NEWSLETTER

grupobeit.com

BLOG DEL CEO

En 2026, el Ethical Hacking, los Análisis de Vulnerabilidad y las Pruebas de Penetración dejan de ser ejercicios puntuales para convertirse en una capacidad estratégica continua...

EDICIÓN 52

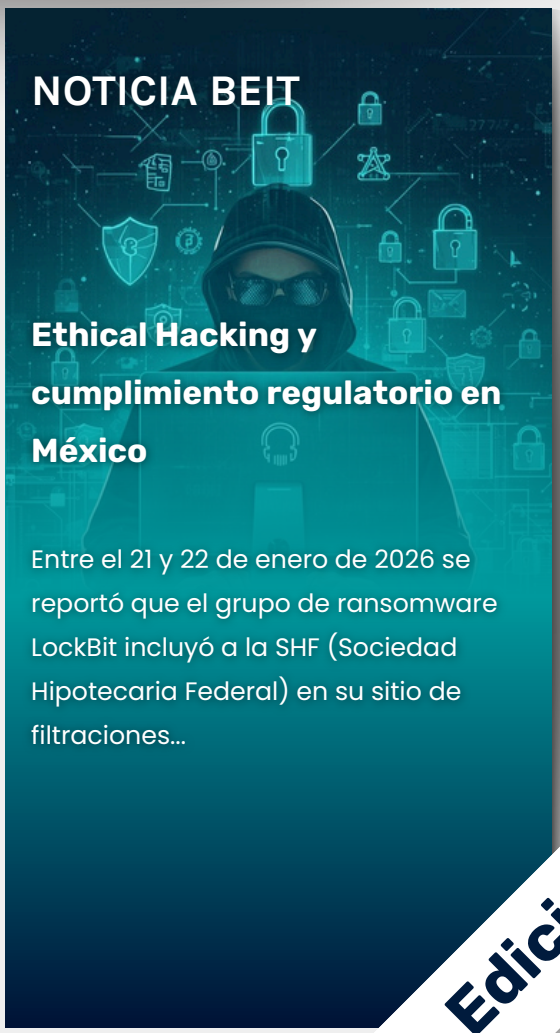
Qué esperar en Ethical Hacking para 2026

En 2026, el Ethical Hacking, los Análisis de Vulnerabilidad y las Pruebas de Penetración dejan de ser ejercicios puntuales para convertirse en una capacidad estratégica continua.

SALES KICK-OFF CON SOPHOS 2026

Nuestro equipo participó en la clínica de ventas impartida por Sophos en las oficinas de LoL, reforzando juntos la visión de construir un entorno digital más seguro...

NOTICIA BEIT



Ethical Hacking y cumplimiento regulatorio en México

Entre el 21 y 22 de enero de 2026 se reportó que el grupo de ransomware LockBit incluyó a la SHF (Sociedad Hipotecaria Federal) en su sitio de filtraciones...

Edición 52

Ethical Hacking: Análisis de Vulnerabilidad y Pruebas de Penetración como pilar estratégico de ciberseguridad

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

En 2026, el Ethical Hacking, los Análisis de Vulnerabilidad y las Pruebas de Penetración dejan de ser ejercicios puntuales para convertirse en **una capacidad estratégica continua.** El crecimiento de ataques automatizados, vulnerabilidades explotables y superficies híbridas ha demostrado que los controles defensivos por sí solos no son suficientes.

Los datos lo confirman: el Verizon Data Breach Investigations Report (DBIR) indica que más del 83 % de las brechas exitosas involucran explotación de vulnerabilidades conocidas, credenciales comprometidas o errores de configuración, todos escenarios que pueden ser detectados mediante pruebas de penetración bien ejecutadas.
Para arrancar 2026 con una postura madura, las organizaciones deben enfocar sus programas de ethical hacking en cuatro ejes clave:

1. Pentesting continuo

El modelo tradicional de pentest anual ya no refleja la realidad operativa. Gartner estima que más del 65 % de los activos digitales cambian al menos una vez al mes (nube, APIs, contenedores). Las organizaciones que adoptan pentesting continuo reducen hasta en 50 % el tiempo de exposición a vulnerabilidades críticas.

2. Priorizar explotación real, no solo CVSS

El NIST y CISA coinciden en que menos del 10 % de las vulnerabilidades publicadas son explotadas activamente, pero concentran la mayoría de los incidentes graves. Los equipos de ethical hacking deben enfocarse en explotabilidad real, rutas de ataque y encadenamiento de fallos, no solo en puntajes teóricos.

3. Seguridad de aplicaciones y APIs como prioridad

OWASP señala que las APIs son ya el vector de ataque más frecuente en aplicaciones modernas, y que fallas como autenticación rota y exposición excesiva de datos lideran los incidentes. Integrar ethical hacking en el SDLC (Software Development Lyfecycle) permite detectar fallos críticos antes de llegar a producción.

4. Ethical hacking como insumo para gobernanza

Los resultados de pentesting deben alimentar métricas ejecutivas: riesgo residual, impacto potencial, tiempo de remediación y exposición regulatoria. En 2026, los consejos directivos exigirán evidencia clara de qué tan explotable es realmente la organización, no solo cuántas vulnerabilidades existen.

En definitiva, el ethical hacking deja de ser una validación técnica para convertirse en una herramienta clave de gestión de riesgo, resiliencia operativa y confianza digital.

Conoce nuestra solución de Ethical Hacking

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Fuentes:

- Verizon — Data Breach Investigations Report 2025: VZ_DBIR_Reports/2025-dbir-data-breach-investigations-report.pdf at main · VCCyberSec/VZ_DBIR_Reports · GitHub
- Gartner — Market Guide for Security Testing Services: Black Duck | 2025 Gartner Magic Quadrant for Application Security Testing
- IBM — Cost of a Data Breach Report 2024: Cost of a data breach 2025 | IBM
- OWASP — Top 10 Security Risks: OWASP Releases 2025 Top 10 List Featuring Two New Security Categories

Ethical Hacking y cumplimiento regulatorio en México

NOTICIA BeIT

Ciberataque a SHF_2026 [LockBit]

Entre el 21 y 22 de enero de 2026 se reportó que el grupo de ransomware LockBit incluyó a la SHF (Sociedad Hipotecaria Federal) en su sitio de filtraciones. Este hecho refuerza la importancia de fortalecer la protección digital, ya que gran parte de los ciberataques se originan por robo de credenciales y malas prácticas de autenticación por parte de los usuarios, basados en estudios de Sophos en 2024 y 2025.

Nuestra visión como Grupo BeIT y la propuesta de Ethical Hacking que brindamos, se enfoca en la prevención. El análisis de vulnerabilidad, pruebas de penetración, análisis de código , monitoreo de la dark web y deep web, que ayudan a nuestros clientes a identificar un baseline esencial para reducir riesgos y elevar la resiliencia organizacional. La ciberseguridad es corresponsabilidad: actúa hoy. admmarketing@buromc.com
+52 56 5100 8613

Cronología del Ciberataque

1. La publicación de LockBit
· La inclusión de la SHF apareció el 21 de enero de 2026 en el portal de LockBit.
· El grupo fijó un plazo de rescate hasta el 5 de febrero de 2026. Si no se paga, la información robada sería publicada.
· No se ha dado a conocer el monto solicitado, pero los ataques de LockBit suelen exigir pagos millonarios en criptomonedas.

2. ¿Por qué este ataque es especialmente grave?
La SHF no es un banco comercial:

- Es una entidad de segundo piso que financia vivienda y opera como brazo hipotecario del Estado mexicano.
- Administra documentación financiera, contractual y operativa estratégica.
- Una filtración en esta institución podría representar una amenaza a la seguridad nacional, al exponer:
- Vulnerabilidades del sistema financiero mexicano
- Información sensible de desarrolladores, financieras, bancos y ciudadanos
- Hasta el momento, la SHF no ha emitido un comunicado oficial detallando el daño, según reportes periodísticos.

3. Confirmaciones desde plataformas de monitoreo de Ransomware

- · La plataforma de inteligencia ransomware.live confirmó que gob.mx (dominio usado por el gobierno mexicano, donde se aloja la SHF) fue listado como víctima por LockBit el 21 de enero de 2026.

4. Línea del tiempo del caso SHF

Fecha Evento:

- 21 ene 2026 LockBit publica a SHF como víctima en la dark web
- 22 ene 2026 Medios mexicanos confirman la advertencia de LockBit y el plazo al 5 de febrero
- 5 feb 2026 Fecha límite impuesta para el pago antes de la filtración masiva

5. Riesgos si LockBit libera la información

De acuerdo con incidentes previos del grupo en México, una filtración podría incluir:

- Datos laborales, fiscales y personales
- Información contractual y financiera
- Documentos de identidad oficiales
- Información de dependencias y empresas relacionadas
- Ejemplos previos muestran que LockBit ha filtrado:
  - CURP, direcciones, teléfonos
  - -RFC, datos bancarios
  - -Contratos y antecedentes penales

Fuentes:

PeriodismoHoy

Publicación | LinkedIn

Edición 52

NEWSLETTER BeIT

Qué esperar en Ethical Hacking para 2026

El 2026 estará marcado por una evolución clara en las pruebas ofensivas: ataques más automatizados, pruebas más especializadas y mayor presión regulatoria. Según CISA (Cybersecurity and Infrastructure Security Agency), el uso de herramientas automatizadas por atacantes ha reducido el tiempo entre la divulgación de una vulnerabilidad y su explotación a menos de 48 horas en promedio.

Para prepararse adecuadamente, las organizaciones deben considerar:

Adoptar modelos híbridos de pentesting

Combinar automatización + hackers expertos permite mayor cobertura sin perder profundidad. Forrester estima que este enfoque reduce costos hasta en 30 % y mejora la detección de fallos críticos complejos.

Incluir pruebas sobre identidades y nube

Microsoft reporta que más del 60 % de los ataques exitosos involucran abuso de identidades. Las pruebas de penetración deben incluir IAM, privilegios, tokens, APIs y configuraciones cloud.

Medir detección y respuesta, no solo explotación

En 2026, un pentest exitoso no será solo “lograr acceso”, sino evaluar si el SOC detecta, responde y contiene el ataque.

Integrar ethical hacking en la estrategia ejecutiva
Los resultados deben traducirse en riesgo financiero, impacto operativo y exposición reputacional. Las organizaciones que lo hacen reducen significativamente su MTTR (Mean Time to Recovery) mejoran la toma de decisiones en crisis.

La conclusión es clara: el ethical hacking será un requisito estratégico, no técnico. Las organizaciones que lo integren de forma continua estarán mejor preparadas para resistir ataques reales y cumplir con las expectativas regulatorias y del mercado.

Para preparar a tu organización frente a amenazas, consulta nuestra solución de Ethical Hacking.

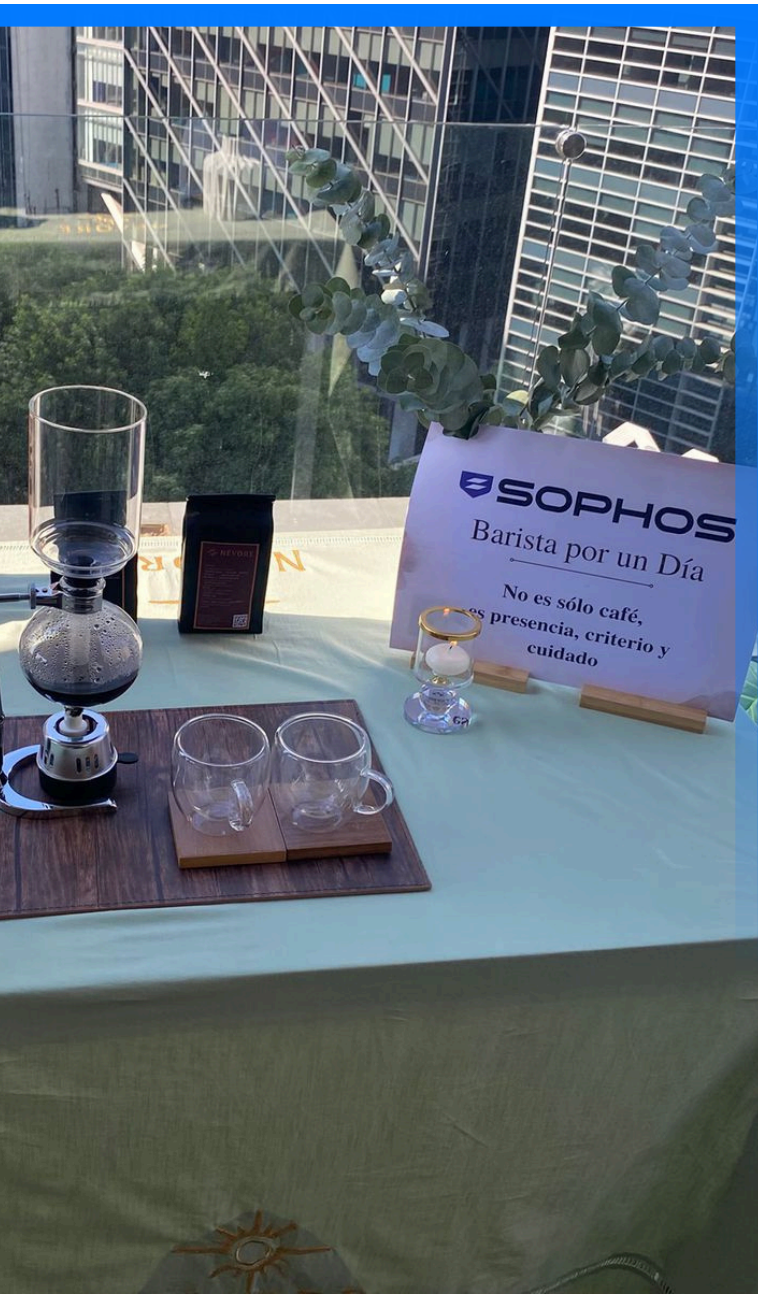
Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Fuentes:

- CISA — Known Exploited Vulnerabilities Catalog: Known Exploited Vulnerabilities Catalog | CISA
- Forrester — The State of Security Testing: The State Of Application Security, 2025 | Forrester
- Microsoft — Digital Defense Report 2025: Microsoft Digital Defense Report 2025 | Microsoft

SALES KICK-OFF CON SOPHOS 2026



Nuestro equipo participó en la clínica de ventas impartida por Sophos en las oficinas de LoL, reforzando juntos la visión de construir un entorno digital más seguro.

Como partners estratégicos, seguimos fortaleciendo nuestras capacidades para ofrecer soluciones de ciberseguridad de clase mundial, impulsando la innovación, la protección avanzada y el acompañamiento experto que nuestros clientes merecen.

En Grupo BeIT, seguimos aprendiendo, colaborando y creciendo para brindar siempre el mejor nivel de defensa digital.