SEGURIDAD EN JOOMLA:
BLINDANDO TU PYME SIN VOLVERTE LOCO
GUÍA PRÁCTICA PARA PEQUEÑAS Y MEDIANAS EMPRESAS

1. HERRAMIENTAS NATIVAS

AUTENTICACIÓN MULTIFACTOR (MFA)

El muro que nadie salta. ¡Actívalo hoy!
(Usa Google Authenticator o llaves físicas)

Obliga MFA a todos los usuarios con acceso al backend

ARCHIVO .htaccess

Tu primer escudo real. Bloquea ataques (SQL, XSS), protege configuration.php, evita listado de directorios

2. CONFIGURACIONES TÉCNICAS CLAVE

PERMISOS DE ARCHIVOS Y CARPETAS

Carpetas → 755.
Archivos → 644

Un permisoo mal configurado es come dejar la puerta abierta

PRINCIPIO DEL MÍNIMO PRIVILEGIO

Menos es más (y más seguro).
No des más permisos de los necesarios

ACL. details

3. EVITA ESTOS ERRORES COMUNES

- Usar "admin" como usuario
- No actualizar Joomla o extensiones
- Instalar extensiones pirata
- No tener copias de seguridad automáticas
- Usar contraseñas tipo "123456"

CHECKLIST RÁPIDO PARA HOY

- [x] Activar MFA
- [x] Revisar .htaccess
- [x] Configurar permisos 755/644
- [x] Aplicar principio de mínimo privilegio
- [x] Actualizar todo (Joomla + extensiones)
- [x] Copias de seguridad automáticas

Si haces esto, estarás por delante del 80% de webs vulnerables

CONCLUSIÓN: SEGURIDAD SIN DRAMA

La seguridad no va de paranoia... va de sentido común.
No necesitas herramientas mágicas. Necesitas disciplina.
Tu presupuesto no importa tanto como tus decisiones