T.I RESCUE®
SEGURIDAD INFORMÁTICA

GUÍA OPERATIVA · TEMPORADA DE VENTAS 2026

# Checklist de hardening para tu tienda virtual

Proteger tu e-commerce frente al fraude y los ataques DDoS exige planeación **antes, durante y después** de la temporada de ofertas. Esta es tu ruta de trabajo para CyberLunes y Black Friday.

T-30 · Preparación
T-7 · Bloqueo de cambios
T-0 · Monitoreo activo
T+15 · Post-evento

Marca cada tarea a medida que la completes. Cada fase tiene un objetivo distinto: **blindar antes**, **congelar y vigilar durante**, y **cerrar bien después** — porque los chargebacks y la extorsión llegan cuando ya bajaste la guardia.

## T-30 Preparación
30 DÍAS ANTES DEL EVENTO

- [ ] **Pentesting.** Analiza tu sitio web y APIs bajo la guía de seguridad OWASP para detectar fallos de código antes que los atacantes.
- [ ] **Simulación ofensiva.** Contrata ejercicios de Red Team para probar la resistencia de tus bases de datos frente a ataques reales.
- [ ] **Hosting blindado.** Aloja tu backend en servidores dedicados sobre nubes privadas Tier III: costos fijos y sin facturas sorpresa de las nubes elásticas.

## T-7 Bloqueo de cambios
7 DÍAS ANTES DEL EVENTO

- [ ] **Congelación de código (Code Freeze).** Prohíbe de forma estricta cualquier actualización de programación o instalación de plugins en la tienda.
- [ ] **Hardening de WAF.** Configura reglas específicas para proteger los endpoints críticos: `/api/cart` `/api/checkout` `/api/login`.
- [ ] **Copias de seguridad.** Asegura respaldos inmutables bajo las pautas de continuidad de negocio ISO 22301.

## T-0 Monitoreo activo
DÍA DE LANZAMIENTO

- [ ] **Vigilancia SOC activa.** Monitorea en tiempo real el uso de CPU de tus bases de datos y servidores web para detectar saturaciones a tiempo.
- [ ] **Control de errores de red.** Revisa de inmediato si la plataforma empieza a arrojar errores `HTTP 502` o `504`, señal de saturación del servidor.

## T+15 Post-evento
15 DÍAS DESPUÉS DEL EVENTO

- [ ] **Conciliación de contra-cargos.** Monitorea y atiende las disputas bancarias tempranas para defender tus ingresos y tu reputación.
- [ ] **Ajuste de filtros.** Revisa las IPs bloqueadas durante el evento y optimiza el WAF para reducir falsos positivos en el futuro.
- [ ] **Prevención de extorsiones (RDoS).** Reporta y bloquea los correos que exijan pagos en criptomonedas bajo amenaza de tumbar tu plataforma durante los despachos logísticos de fin de año.

**¿No tienes equipo para cubrir las cuatro fases?** En T.I. RESCUE operamos el SOC, el WAF y la infraestructura blindada por ti, antes, durante y después del pico. Escríbenos a **tirescue.com**.