

Las interrupciones por certificados afectan a todos

Según Security Magazine, el 72 % de las organizaciones ha sufrido al menos una interrupción relacionada con certificados en el último año; el 67 % las experimenta mensualmente y el 45 %, semanalmente. Estas interrupciones pueden deberse a certificados caducados o invalidados, generando problemas operativos y de seguridad. El CLM automatizado ayuda a prevenirlas y a proteger la continuidad del negocio, la seguridad de las redes y la confianza de los clientes. A continuación, algunos casos recientes que han sido noticia a nivel internacional:

Más información

Spotify

286 millones de usuarios activos y hasta 10 millones de clientes afectados durante una caída de 30 minutos.



Microsoft Teams

Más de 20 millones de usuarios diarios afectados; muchos usuarios se cambiaron a la plataforma competidora Slack.



Shopify

Pérdida directa de ingresos por la disminución en la adquisición de nuevos clientes y el aumento de costes en soporte técnico.



Fortinet

Pérdidas económicas directas debido a la ralentización comercial y al sobrecoste en atención al cliente.



Xero

Más de 3,95 millones de suscriptores afectados y más de 1000 aplicaciones integradas bloqueadas. El personal de las empresas cliente no pudo recibir su nómina ese mes.



Google Voice

Más de 4 horas de interrupción que impidieron a los usuarios utilizar los servicios o productos.



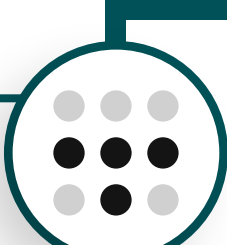
Spotify

9 horas de interrupción total en las que ningún podcast estuvo accesible.



Tailscale.com

Un certificado caducado causó una caída de servicio de 90 minutos.



2024



Microsoft Azure

Fallos en la gestión de certificados causaron interrupciones en EE. UU., afectando a empresas que dependen de la infraestructura cloud de Microsoft.

Microsoft Teams

Una interrupción de unos minutos provocó varias horas de fallos, llevando a los usuarios a optar por soluciones de la competencia.



Outlook

Aunque la caída total duró pocos minutos, los usuarios sufrieron varias horas de inestabilidad antes de restablecer el servicio normal.



GitHub

Atacantes accedieron de forma no autorizada a repositorios de código y robaron certificados de firma de código de las aplicaciones GitHub Desktop y Atom.



Cisco (Deux en 2023)

Más de 20 000 clientes afectados por la interrupción de servicios cloud, almacenamiento de datos y herramientas de comercio



Starlink

Caída global de varias horas con amplia cobertura en medios internacionales.



2023

Bank of England

Un sistema crítico de pagos colapsó por un certificado caducado, provocando una caída de 90 minutos en la red CHAPS y liquidaciones minoristas.



ServiceNow

Fuerte malestar de los usuarios tras un error en un certificado raíz que interrumpió los servicios de más de 600 organizaciones.



Real Debrid

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



2025



Google Chromecast

Interrupción masiva que dejó inoperativos los dispositivos Chromecast debido a la expiración de un certificado emitido en 2015 con validez de 10 años.

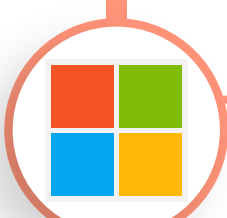
Starlink

Un certificado de estación terrestre caducado provocó un apagón global que afectó a 60 000 clientes (suceso idéntico al ocurrido en 2023).



Microsoft

Varios portales de gestión de Microsoft 365 y Azure se vieron afectados a escala mundial.



League of Legends

Los jugadores no pudieron iniciar sesión durante horas por un certificado SSL caducado, un fallo que Riot ya había sufrido 10 años antes.

