PROTECCIÓN DIGITAL PARA SU INSTITUCIÓN

PROPUESTA DE SERVICIO —

FIREWALL DE APLICACIONES WEB (WAF)

WAF + CDN + DNS administrados para blindar su presencia digital contra ataques reales.

PREPARADO PARA

Cooperativa de Ahorro y Crédito Abierta "San Francisco Solano" R.L.

Sitio evaluado: sfs.com.bo (WordPress) · Escaneo OWASP ZAP del 10 de agosto de 2026

COCHABAMBA, 10 DE AGOSTO DE 2026 · INFO@HABILWEB.COM · +591 71490444 · WWW.HABILWEB.COM

Documento de entendimiento preliminar — la propuesta económica se presentará en la cotización formal.

+90.000

ataques por minuto contra sitios WordPress.
Cada minuto, todos los días.

ARISHI

UNA COOPERATIVA FINANCIERA ES UN BLANCO PRIORITARIO

Nadie deja abierta la puerta principal de su institución. En el mundo digital pasa igual — solo que para un atacante es mucho más fácil entrar, hacer cambios sin que nadie lo note y desaparecer sin dejar rastro. Y las instituciones financieras encabezan la lista de objetivos: mueven dinero y datos sensibles de miles de socios.

El sitio institucional de la Cooperativa opera sobre WordPress, la plataforma más usada del mundo y, precisamente por eso, la más atacada. Este documento resume (1) por qué usar WordPress sin protección ya es un riesgo en sí mismo, (2) qué encontramos en un escaneo de seguridad real de sfs.com.bo, y (3) cómo el servicio administrado de HABILWEB cierra esas brechas.

USAR WORDPRESS SIN BLINDAJE YA ES PELIGROSO

WordPress mueve casi la mitad de la web. Esa popularidad lo convierte en el blanco número uno: los bots no eligen víctima, escanean todo — un sitio nuevo recibe más de 2.000 intentos de ataque en sus primeras 24 horas.

~13.000

sitios web hackeados cada día (≈ 4,7 millones al año).

SOPHOS

90.000 /min

ataques por minuto contra sitios WordPress.

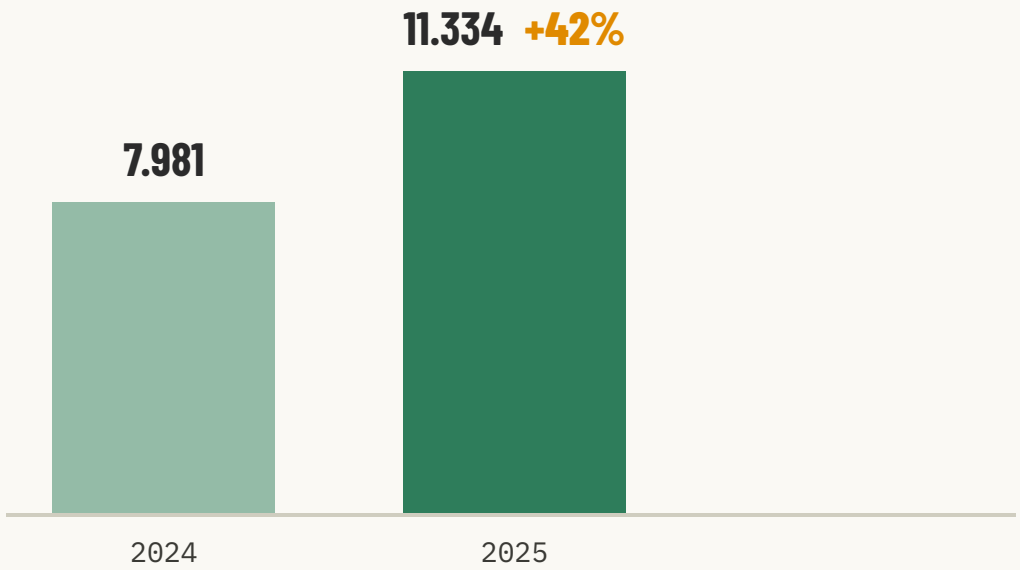
ARISHI

5 horas

entre que se descubre una falla y su explotación masiva.

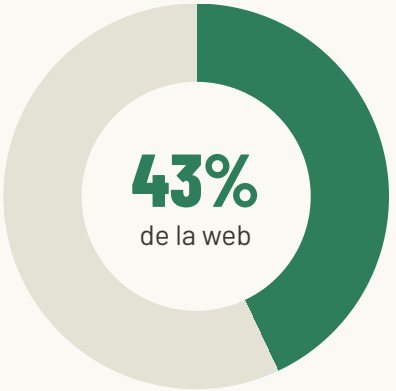
PATCHSTACK 2026

VULNERABILIDADES NUEVAS POR AÑO EN EL ECOSISTEMA WORDPRESS



FUENTE: PATCHSTACK 2026

WORDPRESS MUEVE EL 43% DE TODA LA WEB



Por eso es el blanco número uno de los atacantes.

97%

DE LOS ATAQUES SON AUTOMATIZADOS

— bots que no descansan

WPMANAGENINJA

91%

DE LAS VULNERABILIDADES ESTÁN EN PLUGINS

— no en el núcleo de WordPress

PATCHSTACK 2026

> La conclusión es directa: el sitio de la Cooperativa usa WordPress con plugins (Elementor, Essential Addons, Download Manager) — el terreno exacto donde se concentra el 91% de las vulnerabilidades — y los atacantes son bots que prueban cada falla nueva en cuestión de horas. Esperar a ser atacado no es una estrategia: se necesita un firewall de aplicaciones web (WAF) delante del sitio.

QUÉ ENCONTRAMOS EN sfs.com.bo

No hablamos en abstracto: ejecutamos un escaneo de seguridad OWASP ZAP 2.17.0 sobre el sitio de la Cooperativa el 10 de agosto de 2026. Resultado: 12 alertas — 0 de riesgo alto, 7 de riesgo medio (la mayoría sistémicas, es decir que afectan a todo el sitio) y 5 de riesgo bajo.

0

alertas de riesgo ALTO — aún no hay una puerta abierta de par en par

7

alertas de riesgo MEDIO — la mayoría sistémicas (afectan a todo el sitio)

5

alertas de riesgo BAJO — fugas de información y configuración

EN LENGUAJE SIMPLE

Hoy el sitio no tiene una política de seguridad de contenidos (CSP) efectiva, no obliga a los navegadores a usar siempre la conexión cifrada (HSTS), carga scripts de terceros sin verificación de integridad y utiliza un componente JavaScript con vulnerabilidades públicamente conocidas (DOMPurify 3.2.6, incluido por el plugin Essential Addons for Elementor, con más de 15 CVE publicados).

Ninguna de estas brechas por sí sola implica que el sitio esté comprometido, pero en conjunto dejan el terreno preparado para ataques de inyección de código (XSS), clonación/phishing y robo de sesiones — exactamente el tipo de ataque que los bots automatizados intentan a diario.

> Estas brechas son la puerta de entrada típica para suplantar la imagen institucional de la Cooperativa ante sus socios. Cerrarlas cuesta mucho menos que un solo incidente.

LOS 12 HALLAZGOS, EXPLICADOS RIESGO MEDIO

HALLAZGO	RIESGO	QUÉ SIGNIFICA PARA LA COOPERATIVA	CÓMO LO ABORDA HABILWEB
Librería JS vulnerable (DOMPurify 3.2.6)	MEDIO	Componente del plugin Essential Addons for Elementor con más de 15 CVE públicos (bypass XSS).	Parcheo virtual en el WAF + recomendación de actualizar el plugin.
CSP: directiva wildcard / sin fallback / unsafe-inline (4 alertas, sistémicas)	MEDIO	Sin una política CSP real, un atacante que logre inyectar código puede ejecutarlo sin restricción en el navegador del socio.	El WAF/CDN inyecta cabeceras CSP endurecidas para todo el sitio.
Falta integridad en recursos externos (SRI) — 6 instancias	MEDIO	Scripts y estilos de Google Fonts / Tag Manager se cargan sin verificación; si el tercero es comprometido, el sitio ejecuta su código.	Reglas de origen confiable + ajuste de etiquetas en hardening.
Sitio accesible solo por HTTP en una prueba	MEDIO	Hubo al menos una respuesta sin cifrado; el tráfico podría ser leído o alterado en tránsito.	HTTPS forzado extremo a extremo con SSL incluido en el plan.

LOS 12 HALLAZGOS, EXPLICADOS RIESGO BAJO

HALLAZGO	RIESGO	QUÉ SIGNIFICA PARA LA COOPERATIVA	CÓMO LO ABORDA HABILWEB
Strict-Transport-Security (HSTS) no establecido	BAJO	El navegador no está obligado a usar siempre HTTPS: abre la puerta a ataques de degradación (SSL stripping).	El WAF añade la cabecera HSTS en todas las respuestas.
Cookies sin atributo SameSite (__wpdm_client)	BAJO	Cookies del plugin Download Manager pueden viajar en peticiones de otros sitios (CSRF).	Reescritura de cookies en el borde + hardening de WordPress.
Divulgación de marcas de tiempo Unix (sistémico)	BAJO	El sitio revela información interna útil para perfilar el servidor.	Filtrado/normalización de respuestas en el WAF.
Redirecciones con contenido (posible fuga) — 4 instancias	BAJO	Las redirecciones devuelven cuerpo de respuesta; podría filtrarse información sensible.	Normalización de redirecciones en el borde.
Inclusión de JS entre dominios — 3 instancias	BAJO	Scripts de terceros (Google Tag Manager) sin control centralizado.	Lista de orígenes permitidos vía CSP administrada.

Las 4 alertas de CSP del reporte se agrupan en una sola fila por tratarse de la misma causa raíz. El reporte técnico completo de OWASP ZAP (16 páginas, con URLs, evidencia y referencias CVE/CWE) está disponible para el área de sistemas de la Cooperativa.

QUÉ MEJORA EL PLAN SEGURIDAD WEB DE HABILWEB

Proponemos el Plan Seguridad Web: WAF + CDN + DNS, 100% administrado por HABILWEB desde Cochabamba. La Cooperativa no necesita conocimientos técnicos ni cambios en su equipo: nosotros configuramos, monitoreamos y mantenemos la protección.

01

WAF — FIREWALL DE APLICACIONES

Frena inyecciones SQL, XSS y ataques DDoS en tiempo real, antes de que toquen el servidor. Incluye reglas OWASP y reglas específicas para WordPress/CMS, con parcheo virtual: bloquea la explotación de vulnerabilidades conocidas (como las del plugin detectado) mientras se actualiza el componente.

02

CABECERAS DE SEGURIDAD ADMINISTRADAS

Resolvemos de raíz 7 de los 12 hallazgos del escaneo: CSP endurecida, HSTS, HTTPS forzado y control de orígenes de scripts — sin tocar el código del sitio.

03

CDN — RED DE DISTRIBUCIÓN

El sitio carga más rápido para los socios en todo el país y absorbe los picos de tráfico malicioso. Protección DDoS ilimitada y certificado SSL incluido.

QUÉ MEJORA EL PLAN SEGURIDAD WEB DE HABILWEB

04

DNS PROTEGIDO

Zonas y registros administrados con red de protección DDoS: cada visitante y cada correo llega al lugar correcto, sin secuestro de dominio.

05

MITIGACIÓN DE BOTS

El 97% de los ataques son automatizados; el filtrado en el borde los descarta antes de que consuman recursos o encuentren una brecha.

06

MONITOREO Y SOPORTE LOCAL

Equipo en Cochabamba, atención por WhatsApp y llamada. Si algo ocurre, actuamos — cada hora cuenta.

Complemento recomendado (fuera del alcance de esta propuesta inicial): actualización del plugin con la librería vulnerable y hardening puntual de WordPress (cookies SameSite, atributos de integridad SRI). El WAF mitiga el riesgo de inmediato; la actualización lo elimina de forma definitiva.

UN SERVICIO, CUATRO CAPAS, CERO CARGA PARA SU EQUIPO

Este es un documento de entendimiento preliminar: consolida los hallazgos del escaneo y el alcance del servicio propuesto. La propuesta económica se presentará en la cotización formal, una vez validado el alcance con la Cooperativa. La implementación no requiere migrar el sitio ni interrumpir el servicio: el cambio se realiza a nivel de DNS de forma transparente.

CAPA 1

WAF

Firewall de aplicaciones

CAPA 2

CDN

Red de distribución

CAPA 3

DNS

DNS protegido

CAPA 4

MONITOREO

Soporte local

¿CONVERSAMOS?

BLINDEMOS EL SITIO DE LA COOPERATIVA ANTES DE QUE LO NECESITE.

WhatsApp / Llamadas: +591 71490444 · info@habilweb.com · www.habilweb.com

Fuentes de cifras de mercado: Sophos, Arishi, WPManageNinja, Patchstack 2026 (cifra 2024 calculada a partir del +42% reportado). Hallazgos técnicos: escaneo OWASP ZAP 2.17.0 sobre https://sfs.com.bo, 10 de agosto de 2026. Documento interno de trabajo — no constituye aún una oferta comercial.