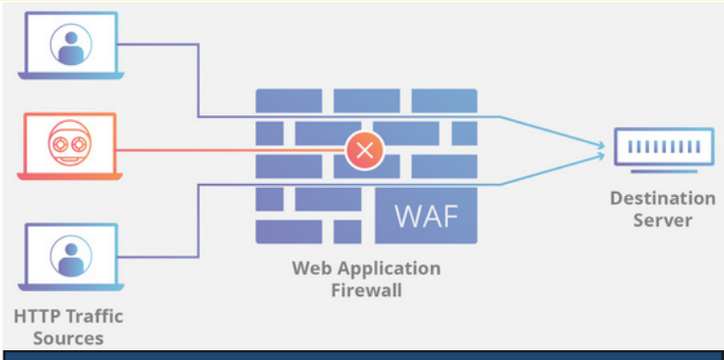
# WAF
## Firewall de Aplicaciones Web

COSIM
22 años en CiberSeguridad

## Proteja su Web Transaccional

Las aplicaciones web son un objetivo clave para los ciberataques ya que son facilmente accesibles y ofrecen un punto de entrada fácil a datos valiosos. Las organizaciones necesitan proteger las aplicaciones web de las amenazas cibernéticas existentes y emergentes sin afectar el rendimiento, el tiempo de negocio o el tiempo de actividad. El rápido ritmo de los cambios en las aplicaciones puede hacer que sea muy dificil para los equipos de seguridad mantenerse al día con las reglas de actualización que protegen adecuadamente los activos web. Esto puede crear brechas de seguridad y vulnerabilidades que los ciberdelincuentes pueden explotar, dando lugar a costosas filtraciones de datos. Asimismo, las organizaciones buscan implementar soluciones de seguridad que puedan escalar con sus aplicaciones para igualar el crecimiento en la demanda de los usuarios, asegurando que los activos web estén protegidos.




## ¿Qué es un WAF?

**Es un dispositivo hardware o software que permite proteger los servidores de aplicaciones web contra determinados ataques específicos en Internet sobre el protocolo HTTP/HTTPS. Se controlan las transacciones al servidor web de nuestro negocio. Es un control complementario al firewall de red tradicional.**

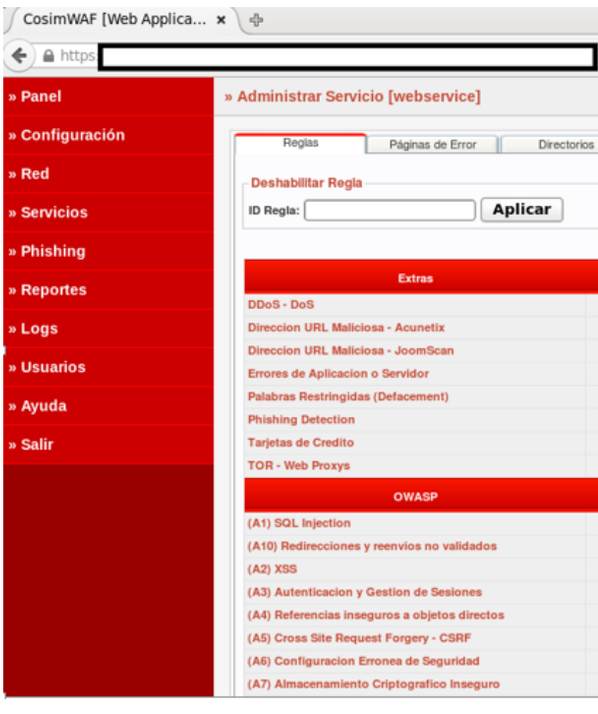
## Solución CosimWAF para el cumplimiento de OWASP y PCI-DSS

CosimWAF ofrece una capa de seguridad adicional altamente escalable de protección contra ataques a las aplicaciones web, emitiendo alertas de seguridad y bloqueando a los atacantes antes de que lleguen a comprometer los servidores web, filtrando todo el tráfico HTTP/HTTPS de entrada desde Internet, através de reglas parametrizables por la organización.
CosimWAF cuenta con su propio PANEL WEB de administración sobre los sitios y aplicaciones web que están siendo protegidos .

## Reglas y Políticas de Seguridad para su Banca Web

Más de 500 reglas de protección contra ataques a las aplicaciones Web, como ser: Inyecciones SQL, XSS, CSRF, RFI, LFI, inyecciones LDAP, ejecución remota de código, entre otros.

- Detección y bloqueo de ataques ejecutados por herramientas automatizadas (Acunetix, Nessus, SQLMap, etc.)
- Protección de la autenticación de clientes contra ataques de fuerza bruta o diccionario de contraseñas.
- Protección de múltiples servidores web de la Entidad.
- Protección contra ataques de Negación de Servicios (DoS)
- Protección de Web-Services.
- Protección contra ataques bots (SPAM) a formularios.
- Bloqueo de visitantes anónimos (TOR o proxys) así como de países en lista negra según la UIF.
- Pantallas de error personalizadas para no brindar detalles técnicos a posibles atacantes.
- Intentos de acceso no autorizado al panel de administración de Cosim-WAF.



# Algunos Beneficios de Cosim-WAF

1. Permite bloqueo automático o manual contra ataques a los sitios web protegidos.
2. Más de 500 reglas de seguridad configurables para diferentes ataques (SQL, XSS, entre otros)
3. Permite generar reportes técnicos y ejecutivos, exportarlos en HTML o PDF con su propio logo.
4. Las alertas son notificadas vía correo electrónico al personal de seguridad de la entidad.
5. Permite generar backups de configuraciones, logs y de las reglas del WAF, además de poder visualizar el consumo de recursos de hardware y ancho de banda en la red.
6. Permite una administración intuitiva de la herramienta y sus reglas desde el panel web (GUI).
7. Permite actualizaciones automáticas tanto de la plataforma WAF como de nuevas reglas.
8. Permite administración de usuarios técnicos con diferentes roles y niveles de configuración.
9. Las reglas por defecto están enfocadas en el cumplimiento del estándar PCI-DSS Req. 6.6.
10. Soporte y capacitación local (Bolivia) a cargo de personal de COSIM certificado en el manejo de la herramienta.

## Menú de Reportes

La entidad puede generar reportes por aplicación, fecha, país, dirección IP:

- Ataques detectados.
- Bloqueos por IP.
- Errores generados por la aplicación o servidor web.
- Visitas de clientes
- Accesos al panel de administración.
- Gráfica estadística de ataques


## Características principales

### Bloqueo de IPs sospechosas y Lista Negra

Permite manejar listas negras (UIF - Unidad de Investigación Financiera) y listas blancas (según políticas de la entidad). Bloque automatizado de atacantes.

El bloqueo de IPs puede ser temporal, permanente o removido de forma manual por el administrador WAF.

### Dashboard de Servicios Protegidos

Soporta aplicaciones web desarrolladas en ASP.NET, PHP, ASP, JSF, JSP, o Web-Services.

Soporta servidores web sobre plataformas Apache, Tomcat, CheroKee, y Microsoft IIS.

Soporta aplicaciones web sobre protocolos HTTP y HTTPS. Balanceo de carga y caching web.

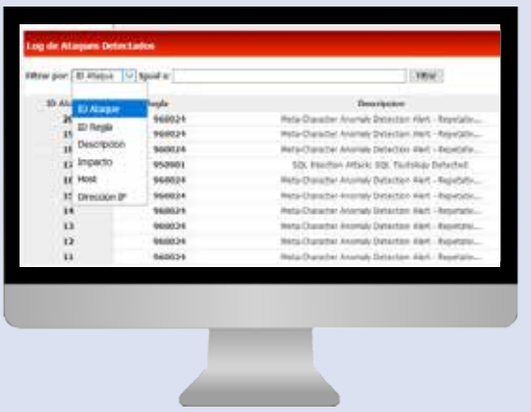
Permite administrar certificados digitales.

# Capacidades principales

## Seguimiento a Ataques

Cada ataque registrado cuenta con un ID de ataque (según OWASP Top Ten), ID de regla, descripción del ataque, Nivel de impacto (CVSS), Host afectado, fecha-hora, navegador y dirección IP del atacante.

Se puede aplicar filtros para realizar seguimiento específico por tipo de ataque.




## Administración de Reglas

Las reglas de seguridad pueden ser activas/desactivadas por el administrador del WAF, así como su notificación automática vía correo electrónico (SMTP/SSL). a las direcciones parametrizadas por el administrador.

CosimWAF trae configurado por defecto una serie de reglas según el OWASP top ten y el Requisito 6.6 del estándar de seguridad de datos PCI-DSS.

## Reporte Técnico por Ataque

El reporte técnico incluye todo el log detallado del ataque mencionado anteriormente, asimismo, puede exportarse en formato PDF con el logo de la entidad como parte de la cabecera del reporte generado para efectos de auditoría.


## Gráfica de Ataques Detectados

Consiste en una gráfica estadística generada automáticamente por CosimWAF sobre la cantidad de ataques clasificados según su tipo:

* SQL Injection
* XSS reflejado
* Escaners de Vulnerabilidades
* Errores de Configuración
* Intentos de Defacement
* Directory Traversal

*Gestione cuentas de usuarios (Administrador u Operador WAF) con sus respectivos perfiles.*

*Cobramos una tarifa plana en función de tu plan. Cosim no factura por picos de ancho de banda.*

*"El volumen y la sofisticación de los ataques hace que mantenerse actualizado sobre los tipos de amenazas de seguridad y las medidas de protección sea un desafío para los administradores de aplicaciones y equipos de seguridad. Con nuestra experiencia en la industria de Hacking Web, CosimWAF ofrece seguridad avanzada y rentable para las más recientes aplicaciones de Banca Web y Móvil"*

Luis Antonio Rosales
**Autor de CosimWAF**