Folleto de la solución

# Servicios de asesoramiento de Sophos

Reducción proactiva de riesgos y resiliencia frente a las ciberamenazas en constante evolución

## Evaluaciones de seguridad personalizadas a cargo de expertos

Con las continuas exigencias de la transformación digital, el auge de la IA y las ciberamenazas en constante evolución, las organizaciones previsoras son conscientes de que la ciberseguridad no es solo un reto técnico, sino una prioridad estratégica. Los adversarios avanzados, el escrutinio reglamentario y las expectativas de las partes interesadas exigen un enfoque integral y proactivo para proteger los activos digitales. Los servicios de asesoramiento de Sophos ofrecen expertos independientes, experiencia y estrategias personalizadas para identificar vulnerabilidades sistémicas, reforzar las defensas y mejorar la resiliencia empresarial.

Mediante el uso de tácticas, técnicas y procedimientos (TTP) reales utilizados por los ciberdelincuentes, nuestros expertos en seguridad altamente cualificados ponen a prueba sus redes, sistemas y empleados para ayudar a su organización a:

- Identificar vulnerabilidades antes de que los atacantes puedan explotarlas.
- Reforzar las defensas contra amenazas sofisticadas.
- Satisfacer los requisitos normativos.
- Evaluar la preparación para responder ante incidentes.

- Generar confianza entre los clientes, los Partners y las partes interesadas

## Refuerzo proactivo de las defensas y la postura de seguridad

### Pruebas de penetración (pentest)

Las pruebas de penetración simulan ciberataques reales para identificar vulnerabilidades en sistemas, redes y aplicaciones. Los testers experimentados (hackers éticos) tratan de explotar las debilidades para demostrar cómo podría sacarles partido un atacante.

Existen dos tipos principales de pruebas de penetración. Las pruebas de penetración externas se centran en los sistemas a los que se puede acceder desde Internet, como sitios web, VPN y servicios de cara al público. Simulan un atacante que intenta vulnerar su perímetro desde el exterior. Las pruebas de penetración internas simulan una amenaza interna o un atacante que ya ha superado el perímetro, y se centran en los sistemas, las aplicaciones y los datos de la red interna.

#### Por qué son importantes:

- Identifican vulnerabilidades ocultas que los escaneados rutinarios pueden pasar por alto.
- Proporcionan recomendaciones prácticas para reforzar las defensas.
- Ayudan a cumplir la normativa (por ejemplo, PCI DSS, HIPAA, RGPD, SRI, ISO 27001, SOC 2).
- Demuestran un compromiso con la gestión proactiva de riesgos.
- Ofrecen una cobertura completa de los riesgos de seguridad perimetral e interna.

### Preguntas clave que ayudan a responder:

- ¿Dónde están las vulnerabilidades más críticas de nuestra infraestructura?
- ¿Con qué facilidad podría un atacante burlar nuestras defensas externas?
- ¿Qué riesgos existen dentro de nuestra red si un atacante consigue acceder a ella?
- ¿Qué impacto podría tener un ataque fructífero?
- ¿Qué medidas podemos tomar para subsanar las deficiencias identificadas?

## Pruebas de penetración en redes inalámbricas

Las pruebas de penetración en redes inalámbricas evalúan la seguridad de las redes Wi-Fi y la infraestructura de una organización, y comprueban que cumplen con los requisitos normativos pertinentes. Los testers tratan de explotar las vulnerabilidades en el cifrado, la autenticación y los controles de acceso.

Las pruebas de penetración en redes inalámbricas tienen dos ámbitos de aplicación. Las pruebas pasivas consisten en supervisar el tráfico inalámbrico para identificar dispositivos no autorizados, puntos de acceso no autorizados y errores de configuración sin intentar conectarse activamente. Las pruebas activas simulan un atacante que intenta explotar las vulnerabilidades de la red inalámbrica vulnerando el cifrado, eludiendo la autenticación y obteniendo acceso no autorizado.

### Por qué son importantes:

- Protegen los datos confidenciales que se transmiten a través de redes inalámbricas.
- Identifican puntos de acceso no autorizados y errores de configuración.
- Garantizan que las políticas de seguridad inalámbrica se ajustan a las prácticas recomendadas.
- Reducen el riesgo de filtraciones de datos debido a vulnerabilidades Wi-Fi.
- Evalúan tanto los riesgos de exposición pasiva como los de explotación activa.

### Preguntas clave que ayudan a responder:

- ¿Pueden usuarios no autorizados acceder a nuestras redes inalámbricas?
- ¿Utilizamos métodos de cifrado y autenticación seguros?
- ¿Hay dispositivos no autorizados conectados a nuestra red?
- ¿Puede un atacante burlar nuestras protecciones inalámbricas?
- ¿Qué medidas podemos tomar para mejorar la seguridad inalámbrica?

## Evaluaciones de seguridad de las aplicaciones web

Las aplicaciones web suelen manejar datos críticos de la empresa y de los clientes, lo que las convierte en blancos predilectos para los atacantes. Las evaluaciones de seguridad de las aplicaciones web garantizan la seguridad de estas aplicaciones centrándose en vulnerabilidades comunes como la inyección de código SQL, las secuencias de comandos entre sitios (XSS) y la autenticación rota.

Estas evaluaciones pueden incluir pruebas de caja negra (black box testing), en las que el tester simula ser un atacante externo sin conocimiento previo del funcionamiento interno de la aplicación, o pruebas de caja blanca (white box testing), en las que el tester tiene acceso completo al código fuente y a la arquitectura, lo que permite un análisis más profundo de las posibles vulnerabilidades.

### Por qué son importantes:

- Protegen los datos de los clientes y de la empresa gestionados por las aplicaciones web.
- Identifican fallos de codificación y configuración que aumentan el riesgo.
- Ayudan a cumplir estándares como OWASP Top 10 y PCI DSS.
- Reducen el riesgo de ataques de tipo defacement de sitios web, filtraciones de datos y daños a la reputación.
- Ofrecen una perspectiva externa y un análisis en profundidad de la seguridad de las aplicaciones.

### Preguntas clave que ayudan a responder:

- ¿Son nuestras aplicaciones web vulnerables a los métodos de ataque más habituales?
- ¿Los datos confidenciales quedan expuestos debido a fallos de codificación o errores de configuración?
- ¿Puede un atacante externo explotar las vulnerabilidades, o existen problemas más graves en el código?
- ¿Cómo podemos proteger la autenticación de los usuarios y la administración de las sesiones?
- ¿Qué medidas de remediación son necesarias para corregir las vulnerabilidades de las aplicaciones web?

## Resumen de los servicios de asesoramiento de Sophos

| Tipo de prueba | Enfoque | Preguntas clave que abordan | Escenarios de ejemplo |
|---|---|---|---|
| **Pruebas de penetración (pentest)** | Infraestructura, sistemas y redes | ¿Dónde están las vulnerabilidades? ¿Cómo puede un atacante burlar nuestras defensas? | Externas: pruebas de sitios web y servicios de cara al público; internas: pruebas de controles de acceso interno y aumento de privilegios |
| **Pruebas de penetración en redes inalámbricas** | Seguridad Wi-Fi, cifrado, controles de acceso | ¿Es segura nuestra red Wi-Fi? ¿Hay dispositivos no autorizados? | Probar la seguridad de la red Wi-Fi de una oficina; identificar puntos de acceso no autorizados; intentar conexiones no autorizadas |
| **Evaluaciones de seguridad de las aplicaciones web** | Aplicaciones web, fallos de codificación, autenticación | ¿Son seguras nuestras aplicaciones? ¿Quedan expuestos los datos confidenciales? ¿Cómo podemos subsanar las vulnerabilidades? | Pruebas de portales de clientes, sitios de comercio electrónico, aplicaciones web internas; identificar inyección de código SQL, XSS o fallos de autenticación |

## Otros servicios de pruebas de ciberseguridad

Ninguna evaluación o técnica individual aislada proporciona una visión completa de la seguridad de una organización. Cada prueba de adversarios tiene sus propios objetivos y niveles de riesgo aceptables. Sophos puede trabajar con su organización para determinar la combinación de pruebas y técnicas que debe utilizar para evaluar su postura de seguridad y sus controles a fin de identificar sus vulnerabilidades.

**Más información:**
**es.sophos.com/advisory-services**

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com



2025-05-30 BRES (MP)