

PENTESTING PARA EL
SECTOR LOGÍSTICO

UNA GUÍA EJECUTIVA PARA TOMADORES DE DECISIÓN EN LOGÍSTICA Y TRANSPORTE

QUÉ ESPERAR Y CÓMO PREPARARSE



www.proyectoscsi.mx

Introducción

En el sector logístico y de transporte, la tecnología impulsa la operación: sistemas de gestión de almacenes (WMS), rastreo satelital, ERP, portales de clientes y plataformas de transporte.

Sin embargo, esa misma digitalización abre una puerta a nuevas amenazas. Un ciberataque puede detener embarques, alterar registros o comprometer datos críticos.

El pentesting (prueba de penetración) permite detectar vulnerabilidades antes de que un atacante lo haga. Pero más allá de la parte técnica, su valor radica en lo que significa para la continuidad de negocio, cumplimiento y reputación de una empresa.



¿Por qué el pentesting es esencial para la logística moderna?

El entorno logístico actual es un blanco atractivo por tres razones:

1. **Interconexión:** sistemas de transporte, aduanas y clientes comparten datos.
2. **Disponibilidad crítica:** un sistema caído significa embarques detenidos.
3. **Cadena de confianza:** las certificaciones como CTPAT y OEA exigen demostrar controles de ciberseguridad.

Un pentest simula los ataques más probables —internos y externos— para evaluar la resistencia de tu infraestructura tecnológica.

Detecta debilidades en redes, aplicaciones, credenciales o configuraciones antes de que sean explotadas.

¿Qué obtiene una empresa del sector logístico al realizar un pentest?

Sistemas:	Visibilidad completa de vulnerabilidades en red, sistemas y accesos.
Finanzas:	Reducción de pérdidas por interrupciones o fraudes digitales.
Departamento Legal:	Cumplimiento de auditorías y certificaciones (CTPAT, ISO 27001, OEA).
Dirección General:	Protección de la continuidad operativa y reputacional ante clientes y socios.



Tipos de pentesting más relevantes para logística

Infraestructura y red:	Evalúa firewalls, routers, servidores y VPNs.
Aplicaciones web:	Portales de clientes, intranets o sistemas de seguimiento.
WiFi Corporativa	Accesos inalámbricos usados en patios, almacenes y oficinas.
Ingeniería social:	Simula ataques de phishing a personal administrativo y operativo.
Pruebas físicas (opcionales):	Evaluación de accesos a salas de servidores o dispositivos críticos.

¿Qué esperar del proceso de pentesting?

Etapa 1 – Planeación

Se define alcance, objetivos, infraestructura y reglas de ejecución.

La empresa conoce qué se va a probar y cómo se evitarán interrupciones.

Etapa 2 – Ejecución

Los especialistas simulan ataques reales utilizando metodologías internacionales (OWASP, OSSTMM, NIST SP 800-115).

Etapa 3 – Análisis y entrega

El reporte final incluye hallazgos priorizados, su impacto, riesgo de explotación y recomendaciones correctivas.

Se acompaña de una reunión ejecutiva para explicar los resultados sin tecnicismos.



Cómo prepararse para una prueba exitosa

- Designar un responsable de coordinación (TI o Seguridad).
- Validar respaldos y accesos antes del inicio.
- Comunicar al personal involucrado que se realizará la prueba.
- Establecer tiempos de ventana para ejecución.
- Asegurar que los hallazgos se traduzcan en acciones medibles.

Resultados esperados

Un pentest bien realizado entrega:

- Un mapa claro de vulnerabilidades priorizadas.
- Acciones concretas de mitigación.
- Evidencia de cumplimiento ante auditores o clientes.
- Reducción del riesgo operativo y reputacional.

El objetivo no es demostrar que existen fallas, sino construir un entorno digital más fuerte, confiable y preparado para los desafíos de la cadena de suministro moderna.



Conclusión

México, es uno de los países más activos de Latinoamérica, depende cada día más de sistemas interconectados entre clientes, transportistas y autoridades.

Un incidente de ciberseguridad podría no solo afectar una empresa, sino toda una cadena logística.

Un pentest brinda la tranquilidad de saber dónde están los riesgos y cómo mitigarlos antes de que causen pérdidas.

En **Proyectos CSI**, ayudamos a empresas logísticas a fortalecer su infraestructura tecnológica con pruebas de penetración diseñadas para minimizar interrupciones y maximizar resultados.

 **Solicita una evaluación gratuita de preparación para pentest**



Escríbenos a ingenieria@Proyectoscsi.mx

Llámanos al 33 4170 8104

Visítanos en <https://proyectoscsi.mx>

Infórmate en blog.proyectoscsi.mx