# INFORME DE IMPLEMENTACIÓN CLOUDFLARE Y REGLAS DE SEGURIDAD WAF EN EL DOMINIO INSTITUCIONAL

El presente informe detalla la implementación estratégica de Cloudflare como Capa de Seguridad Perimetral (WAF - Web Application Firewall) para el dominio oficial del instituto. Esta migración implicó el cambio de los Nameservers de tenjoculturayturismo.gov.co para que el tráfico del sitio web sea gestionado y filtrado directamente por la infraestructura global de Cloudflare antes de llegar a nuestro servidor de alojamiento.

Este cambio fundamental transforma la postura de seguridad de la plataforma, moviéndola de un enfoque reactivo (limpiar el servidor después de un ataque) a un enfoque proactivo (detener el ataque en el borde).

## Beneficios Clave y Ganancias en Seguridad

La integración de Cloudflare WAF y la aplicación de reglas de seguridad específicas ofrecen las siguientes ventajas inmediatas:

| Categoría | Beneficio Clave | Ganancia en Seguridad |
|---|---|---|
| Seguridad | Defensa perimetral robusta y siempre activa. | Protección inmediata contra listas negras de bots, vulnerabilidades Zero-Day conocidas y ataques DDoS volumétricos. |

| Categoría | Beneficio Clave | Ganancia en Seguridad |
|---|---|---|
| Rendimiento | Filtrado de tráfico no deseado (bots, spam, atacantes). | Reducción drástica en la carga del servidor de hosting, asegurando que los recursos (CPU/RAM) se utilicen únicamente para servir contenido a visitantes legítimos. |
| Continuidad | Mayor disponibilidad del sitio. | Mitigación instantánea de ataques que podrían saturar o tumbar el servidor, garantizando que la plataforma permanezca accesible. |
| Inteligencia | Visibilidad sobre el panorama de amenazas. | Reportes detallados sobre la geolocalización, tipo y frecuencia de los ataques bloqueados, permitiendo refinar continuamente las políticas de seguridad. |
| Costo | Ahorro de costos operativos. | Menos tiempo invertido por el equipo de TI en respuesta a incidentes, limpieza de *malware* y recuperación de copias de seguridad por hackeos. |

# Implementación de reglas de seguridad WAF

Objetivo: Proteger la infraestructura del instituto contra accesos no autorizados, ataques de fuerza bruta y explotación de vulnerabilidades conocidas en la plataforma WordPress.

1. Restricción Geográfica de Acceso Administrativo

Regla: Bloqueo de acceso a wp-admin y wp-login.php para peticiones fuera de Colombia.

- Lo que hace: Filtra cualquier intento de inicio de sesión que no provenga de una IP colombiana.
- Justificación Técnica: El 90% de los ataques de fuerza bruta (intentos automatizados de adivinar contraseñas) provienen de redes de bots distribuidas globalmente (frecuentemente de países como China, Rusia o EE. UU.).
- Beneficio: Elimina de golpe la mayoría de los intentos de hacking automatizado. Al detener estas peticiones en el "borde" (Cloudflare), el servidor del instituto ni siquiera se entera del ataque, ahorrando CPU y memoria.

2. Bloqueo del Protocolo XML-RPC

Regla: Denegar acceso al archivo xmlrpc.php.

- Lo que hace: Deshabilita una función antigua de WordPress que permite interactuar con el sitio de forma remota.
- Justificación Técnica: Este archivo es uno de los vectores de ataque más comunes. Los atacantes lo usan para:

    a. Ataques de Fuerza Bruta Amplificados: Permite probar cientos de combinaciones de usuario/contraseña en una sola petición.
    b. Ataques DDoS: El archivo puede ser usado para convertir el sitio en un "amplificador" de ataques hacia otros servidores.
- Beneficio: Cierra una de las vulnerabilidades más explotadas de WordPress sin afectar la navegación de los usuarios o estudiantes.

## Resumen de Beneficios para el Instituto

Al migrar los nameservers a Cloudflare y aplicar estas reglas, el instituto obtiene:

1. Seguridad Proactiva: Las amenazas se detienen antes de llegar al servidor de hosting. Si un atacante intenta entrar, Cloudflare lo bloquea en sus propios servidores.
2. Optimización de Rendimiento: Al filtrar el "tráfico basura" y los bots maliciosos, el ancho de banda y la potencia del servidor se reservan exclusivamente para los estudiantes y docentes.
3. Reducción de Costos de Mantenimiento: Menos ataques exitosos significan menos tiempo dedicado a "limpiar" el sitio de virus o recuperar copias de seguridad por hackeos.
4. Visibilidad: Cloudflare entrega reportes detallados de cuántos ataques han sido detenidos, permitiendo al equipo de TI presentar métricas reales de protección.