



Encriptado con clave desechable | Encriptado de extremo a extremo

26 de agosto de 2026. Es posible que actualicemos este documento de vez en cuando para reflejar las mejoras que realizamos para complacer a los clientes, como reforzar las protecciones, optimizar el rendimiento y aumentar la resiliencia.

Resumen

La misión de Ring es hacer los hogares más seguros. La privacidad, la seguridad y el control del cliente son fundamentales para esa misión. Hasta ahora, Ring protegía los vídeos de los clientes mediante el encriptado estándar del sector. De forma predeterminada, todo el contenido de vídeo de los clientes se cifra en tránsito y en reposo en la nube. Ring también ofrece encriptado de extremo a extremo como opción para los clientes que desean el máximo control, siendo el primer proveedor importante de cámaras de seguridad inteligente para el hogar en hacerlo. En este documento se describe una actualización significativa de las ofertas de encriptado de Ring.

Resumen

TAKE (El encriptado con clave desechable) se está implementando gradualmente como el nuevo encriptado predeterminado para todos los clientes de Ring. Te ofrece un control aún mayor sobre cómo y cuándo Ring procesa tus vídeos, al tiempo que mantiene las funcionalidades que ya utilizas. Con el encriptado con clave desechable, tus vídeos se cifran con claves que cambian con frecuencia; Ring solo puede abrir su copia de esas claves dentro de un enclave seguro. El acceso de Ring al enclave está restringido por controles de acceso, cifrado y aislamiento de hardware, de modo que Ring solo puede utilizar claves para activar las funcionalidades en tu cuenta. Ring eliminará de forma permanente la copia de tus claves transcurridas 24 horas. Si más adelante activas una funcionalidad que necesita procesar vídeos antiguos, la app de Ring puede proporcionar temporalmente las claves para activar esa funcionalidad y Ring las eliminará después otra vez.

El encriptado de extremo a extremo (E2EE) seguirá estando disponible como opción para los clientes. En este modo opcional, Ring no tiene acceso al contenido, ni siquiera temporalmente. Ring solo almacena vídeos encriptados y no puede descifrarlos; solo tú tienes las claves necesarias para descifrar el vídeo. Las funcionalidades que requieren que Ring procese vídeos, como la búsqueda de vídeos, la descripción de vídeo y los usuarios compartidos, no están disponibles en el encriptado de extremo a extremo. Las funcionalidades que no requieren que Ring procese los vídeos, como el vídeo en directo, la reproducción de eventos y la grabación ininterrumpida, seguirán funcionando.

Por qué es importante: Ring ha diseñado el encriptado con clave desechable para que sea nuestro encriptado ¹predeterminado más sólido hasta la fecha. Con el encriptado con clave desechable, la copia de Ring de tus claves se abre dentro de un enclave seguro; solo la libera para activar las funcionalidades activas en tu cuenta, y Ring elimina permanentemente esa copia después de 24 horas; solo tú conservas una copia duradera. Esta actualización refuerza un compromiso: la privacidad es un principio fundamental de cómo construimos y diseñamos en Ring. Esta arquitectura es una base en la que continuaremos invirtiendo y fortaleciendo.

Ambos modos (encriptado con clave desechable y encriptado de extremo a extremo) estarán disponibles para todos los clientes de cámaras de seguridad Ring compatibles, independientemente del estado de la suscripción. El encriptado con clave desechable se implementará de forma gradual y los clientes recibirán una notificación cuando reúnan los requisitos para inscribirse. Para más información sobre las funcionalidades compatibles con el encriptado con clave desechable durante el periodo de implementación, visita [el servicio de ayuda de Ring](#).

¹ El encriptado con clave desechable se convertirá en el nivel de encriptado predeterminado de Ring una vez que esté completamente implementado para todos los clientes.
Información privilegiada y confidencial

43
44
45
46

Este documento describe la nueva arquitectura de encriptado de Ring para los vídeos capturados por las cámaras Ring y almacenados en la infraestructura de Ring.^{1,2} Los vídeos que los clientes decidan compartir con terceros fuera de Ring están cubiertos por los marcos de seguridad de dichos terceros.

¹ En este informe se describe cómo la arquitectura de encriptado de Ring protege los vídeos almacenados en nombre de los clientes con una suscripción a Ring (incluidas las pruebas gratuitas). No se aplica a los vídeos que los clientes decidan compartir con Ring u otros, como los vídeos compartidos a través de la herramienta de donación de vídeos de Ring, los enlaces compartidos o Neighbors.

² Tal y como se describe más adelante en este documento, algunos métodos de recuperación y compatibilidad de funcionalidad no estarán disponibles hasta que el encriptado con clave desechable se haya implementado para todos los clientes.

Qué significa esto en la práctica

Con el encriptado con clave desechable:

1. El videotimbre detecta movimiento en la puerta principal y te lo notifica. Tus vídeos se cifran con claves que cambian con frecuencia. Ring recibe una copia de esas claves y las abre en un enclave seguro.
2. Ring utiliza temporalmente esas claves para procesar el vídeo y admitir funcionalidades activas en tu cuenta, como la búsqueda de vídeo.
3. Después de 24 horas, Ring eliminará de forma permanente su copia de las claves y ya no podrá procesar tus vídeos por sí solo.
4. Una semana después, abres la app de Ring para ver el clip. Dado que Ring ya no tiene las claves, tu app proporciona la clave que Ring necesita para preparar el vídeo para la reproducción, por ejemplo, adaptando la calidad del vídeo a tu conexión. Ring elimina esa clave cuando finaliza el procesamiento, y tu teléfono, tablet o navegador web descifra el vídeo para que puedas verlo.

Con encriptado de extremo a extremo:

1. El videotimbre detecta movimiento en la puerta principal y te lo notifica. Tus vídeos se cifran con claves que cambian con frecuencia. Ring no recibe ninguna copia de esas claves.
2. Ring almacena el vídeo encriptado y lo envía a tus dispositivos, pero no puede descifrarlo en ningún momento.
3. Ring no tiene las claves, por lo que no hay nada que Ring deba eliminar.
4. Una semana después, abres la app de Ring para ver el clip. No se envía ninguna clave a Ring, por lo que Ring no puede preparar el vídeo para su reproducción. Tu teléfono, tablet o navegador web lo descifra y lo reproduce por sí solo.
5. Las funcionalidades como la búsqueda de vídeos, la descripción de vídeo y los usuarios compartidos no están disponibles, puesto que solo tú tienes las llaves.

El encriptado con clave desechable te ofrece acceso a todas las funcionalidades con controles más estrictos. Los clientes que prefieran un control exclusivo sin acceso a las funcionalidades de la nube pueden activar el encriptado de extremo a extremo. Los vídeos siguen estando protegidos con el modo en el que se grabaron, incluso si cambias de modo más adelante. Cambiar los modos solo afecta a las grabaciones nuevas.

Qué cambia con el encriptado con clave desechable

El encriptado con clave desechable será el nuevo valor predeterminado para los vídeos de Ring y reemplazará al valor predeterminado actual una vez que se haya implementado por completo para todos los clientes. Se basa en las protecciones actuales de Ring y añade varios cambios importantes:

	HOY	CON EL ENCRYPTADO CON CLAVE DESECHABLE
ENCRYPTADO PREDETERMINADO	El contenido de vídeo se cifra en tránsito y en reposo	Todas las protecciones actuales, además de que cada cámara añade su propia capa adicional de encriptado con claves únicas que cambian con regularidad y de forma automática.
ACCESO A LA NUBE	Los servicios en la nube de Ring pueden acceder al vídeo	Los servicios en la nube de Ring solo pueden acceder a las claves para las funcionalidades activas en tu cuenta, y solo durante el periodo de 24 horas. Después de eso, Ring solo podrá acceder a la clave si tu app de Ring se la proporciona para una funcionalidad que utilices.
ELIMINAR CLAVE	No eliminar	Ring elimina las claves cada 24 horas de forma rotativa. Después de la eliminación, Ring ya no conserva esas claves.
TUS TELÉFONOS, TABLETS Y NAVEGADORES WEB	Puedes ver tus vídeos	Lo mismo. Los teléfonos, las tablets y los navegadores web guardan sus propias claves para que puedas ver los vídeos en cualquier momento, incluso después de que Ring elimine su copia.

Recuperación de claves

El encriptado con clave desechable y el encriptado de extremo a extremo ofrecen varios métodos de recuperación para que los clientes mantengan el acceso a sus vídeos en caso de pérdida del dispositivo. Ring no puede realizar estas acciones en nombre del cliente. La recuperación se realiza en autoservicio: el cliente elige entre varios métodos de recuperación. Todos los métodos estarán disponibles una vez que se implemente por completo el encriptado con clave desechable. Si estás inscrito en el encriptado con clave desechable, puedes comprobar qué métodos de recuperación están disponibles en la app de Ring en Centro de control > Encriptado de vídeo > Cámaras inscritas.

MÉTODO DE RECUPERACIÓN	¿CÓMO FUNCIONA?	ENCRYPTADO CON CLAVE DESECHABLE	ENCRYPTADO DE EXTREMO A EXTREMO
COPIA DE SEGURIDAD EN LA NUBE (IOS)	Tu clave está almacenada en el Llavero de iCloud y se ha restablecido automáticamente en tu nuevo iPhone o iPad.	Sí	Sí
COPIA DE SEGURIDAD EN LA NUBE (ANDROID)	Tu clave se almacena en Google Blockstore y Google Drive, y se puede restaurar en tu nuevo teléfono o tablet Android.	Sí	Sí

NOTIFICACIÓN PUSH/CÓDIGO QR	Uno de tus teléfonos o tablets actuales aprueba el nuevo	Sí	Sí
FRASE DE CONTRASEÑA	Debes introducir tu frase de contraseña de recuperación en el nuevo teléfono o tablet	Sí	Sí
RECUPERACIÓN POR CÁMARA	Tu clave se almacena en tu cámara Ring. Abre la app de Ring en un teléfono nuevo, sitúate cerca de la cámara Ring y la app se conectará a través de Bluetooth o wifi para restablecer el acceso. Activada de forma predeterminada para el encriptado con clave desechable en cámaras con hardware compatible. Se puede desactivar si no deseas guardar las claves en las cámaras Ring.	Sí	No
CLAVE	Si inicias sesión con una clave que incluye un acceso encriptado a tus claves.	Sí	Sí

La recuperación está diseñada para ser automática siempre que sea posible. Para los clientes que necesiten recuperar manualmente, la frase de contraseña generada durante el registro funciona en cualquier dispositivo y cualquier plataforma, por lo que es la alternativa universal.

[Compartir vídeos y acceso en el encriptado con clave desechable](#)

Solo los teléfonos, tablets y navegadores web registrados pueden ver vídeos descifrados. Si eliminas un teléfono o una tablet de tu cuenta, dejará de tener acceso a tus vídeos. Compartir el acceso a las cámaras con los usuarios compartidos funciona de la misma manera: cuando das a otra persona acceso a una de tus cámaras, sus dispositivos pueden ver vídeos descifrados de esa cámara. Las personas que añadas no podrán ver las grabaciones capturadas antes de ser añadidas, y puedes eliminarles el acceso en cualquier momento; una vez eliminado, ya no tienen acceso a tus vídeos.

Tú decides si quieres compartir tus vídeos, cuándo y con quién. Puedes compartir las grabaciones directamente desde la app de Ring con tus amigos, familiares o cualquier otra persona que elijas, y también puedes descargar vídeos para compartirlos con otros métodos. En las regiones en las que esté disponible la funcionalidad solicitudes de la comunidad de Ring, puedes elegir compartir las grabaciones relevantes con un organismo local de seguridad pública para apoyar una investigación oficial en tu zona. También hemos actualizado nuestras [Pautas para fuerzas y cuerpos de seguridad](#) para reflejar los cambios resultantes de la arquitectura del encriptado con clave desechable.