilidades basadas en el código de un sistema operativo o una app.

Riesgos en la web

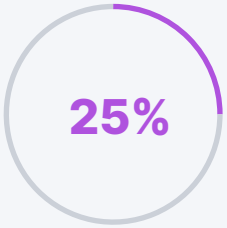
Incluso en una conexión segura, no se puede garantizar que navegar por Internet sea seguro. No es necesario que los dispositivos se vean comprometidos para que surjan problemas. Hacer clic en enlaces o anuncios maliciosos, o visitar sitios web problemáticos, puede dar lugar a criptojacking y al robo de credenciales mediante phishing. El criptojacking —en el que los atacantes utilizan los recursos de procesamiento y memoria de un dispositivo para minar criptomonedas— puede ralentizar un dispositivo hasta dejarlo inservible.

¡Ah! El phishing, nuestro eterno enemigo. La IA generativa hace que sea más fácil que nunca crear un mensaje de phishing convincente. Los usuarios ya no pueden dar por sentado que los mensajes maliciosos estarán plagados de errores ortográficos y otros indicios reveladores típicos.

Las 30 marcas más utilizadas en campañas de phishing

A los delincuentes les gusta imitar a las marcas populares. Los usuarios son más propensos a hacer clic en un enlace de un servicio que utilizan y con el que están familiarizados; los atacantes se aprovechan de la confianza que los usuarios depositan en las instituciones que utilizan a diario. Los atacantes tienen un interés especial en atacar a los bancos y los servicios financieros, ya que es probable que las cuentas comprometidas contengan tanto dinero como información confidencial.

Tenga en cuenta que estas marcas no han hecho nada malicioso; los atacantes se aprovechan de su reputación de confianza para atraer a usuarios desprevenidos hacia un ataque de phishing.



de las **organizaciones** cayó víctima de un enlace de phishing.

Entretenimiento/ Networking	Comercios	Servicios	Servicios bancarios y financieros
Netflix Facebook Steam eBay, Inc. WhatsApp	Microsoft Apple Adobe	Optus AT&T Amazon DHL British Telecom Orange Comcast East Japan Railway Company	Allegro Servicio de Impuestos Internos de EE. UU. Rakuten Coinbase PayPal AEON Card Sumitomo Mitsui Banking Corporation Navy Federal Credit Union Bradesco Bank of America Corporation Grupo HSBC Raiffeisen Bank American Express ING Direct

Reflexiones de nuestro CISO

Además de los controles técnicos, es fundamental preparar de manera proactiva a los empleados para que reconozcan y denuncien los intentos de phishing y otras amenazas de ingeniería social mediante programas de sensibilización, capacitación y pruebas de phishing. Las pruebas de phishing deberían aprovechar la inteligencia artificial para ofrecer pruebas adaptadas a las habilidades de los usuarios y mantenerlas actualizadas en función de las nuevas y diversas amenazas.

La proliferación de riesgos: amenazas persistentes avanzadas

Hasta ahora, hemos hablado de los riesgos relacionados con:

- Sistema operativo y configuración del dispositivo
- Apps móviles
- Networking y navegación por Internet

Cualquier riesgo, ya sea una vulnerabilidad del sistema operativo, una app móvil con un manejo de datos deficiente o un usuario que se conecte a una red Wi-Fi pública, puede tener un impacto significativo en la seguridad de sus datos. O tal vez no, dependiendo de sus políticas de configuración y de la capacitación de los usuarios.

Pero cuando estos riesgos se acumulan, se convierten en un problema. Los grupos de amenazas avanzadas combinan vulnerabilidades para crear exploits sofisticados. Aunque los autores de estos ataques avanzados han mostrado históricamente moderación al centrarse en objetivos de gran valor, sus herramientas están empezando a difundirse más ampliamente, lo que podría poner en peligro a los ciudadanos promedio.

Comprender estas amenazas avanzadas es esencial para defenderse de ellas. Jamf Threat Labs evaluó los diversos mecanismos de ejecución de exploits (incluidos los ataques de cero clics y de un clic) así como los modelos de implementación operativa utilizados en operaciones de vigilancia selectiva, con el fin de obtener datos de inteligencia sobre usuarios de alto riesgo, como periodistas, ejecutivos de empresas, políticos, activistas y otros. El análisis incluye temas como las vulnerabilidades de los sistemas operativos y las apps de terceros, la respuesta de los proveedores y mucho más. Esto es lo que encontraron.

Los ataques de cero clics siguen siendo altamente relevantes

Los ataques cero clics contra dispositivos Apple y Android siguen siendo un vector de amenaza activo en 2025, especialmente para periodistas y altos ejecutivos. Esta evidencia se ve reforzada por el descubrimiento de un ataque contra usuarios de WhatsApp a través de una vulnerabilidad en el análisis de imágenes (CVE-2025-43300).

Este hallazgo demuestra que los atacantes continúan ejecutando códigos sin ninguna interacción por parte del usuario, eludiendo las defensas tradicionales basadas en la detección. Estos ataques suelen estar relacionados con operaciones de vigilancia selectiva o de recopilación de inteligencia.

La continua aparición de vulnerabilidades de cero clics en el mundo real confirma que los atacantes motivados siguen teniendo tanto la capacidad como la intención de invertir en el costoso desarrollo de exploits.

Cómo proteger su organización:
Implemente sistemas de detección posterior a la explotación, telemetría de comportamiento y monitoreo basado en anomalías, en lugar de depender únicamente de controles de interacción del usuario.

Siguen produciéndose los ataques a los navegadores, incluyendo la distribución encubierta a través de anuncios.

Apple y Google publicaron numerosos parches de seguridad para los navegadores a lo largo del año. Chrome recibió 250 parches de seguridad; Safari recibió más de 75, lo que indica que se siguen detectando problemas de seguridad relacionados con la memoria que pueden activarse a través de contenido web malicioso.

Estas vulnerabilidades resultan especialmente atractivas porque pueden explotarse mediante JavaScript en sitios web o anuncios maliciosos, lo que reduce los costos operativos para los atacantes. Los informes de inteligencia sobre amenazas confirman que los proveedores de spyware comercial siguen recurriendo a cadenas de explotación de un solo clic, combinando vulnerabilidades ya explotadas con fugas del entorno de pruebas para lograr el control total del dispositivo.

El descubrimiento de las operaciones de Intellexa pone de manifiesto que las organizaciones de inteligencia utilizan activamente este tipo de vulnerabilidades y que también pueden propagarse como ataques de cero clics a través de redes publicitarias.

CÓMO PROTEGER SU ORGANIZACIÓN:
Amplíe su infraestructura de seguridad con inspección del tráfico web, detección de comportamientos de explotación y aplicación de actualizaciones rápidas del sistema operativo y del navegador en entornos móviles administrados.

Las empresas afectadas se defienden activamente, pero la cobertura defensiva sigue siendo insuficiente.

En 2025, los proveedores de plataformas y las grandes empresas tecnológicas intensificaron de manera evidente sus esfuerzos para contrarrestar las operaciones de espionaje selectivo, incluyendo medidas legales, técnicas y arquitectónicas. Las acciones legales de alto perfil, como el litigio de Meta contra NSO Group, ilustran una escalada que va más allá de las defensas puramente técnicas hacia una disuasión legal sostenida.

Al mismo tiempo, Apple sigue invirtiendo en medidas de mitigación a nivel de plataforma, como la extensión de etiquetado de memoria (MTE) y la mejora del modo de bloqueo. Sin embargo, a pesar de estas medidas, siguen existiendo cadenas de explotación que persisten.

Los atacantes avanzados siguen adaptando sus herramientas y técnicas para actuar dentro o al margen de las nuevas medidas de mitigación. Por ejemplo, recientemente se presentó una posible solución alternativa en una conferencia privada.

CÓMO PROTEGER SU ORGANIZACIÓN:
Complemente las medidas de protección de los proveedores con capacidades independientes de detección, visibilidad forense y respuesta ante incidentes, adaptadas a escenarios de ataques dirigidos.

Programas espía a los que hay que estar atentos

Predator | Desarrollador: Intellexa

Predator se basa principalmente en exploits web que se ejecutan con un solo clic, los cuales suelen difundirse a través de enlaces maliciosos o contenido web, incluidos los anuncios. Aprovecha de manera intensiva las vulnerabilidades de WebKit, tal y como reflejan los repetidos parches de Apple. Este modelo es más escalable, pero más sensible a la latencia de los parches. Predator demuestra que los ataques con un solo clic siguen siendo viables desde el punto de vista operativo.

Graphite | Desarrollador: Paragon

Graphite es una plataforma de software espía comercial vinculada a la explotación avanzada de iOS, y se estima que admite la infeccón tanto de tipo cero clics como de un solo clic. En 2025, una exitosa explotación de iMessage de cero clics contra iPhones con todas las actualizaciones instaladas demostró la capacidad de Graphite para comprometer dispositivos sin necesidad de interacción por parte del usuario. Se atribuyeron múltiples infecciones a la misma infraestructura del operador, lo que confirma que se trataba de un ataque coordinado y deliberado, y no de una actividad oportunista. Estos hallazgos consolidan a Graphite como un actor relevante en el mercado del spyware, a pesar de la creciente presión normativa y legal a la que se ven sometidos los proveedores.

Landfall | Desarrollador: N/A

Landfall es una familia de spyware para Android de nivel comercial hasta ahora desconocida, utilizada en una campaña de espionaje móvil dirigida contra dispositivos Samsung Galaxy. Los atacantes aprovecharon una vulnerabilidad crítica de día cero en la biblioteca de procesamiento de imágenes de Samsung para distribuir el software espía a través de archivos de imagen manipulados de forma maliciosa, aparentemente difundidos mediante aplicaciones de mensajería como WhatsApp.

La campaña, que estuvo activa al menos desde mediados de 2024 hasta que Samsung corrigió la vulnerabilidad en abril de 2025, proporcionó a los atacantes amplias capacidades de vigilancia, entre las que se incluían la grabación de audio, el rastreo de la ubicación y la recopilación de contactos, fotos y registros de llamadas. Desde una perspectiva de seguridad, Landfall demuestra que las operaciones de spyware para Android que aprovechan vulnerabilidades de día cero siguen evolucionando fuera del alcance de la opinión pública, lo que pone de relieve la necesidad de una administración proactiva de los parches, la detección de anomalías y la telemetría a largo plazo de los dispositivos en todas las plataformas móviles.

Pegasus | Desarrollador: NSO Group

Pegasus es una plataforma de software espía de alta gama para iOS y Android asociada a cadenas de exploits de cero clics y de un solo clic, lo que permite el control total del dispositivo. Se dirige a un pequeño número de personas de alto perfil y está optimizado para actuar de forma sigilosa y persistente. En 2025, la actividad de NSO se vio afectada por restricciones a la exportación y responsabilidades legales. Desde entonces, la empresa fue adquirida por un grupo de inversionistas, pero se prevé que las agencias de inteligencia sigan utilizando la tecnología, tal vez bajo una marca diferente.

Dante | Desarrollador: Memento Labs

Memento Labs es un proveedor italiano de tecnología de vigilancia y sucesor de la controvertida empresa Hacking Team, que cambió de nombre tras su adquisición en 2019. En 2025, se utilizaron herramientas vinculadas a Memento Labs en una campaña avanzada de ciberespionaje conocida como "Operación ForumTroll", con una vulnerabilidad de día cero que permitía escapar del entorno aislado de Chrome (CVE-2025-2783).Según su director ejecutivo, dejaron de ofrecer soporte para soluciones de Windows y dirigieron sus esfuerzos hacia las plataformas móviles, por lo que se espera que esta familia de malware y estas vulnerabilidades se encuentren en dispositivos Android.

Spyrtacus | Desarrollador: SIO

Spyrtacus es una familia de programas espía de vigilancia comercial que, según se informa, se dirigió activamente a dispositivos Android en 2025. Se distribuyó a través de enlaces maliciosos y técnicas de ingeniería social en la capa de aplicación. Una vez instalado en un dispositivo, Spyrtacus muestra las capacidades típicas del spyware, como la sustracción de datos, el rastreo de la ubicación y la recopilación de mensajes y contactos.

A diferencia del spyware de cero clics, como Pegasus o Graphite, Spyrtacus suele requerir cierto grado de interacción por parte del usuario o técnicas de ingeniería social para iniciar la instalación. La presencia de Spyrtacus en campañas reales pone de manifiesto que no todo el software espía móvil dirigido se basa en la explotación de vulnerabilidades de día cero; por el contrario, los atacantes pueden combinar la ingeniería social con marcos de software espía de uso común para lograr objetivos similares.

Reflexiones de nuestro CISO

A pesar de las importantes medidas de mitigación a nivel de plataforma y del refuerzo de la seguridad por parte de los proveedores, en 2025 los atacantes siguieron descubriendo y aprovechando vulnerabilidades críticas, en particular en componentes de gran valor, como los navegadores (Chrome, Safari) y las aplicaciones de mensajería. Estos componentes siguen siendo objetivos atractivos debido a su complejidad, a su frecuente exposición a contenido no confiable y a su papel central en los flujos de trabajo diarios de los usuarios.

La persistencia de los ataques dirigidos exitosos manifiesta que ninguna estrategia de mitigación elimina por completo el riesgo, en especial frente a adversarios que cuentan con amplios recursos. Por lo tanto, una administración rigurosa de los dispositivos y una aplicación estricta de las actualizaciones siguen siendo algunas de las medidas defensivas más eficaces y controlables de las que disponen las organizaciones.

Esto confirma que la administración de dispositivos móviles no es una función secundaria, sino un control de seguridad fundamental. Para limitar el impacto de las vulnerabilidades recién descubiertas son factores decisivos garantizar actualizaciones de seguridad rápidas, aplicar los estándares de seguridad, mantener la visibilidad de los dispositivos y reducir los periodos de exposición.

Los riesgos son grandes, pero no insuperables.

Se requiere una arquitectura bien pensada para enfrentar estos riesgos. Los pilares de los dispositivos seguros son:

Administración de dispositivos para aplicar restricciones, configuraciones y hacer cumplir las políticas

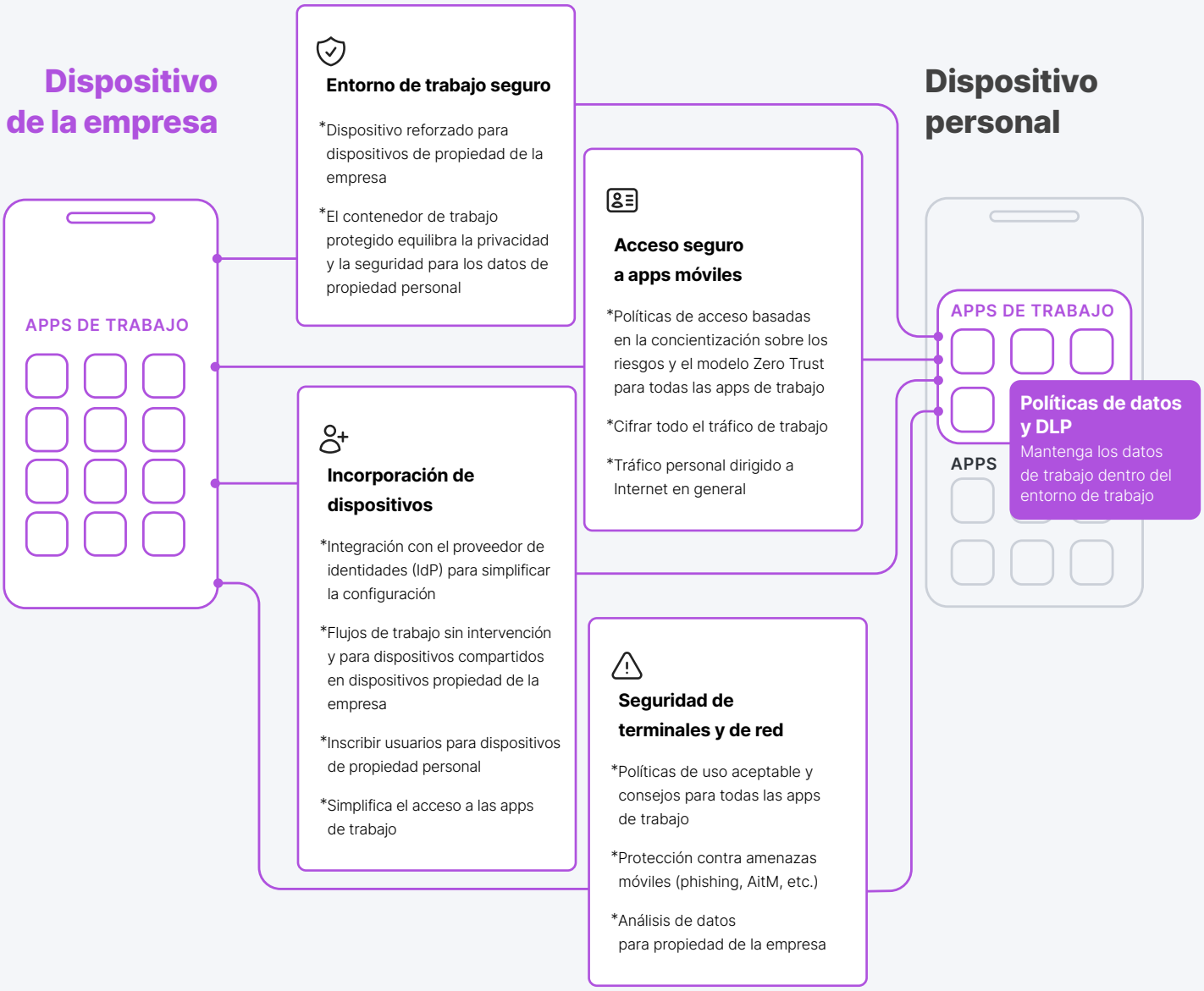
Seguridad de terminales para monitorear el estado y el comportamiento de los dispositivos, en caso de una posible vulneración

Acceso remoto seguro para controlar quién y qué dispositivos pueden acceder a los recursos de la empresa

Todas estas medidas se combinan para garantizar que solo los dispositivos que cumplan con los requisitos y los usuarios autorizados puedan acceder a sus datos confidenciales.

Esto podría variar ligeramente, dependiendo si un **dispositivo es propiedad de la empresa**.

La configuración de sus dispositivos puede representar un riesgo... o un activo para su seguridad. La automatización de las actualizaciones, la verificación de apps y el análisis de comportamiento, junto con la aplicación de políticas de acceso basadas en la conformidad, le acercan mucho más a la protección de sus datos.



Lea el último estudio sobre dispositivos móviles de Jamf Threat Labs

Cómo el spyware Predator burla los indicadores de grabación de iOS

FEBRERO DE 2026

Mediante una sofisticada técnica que aprovecha la mensajería "nil" de Objective-C, el spyware Predator elude los indicadores de grabación de iOS. El malware se engancha a un solo método de SpringBoard que administra todas las actualizaciones de actividad de los sensores; después, establece el puntero self en NULL, lo que provoca que las actualizaciones de los indicadores se ignoren silenciosamente en lugar de mostrarse a los usuarios. Este método es más sutil que las técnicas anteriores, ya que el dispositivo funciona con normalidad sin ofrecer ninguna señal visual de que se está llevando a cabo una vigilancia, lo que permite el acceso encubierto a la cámara y al micrófono en dispositivos totalmente comprometidos.

OpenClaw: la útil IA que podría convertirse silenciosamente en tu mayor amenaza interna

FEBRERO DE 2026

OpenClaw es un marco de código abierto para crear agentes de IA autónomos que puedan ejecutar comandos de shell, acceder a archivos e interactuar con aplicaciones sin límites de seguridad integrados, lo que genera riesgos significativos para la seguridad empresarial. El marco se vuelve peligroso debido al acceso sin restricciones al sistema, al riesgo de fuga de datos y a su vulnerabilidad ante ataques indirectos de inyección de comandos, en los que se incrustan instrucciones maliciosas en contenido empresarial legítimo. Los avisos de seguridad recientes han puesto de manifiesto cómo los atacantes pueden aprovechar diversas vulnerabilidades para obtener acceso persistente, lo que convierte a las implementaciones de OpenClaw en una amenaza interna de alto riesgo que requiere estrategias integrales de detección, prevención y gobernanza para gestionarlas de forma segura en entornos empresariales.

El kill switch de Predator: técnicas de antianálisis no documentadas en el software espía para iOS

ENERO DE 2026

El spyware Predator cuenta con sofisticadas capacidades antianálisis que van mucho más allá de lo documentado hasta ahora, incluyendo un sistema de códigos de error que proporciona información diagnóstica precisa a los operadores sobre las causas de los fallos en las implementaciones. El malware detecta el modo de desarrolladores, las herramientas de jailbreak, las aplicaciones de seguridad y las restricciones geográficas, e implementa técnicas avanzadas contra el análisis forense para ocultar los indicios de grabación a las víctimas.

Estos mecanismos revelan que los operadores reciben retroalimentación detallada cuando falla la segmentación, lo que les permite solucionar los problemas y adaptar su estrategia, lo que demuestra que los proveedores de spyware comercial dedican un esfuerzo considerable a detectar a los investigadores, y no solo a eludir los productos de seguridad.

Jamf Threat Labs descubre que una app móvil de juegos filtra las credenciales de los jugadores

NOVIEMBRE DE 2025

Se descubrió que "World of Warships Blitz", un popular juego para dispositivos móviles con más de 10 millones de descargas, filtraba credenciales de los jugadores y tokens de sesión a través de conexiones HTTP sin cifrar durante el proceso de inicio de sesión y registro. Aunque las credenciales estaban enmascaradas, la filtración permitió ataques de repetición en los que los atacantes podían capturar y reenviar solicitudes de autenticación para secuestrar cuentas. Tras una notificación responsable, los desarrolladores corrigieron el problema de forma cooperativa en la versión 8.4.0.

Esta investigación pone de relieve que incluso las apps más populares pueden contener vulnerabilidades críticas y que es fundamental contar con medidas de seguridad en varios niveles y educar a los usuarios sobre las buenas prácticas en materia de contraseñas.

Jamf Threat Labs descubre apps que filtran credenciales

SEPTIEMBRE DE 2025

Se descubrió que dos aplicaciones móviles filtraban credenciales de usuario e información de identificación personal (PII) a través de conexiones HTTP sin cifrar: una aplicación malaya de administración médica con 15 millones de usuarios y una aplicación de "ahorros" de una empresa india de joyería. Ambas aplicaciones transmiten datos confidenciales en texto sin cifrar, lo que expone a los usuarios al robo de credenciales, al fraude de identidad y al acceso no autorizado a sus cuentas, especialmente en redes públicas.

Este hallazgo pone de relieve la necesidad imperiosa de que las organizaciones implementen sistemas seguros de transmisión de datos y de que los usuarios utilicen soluciones de defensa contra amenazas móviles, ZTNA y filtrado de contenido para bloquear las aplicaciones peligrosas.

Flekst0re: evaluación de la seguridad de tiendas de aplicaciones de terceros

AGOSTO DE 2025

Las tiendas de aplicaciones de iOS de terceros, como Flekst0re, plantean graves riesgos de seguridad, tal y como lo demostró una versión modificada de WhatsApp (de prueba de concepto) que grababa conversaciones en secreto y las transmitía a un servidor remoto, todo ello sin que se notara que no era legítima. Estas plataformas eluden el proceso de revisión de seguridad de Apple al volver a firmar las apps con certificados empresariales, y la función de fuentes personalizadas de Flekst0re permite a los usuarios descargar aplicaciones no verificadas que podrían contener spyware o malware.

Aunque las tiendas de terceros ofrecen comodidad y acceso a apps modificadas, socavan de manera fundamental las medidas de seguridad de iOS, lo que las convierte en un peligro para cualquiera que utilice aplicaciones confidenciales, como las de banca, mensajería o correo electrónico.

jamf

Póngase en contacto con nosotros para obtener más información sobre el panorama de las amenazas móviles.