Recomendaciones de Seguridad

01

ACTUALIZACIONES

Mantener actualizado el sitio web es fundamental para parchear vulnerabilidades existentes en versiones obsoletas.

02

COPIAS DE SEGURIDAD

Realizar copias de seguridad, permite recuperar nuestros sistemas ante desastres provocados por ataques o incidencias en las actualizaciones.

03

CREDENCIALES

Establecer contraseñas seguras y rotar las mismas de forma periódica ayuda a mantener su sitio web seguro.

04

EMPLEO DE CLAVES TEMPORALES

Utilizar claves de un solo uso (OTP) y el doble factor de autenticación (2FA) permite reforzar el sistema de autenticación del sitio web.

05

LIMITAR INTENTOS DE ACCESO

Establecer un número máximo de intentos de conexión ayuda a bloquear ataques de fuerza bruta

06

LIMITAR LA AUTENTICACIÓN POR LOCALIZACIÓN DE IP

Establecer una zona para conectarse al panel de administración limitará los ataques producidos desde otros países.

07

INSTALAR CERTIFICADOS DE SEGURIDAD (SSL)

Implementar un certificado de seguridad en la web permitirá establecer una canal seguro de comunicación además de ayudar al posicionamiento y a tu imagen como empresa.

08

EVALUAR PRESTADORES DE SERVICIO

Analizar las garantías que nos ofrece un tercero (hosting, desarrollador web, etc...) contribuirá al funcionamiento correcto de su sitio web.

09

PROTEGER ARCHIVOS Y CARPETAS DEL SISTEMA

Blindar carpetas y archivos de sistema mediante la limitación de permisos permitirá evitar ataques direccionados a la estructura de archivos de su página web.

10

REVISA LAS APLICACIONES DE TERCEROS

La frecuencia de actualización, la reputación de un proveedor y la auditoría de una aplicación antes de instalarla permitirá evitar posibles intrusiones o fallos en la configuración.