

# Pentesting

Identifica vulnerabilidades hoy,  
evita ataques mañana

La digitalización de las empresas ha traído consigo la necesidad de proteger sus sistemas frente a posibles ciberataques. Estos pueden ocasionar interrupciones en los servicios, pérdidas económicas o la filtración de datos. En este contexto, la ciberseguridad se convierte en un activo esencial para todas las organizaciones, independientemente de su tamaño o sector, garantizando no solo la continuidad operativa, sino también la protección de la información crítica y la confianza de sus clientes y socios.

**Contar con un servicio de pentesting es fundamental para identificar brechas de seguridad antes de que los ciberdelincuentes las exploten.**

Este servicio simula ataques reales, revelando vulnerabilidades en los sistemas de la empresa. Al adelantarse a estas amenazas, se pueden aplicar correcciones a tiempo, reforzando la seguridad y protegiendo los activos digitales de posibles ciberamenazas.

## Identificando brechas internas

Factores como errores humanos, accesos no controlados o falta de formación pueden generar brechas de seguridad. Por eso, es crucial realizar pruebas de penetración para detectar y corregir tanto las vulnerabilidades externas como las internas, garantizando así una protección integral frente a todo tipo de amenazas.

## Beneficios Clave

### Identifica Vulnerabilidades:

Detecta fallos de seguridad antes de que sean aprovechados por ciberdelincuentes.

### Responde ante Incidentes:

Evalúa y mejora la reacción de tu equipo ante ataques.

### Cumple con la Normativa:

Cumple con las nuevas regulaciones como DORA y NIS2, y garantiza la conformidad con normativas consolidadas como GDPR, HIPAA y PCI-DSS.

### Protege los Datos:

Asegura la información crítica de tu empresa.

### Ahorra Costes:

Reduce gastos al prevenir ataques derivados de brechas de seguridad.

### Protección de la reputación:

Evita vulnerabilidades que podrían afectar a la confianza de tus clientes y socios estratégicos.

## Tipos de Pentesting

### Por nivel de acceso

#### Caja Blanca

Acceso total al código y a los sistemas internos.

#### Caja Negra

Sin información previa, simula un ataque externo.

#### Caja Gris

Acceso parcial a la información interna.

### Por objetivo

Redes

Aplicaciones web

Dispositivos móviles

## Fases del Pentesting

- 1. Planificación y preparación**  
Definición del alcance y objetivos.
- 2. Reconocimiento**  
Recolección de información.
- 3. Análisis de vulnerabilidades**  
Identificación de debilidades.
- 4. Explotación**  
Simular ataques para acceder al sistema y evaluar el nivel de riesgo.
- 5. Post-Explotación**  
Obtener información adicional y explorar otras posibles vulnerabilidades.
- 6. Informe y recomendaciones**  
Documentación de hallazgos y recomendaciones.

## Servicios relacionados

Cybersecurity Consulting - CISO as a Service - Data Security  
- Cloud Security - Network Security - Application Security  
- Vulnerability Assessment - Endpoint Security - Threat Intelligence

## Por qué Excelia

### Equipo Especializado:

Nuestro equipo está compuesto por profesionales con una sólida experiencia y certificaciones reconocidas en la industria.

**Enfoque Personalizado:** Nos aseguramos de ofrecer soluciones a medida, adaptando nuestras metodologías y herramientas con las necesidades únicas de tu negocio.

**Informe Claro y Accionable:** Entregamos un informe completo que no solo describe las vulnerabilidades, sino que también ofrece recomendaciones claras y fáciles de implementar.

### Soporte Continuo:

Estamos contigo en cada paso del proceso. Ofrecemos soporte continuo para ayudar a tu equipo a abordar las vulnerabilidades encontradas.