Checklist de Seguridad

20 puntos críticos antes de lanzar tu aplicación

Autenticación y Autorización

- & Contraseñas hasheadas con bcrypt o Argon2
- & Rate limiting implementado en login (máx 5 intentos)
- & Tokens JWT con expiración corta (< 1 hora)
- & Validar permisos en cada endpoint del backend
- & Implementar 2FA para accesos administrativos

Protección de Datos

- & HTTPS obligatorio en toda la aplicación
- & Datos sensibles encriptados en base de datos
- & No exponer IDs secuenciales en URLs
- & Sanitizar todos los inputs (prevenir XSS)
- & Usar queries parametrizadas (prevenir SQL injection)

Infraestructura

- & Firewall configurado correctamente
- & Puertos innecesarios cerrados
- & Backups automáticos funcionando y probados
- & Logs de auditoría habilitados
- & Secrets en variables de entorno, no en código

Monitoreo y Respuesta

- & Alertas para intentos de login fallidos masivos
- & Monitoreo de cambios en archivos críticos
- & Plan de respuesta a incidentes documentado
- & Contactos de emergencia actualizados
- & Procedimiento de rotación de secrets definido