# Caso Auditoría de Seguridad Web Externa basada en OWASP

## Introducción

El portal web oficial de **Interbank** (https://interbank.pe) representa uno de los canales más críticos de interacción digital con sus clientes. A través de este sitio se ofrecen productos, servicios e información clave del banco, además de funcionar como puerta de entrada hacia servicios autenticados como la banca por internet y formularios de atención al cliente.

En el actual panorama de ciberseguridad, los sitios web públicos son objetivos frecuentes de ataques que buscan explotar vulnerabilidades técnicas, debilidades en la configuración de servidores o errores de desarrollo. Por ello, resulta prioritario auditar la seguridad del sitio para prevenir posibles brechas que podrían afectar la integridad, disponibilidad o confidencialidad de los datos y servicios.

**Motivo para la Auditoría:**
Se ha identificado la necesidad de realizar una **Auditoría de Seguridad Web Externa**, centrada en evaluar la exposición del sitio https://interbank.pe ante amenazas externas, sin acceso a sistemas internos ni credenciales. Esta auditoría está alineada con las mejores prácticas del estándar **OWASP Top 10**, ampliamente reconocido para el análisis de riesgos en aplicaciones web.

El objetivo es detectar vulnerabilidades explotables desde Internet y verificar el cumplimiento de prácticas de desarrollo seguro, fortaleciendo la postura de ciberseguridad del banco.

## Descripción de la Organización

**Nombre de la Entidad:** Banco Internacional del Perú - Interbank
**Sector:** Banca y Finanzas
**Ubicación:** Lima, Perú
**Tamaño:** +6000 empleados a nivel nacional
**Servicios Digitales:** Portal web institucional, banca por internet, formularios públicos, contratación de productos financieros en línea.

## Situación Actual

El sitio web de Interbank está disponible públicamente a través del dominio https://interbank.pe. Desde esta plataforma se accede a servicios de alto valor como:

- Banca por internet (login para clientes)
- Simuladores de préstamos y productos financieros
- Formularios de contacto y recopilación de datos personales
- Accesos a subdominios institucionales y campañas digitales

Sin embargo, mediante análisis preliminares pasivos se han detectado posibles debilidades:

1. **Encabezados de Seguridad HTTP:**

- Ausencia de políticas CSP (`Content-Security-Policy`) y HSTS (`Strict-Transport-Security`)
- Falta de `X-Frame-Options`, lo que expone al sitio a ataques de clickjacking

2. **Cookies Inseguras:**
   - Uso de cookies sin los atributos `Secure`, `HttpOnly` o `SameSite`
3. **Exposición Tecnológica:**
   - Uso de bibliotecas JavaScript de terceros con versiones potencialmente vulnerables
4. **Validación Insuficiente en Formularios:**
   - Formularios sin mecanismos visibles anti-spam o verificación CAPTCHA
5. **Mecanismos de Redirección:**
   - Presencia de enlaces a subdominios y servicios autenticados que podrían ser objetivo de phishing o redireccionamiento malicioso

## Justificación para la Auditoría Externa

La evaluación de seguridad externa tiene como finalidad identificar vulnerabilidades técnicas en el sitio web público, verificar el cumplimiento de buenas prácticas de desarrollo seguro y anticiparse a posibles vectores de ataque.

### Razones para la Auditoría:

1. Detección de vulnerabilidades web antes que lo hagan actores maliciosos
2. Evaluación del cumplimiento con OWASP Top 10
3. Prevención de filtraciones de datos o ataques de ingeniería social
4. Fortalecimiento de la seguridad de cookies, sesiones y encabezados HTTP
5. Revisión de la configuración TLS y cifrado de comunicaciones
6. Generación de recomendaciones concretas para el equipo de desarrollo y seguridad

## Producto académico

Plan de auditoría de seguridad web externa según OWASP.