

# Las interrupciones de los certificados afectan a todo el mundo

Según Security Magazine, el 72 % de las organizaciones sufrió al menos una interrupción relacionada con certificados el último año, causadas principalmente por certificados caducados o no válidos. Estas interrupciones generan riesgos operativos y de seguridad. La gestión del ciclo de vida de los certificados (CLM) evita estos problemas al garantizar que los certificados estén siempre actualizados. Al automatizar la CLM, Sectigo ayuda a las organizaciones a prevenir interrupciones, asegurar la continuidad del negocio y mantener la confianza de los clientes. A continuación, se presentan algunas interrupciones recientes relacionadas con certificados que han sido noticia:

Más información

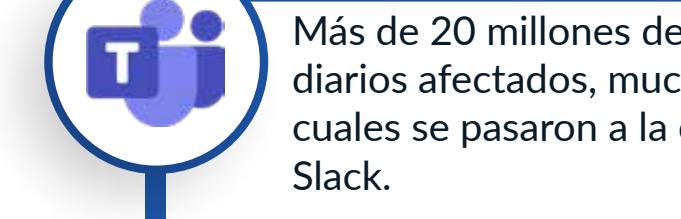
## Spotify

286 millones de usuarios activos con hasta 10 millones de clientes afectados por la interrupción de 30 minutos.



## Microsoft Teams

Más de 20 millones de usuarios diarios afectados, muchos de los cuales se pasaron a la competencia, Slack.



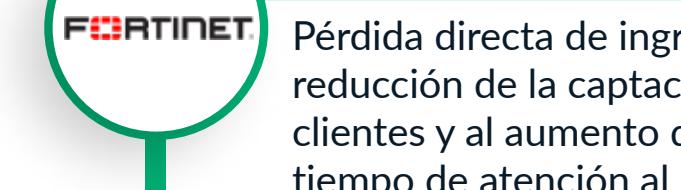
## Shopify

Pérdida directa de ingresos debido a la reducción de la captación de nuevos clientes y al aumento de los costes de tiempo de atención al cliente.



## Fortinet

Pérdida directa de ingresos debido a la reducción de la captación de nuevos clientes y al aumento de los costes de tiempo de atención al cliente.



## Xero

Más de 3,95 millones de suscriptores afectados, con más de 1000 aplicaciones de terceros integradas. El personal de las empresas que utilizan Xero no cobró ese mes.



## Google Voice

Más de 4 horas de interrupción del servicio, durante las cuales los clientes no pudieron utilizar los servicios o productos.



## Spotify

9 horas de interrupción del servicio, durante las cuales no se pudo acceder a los podcasts.



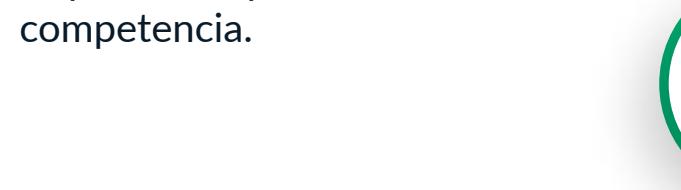
## Tailscale.com

Un certificado caducado provocó una interrupción de 90 minutos.



## Microsoft Teams

Unos pocos minutos de inactividad provocaron varias horas de interrupciones, y muchos usuarios se pasaron a plataformas de la competencia.



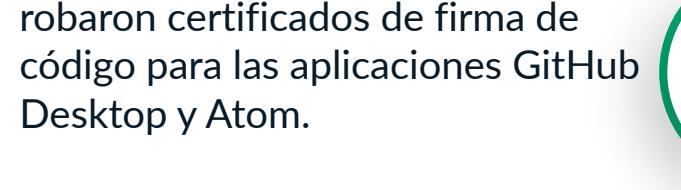
## GitHub

Los intrusos obtuvieron acceso no autorizado a algunos de los repositorios de código de GitHub y robaron certificados de firma de código para las aplicaciones GitHub Desktop y Atom.



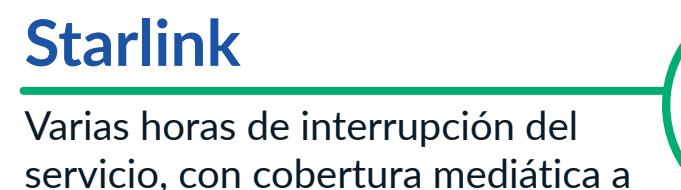
## Cisco (Dos veces en 2023)

Más de 20 000 clientes afectados por la interrupción de la nube, el almacenamiento de datos, las herramientas de comercio electrónico y otros servicios.



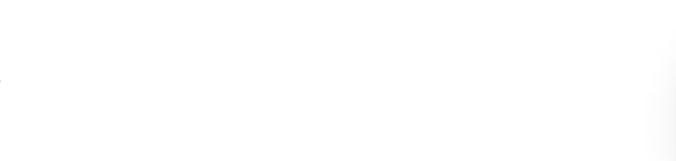
## Starlink

Varias horas de interrupción del servicio, con cobertura mediática a nivel mundial.



## Real Debrid

Un certificado caducado provocó una interrupción del servicio de 45 minutos.



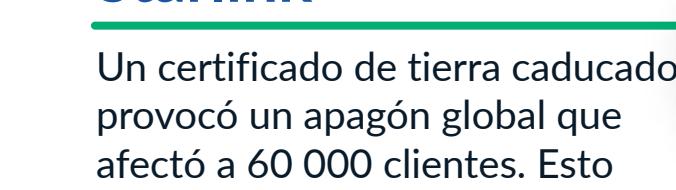
## Banco de Inglaterra

Un sistema de pagos crítico se colapsó debido a un certificado caducado, lo que provocó una interrupción de 90 minutos en CHAPS y en la liquidación minorista.



## Starlink

Un certificado de tierra caducado provocó un apagón global que afectó a 60 000 clientes. Esto también ocurrió en 2023.



## Microsoft

Varios portales de administración de Microsoft 365 y Azure se vieron afectados en todo el mundo.



## League of Legends

Los jugadores no pudieron iniciar sesión durante horas debido a que Riot olvidó renovar el certificado SSL del cliente. Esto también ocurrió hace 10 años.

