

Historias de éxito

1.000 takedowns al día: cómo las grandes marcas detienen amenazas con Axur

Cuando se trata de amenazas digitales, la rapidez y la precisión marcan la diferencia. Cada minuto que un sitio de phishing o un anuncio fraudulento permanece activo representa un riesgo real para su marca y sus clientes.

La solución de takedown de Axur identifica y elimina amenazas de forma proactiva, permitiendo que su equipo se mantenga un paso adelante sin necesidad de invertir en más recursos internos de ciberseguridad.

Casos reales de éxito en takedown con Axur

Sí, estos casos son reales — y los tiempos de respuesta también.



Incidente de phishing en múltiples frentes

- Detectamos una URL de phishing vinculada a un anuncio fraudulento.
10:56 AM
- La tecnología Web Safe Reporting notificó instantáneamente a 15 entidades, incluyendo proveedores de internet y registradores de dominios, activando pantallas de alerta roja.
10:56 AM
- Takedown notificado automáticamente.
11:16 AM
- URL neutralizada en 20 minutos y anuncio eliminado en 10 horas.
09:16 PM
- **Resuelto. Takedown finalizado.**
09:16 PM

Anuncio fraudulento dirigido a clientes de una **aerolínea**, bloqueado.



Perfil falso de alto riesgo en Facebook

- Con tecnología avanzada, nuestro sistema identificó un perfil falso de alto riesgo en Facebook.
08:45 AM
- El cliente aprueba el takedown con un solo clic, manteniendo control total sobre las notificaciones enviadas.
09:35 AM
- Notificación automática enviada a Meta.
09:51 AM
- Meta confirma que el perfil ya no está disponible, en solo 26 minutos.
10:15 AM
- **Resuelto. Takedown finalizado.**
10:15 AM

Gigante del **comercio electrónico** elimina perfil falso en Facebook con una automatización eficiente.



Amenaza de phishing inicialmente inactiva

- Se detectó una URL de phishing, pero fue marcada inicialmente como inactiva.
02:12 AM
- La URL se activó; la plataforma de Axur notificó automáticamente al cliente.
04:28 AM
- Takedown iniciado con un solo clic; proveedor alertado automáticamente.
04:28 AM
- Resuelto. Takedown finalizado.**
04:54 AM

E-commerce fue objetivo de una campaña de phishing alojada en un dominio previamente estacionado.



Takedown con seguimiento automático

- Takedown con un solo clic iniciado.
06:00 PM
- Tras una notificación de seguimiento, Meta solicitó información adicional.
05:51 PM
- Los datos fueron enviados automáticamente y el perfil fue eliminado el mismo día.
07:51 PM
- Resuelto. Takedown finalizado.**
07:51 PM

Institución financiera eliminó un perfil falso en Facebook que se hacía pasar por su soporte oficial.



Anuncio fraudulento detectado y neutralizado

- Un anuncio fraudulento fue identificado por nuestro recolector de Meta.
08:33 AM
- Takedown solicitado automáticamente por nuestro sistema.
09:10 AM
- Meta confirmó la eliminación del anuncio.
10:05 AM
- Resuelto. Takedown finalizado.**
10:05 AM

E-commerce neutraliza rápidamente anuncios fraudulentos, minimizando riesgos para sus clientes.



Anuncio ilegal de producto en marketplace

- Detección automática de un anuncio prohibido de producto.
05:19 PM
- Alerta enviado a través de la API exclusiva de Axur en colaboración con el marketplace Mercado Libre.
05:27 PM
- Anuncio eliminado; Mercado Libre alertó a otros vendedores.
05:41 PM
- Resuelto. Takedown finalizado.**
05:41 PM

Entidad gubernamental eliminó un anuncio ilegal en solo 14 minutos.



URL de phishing utilizando la marca del cliente

- Nuestra plataforma detectó una URL de phishing que se hacía pasar por el sitio del cliente.
02:12 AM
- Takedown solicitado automáticamente.
10:54 AM
- La tecnología Web Safe Reporting alertó de forma instantánea a 15 entidades, activando pantallas rojas de advertencia sobre la amenaza.
10:54 AM
- El registrador confirmó la eliminación de la URL.
11:14 AM
- Resuelto. Takedown finalizado.**
11:14 AM

E-commerce de belleza neutralizó la amenaza de phishing en solo 49 minutos.



Takedown totalmente automatizado de anuncio

- Incidente creado y clasificado automáticamente.
07:28 PM
- Takedown enviado automáticamente a Meta.
07:36 PM
- El anuncio quedó inaccesible.
08:27 PM
- Resuelto. Takedown finalizado.**
08:27 PM

Institución financiera eliminó un anuncio falso en Facebook en solo 51 minutos.

Respuesta inmediata para un takedown eficaz



Por qué la velocidad y la automatización marcan la diferencia

Imagine despertar y descubrir un anuncio falso o una página de phishing que suplanta su marca. Con Axur, no necesita esperar al horario laboral ni depender de acciones manuales. Nuestros sistemas automatizados detectan, señalan y notifican a las entidades correspondientes en pocos minutos — resolviendo muchas amenazas antes de que escalen.

→ **Reduzca el tiempo de exposición — minimice el daño a la marca y evite la pérdida de clientes. Con un tiempo promedio de actividad de solo 9 horas, no tendrá que esperar días para una solución.**



Transparencia y control en cada etapa

No debería tener que adivinar el estado de sus takedowns. Axur ofrece total transparencia — desde la primera alerta hasta la resolución completa — con una línea de tiempo clara y actualizaciones constantes.

→ **Aumente la confianza en sus procesos de seguridad y mantenga documentación completa para cumplir con normativas o respaldar acciones legales, si es necesario.**

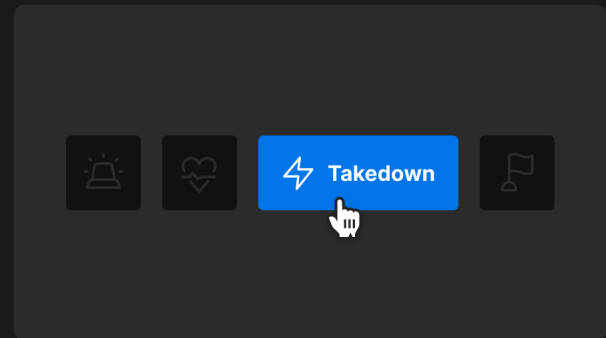


Respuestas para distintos tipos de amenazas

No todas las amenazas se presentan de la misma forma. Ya sea una URL de phishing, un anuncio fraudulento o un producto prohibido listado en un marketplace, la plataforma de Axur se adapta de manera inteligente a cada situación.

Alertamos a ISPs, marketplaces y redes sociales con protocolos personalizados, lo que garantiza takedowns más rápidos y eficaces.

→ **Protección integral — cubriendo múltiples vectores de ataque para asegurar la protección en todos sus canales digitales.**



El diferencial de Axur

Inteligencia automatizada

Nuestros modelos avanzados de IA analizan e identifican amenazas con una precisión incomparable, señalando riesgos antes de que se propaguen.

Alcance global, expertise local

Con conexiones directas a más de 400 ISPs en cinco continentes, garantizamos una respuesta ágil y eficaz — sin importar dónde surja la amenaza.

Web Safe Reporting

Mucho más allá del takedown: nuestra tecnología alerta instantáneamente a las entidades adecuadas, activando medidas de protección como advertencias en el navegador ante sitios de phishing activos.

Proteja su marca, sus clientes y su reputación — más rápido que nunca.

Gartner. Peer Insights. 5/5 ★★★★★

CONOZCA EL MEJOR TAKEDOWN

///AXUR