UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES INSTITUTO DE POSTGRADO

TÍTULO
Modelo de mitigación OWASP Top 10 mediante Web Application Firewall optimizado, aplicado a los servicios productivos de DISPROVEF

AUTOR
Apunte Caspi, John Jairo

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR
Oviedo Bayas, Byron Wladimir

Santa Elena, Ecuador
Año 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
BYRON WLADIMIR OVIEDO BAYAS

Ing. Byron Oviedo Bayas, Ph.D.
TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALFREDO RAMON TUMBACO REYES

Ing. Alfredo Tumbaco Reyes, Mgtr.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
HENRY OMAR CRUZ CARRILLO

Ing. Henry Cruz Carrillo, Ph.D.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **APUNTE CASPI JOHN JAIRO**, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
BYRON WLADIMIR
OVIEDO BAYAS

Ing. Byron Wladimir Oviedo Bayas, Ph.D.

Santa Elena, 23 de junio del 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **APUNTE CASPI JOHN JAIRO**

DECLARO QUE:

El trabajo de Titulación, **MODELO DE MITIGACIÓN OWASP TOP 10 MEDIANTE WEB APPLICATION FIREWALL OPTIMIZADO, APLICADO A LOS SERVICIOS PRODUCTIVOS DE DISPROVEF**, previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 23 de junio del 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JOHN JAIRO APUNTE CASPI

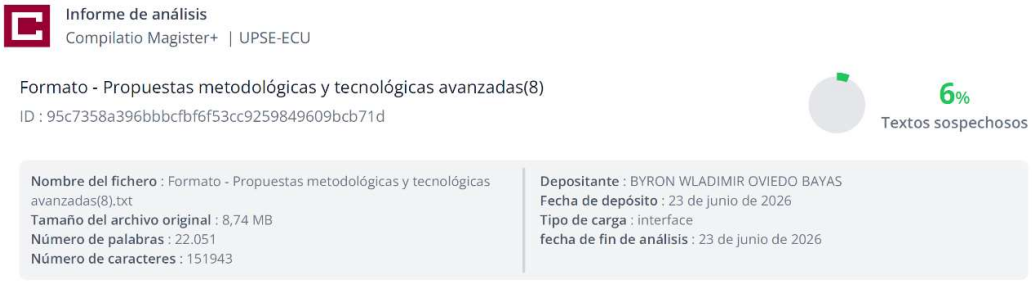
Apunte Caspi John Jairo

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **MODELO DE MITIGACIÓN OWASP TOP 10 MEDIANTE WEB APPLICATION FIREWALL OPTIMIZADO, APLICADO A LOS SERVICIOS PRODUCTIVOS DE DISPROVEF**, presentado por el estudiante, **APUNTE CASPI JOHN JAIRO** fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



Informe de análisis
Compilatio Magister+ | UPSE-ECU

Formato - Propuestas metodológicas y tecnológicas avanzadas(8)
ID : 95c7358a396bbbcfbf6f53cc9259849609bcb71d

6%
Textos sospechosos

Nombre del fichero : Formato - Propuestas metodológicas y tecnológicas avanzadas(8).txt
Tamaño del archivo original : 8,74 MB
Número de palabras : 22.051
Número de caracteres : 151943

Depositante : BYRON WLADIMIR OVIEDO BAYAS
Fecha de depósito : 23 de junio de 2026
Tipo de carga : interface
fecha de fin de análisis : 23 de junio de 2026

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
BYRON WLADIMIR OVIEDO BAYAS

Ing. Byron Wladimir Oviedo Bayas, Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **APUNTE CASPI JOHN JAIRO**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de esta propuesta metodológica y tecnológica avanzada con fines de difusión pública, además apruebo la reproducción de esta propuesta metodológica y tecnológica avanzada dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, 23 de junio del 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JOHN JAIRO APUNTE CASPI

Apunte Caspi John Jairo

AGRADECIMIENTO

Expreso mi sincero agradecimiento a Dios por la fortaleza y constancia que me permitió culminar esta etapa académica. Agradezco profundamente a mi esposa, quien me ha acompañado durante todo el transcurso de este proceso. Su apoyo incondicional ha sido la base para seguir adelante y alcanzar este logro. Agradezco de manera especial a mi tutor, PhD. Byron Oviedo Bayas, por su apoyo y orientación durante el desarrollo de este proyecto.

Quiero hacer un reconocimiento a DISPROVEF por abrirme las puertas y darme la oportunidad de seguir adelante y a su equipo de TI por la colaboración brindada en el desarrollo de esta investigación.

John Jairo Apunte Caspi

DEDICATORIA

Dedico este trabajo a mi esposa, por su amor, paciencia y apoyo incondicional en cada etapa de este proceso. Su esfuerzo constante y su confianza en mí fueron la motivación necesaria para seguir adelante y culminar esta meta profesional.

A mi familia, por su respaldo permanente y por ser el fundamento que impulsa cada logro alcanzado.

John Jairo Apunte Caspi

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo del estudio fue implementar un modelo de mitigación de vulnerabilidades OWASP Top 10 mediante un Web Application Firewall (WAF) optimizado en los servicios productivos de DISPROVEF. La investigación se apoyó en datos cuantitativos extraídos directamente del tráfico real de los servicios expuestos a Internet. Cada solicitud fue inspeccionada por el WAF y generó un evento medible, clasificable y comparable. Se aplicó un diseño cuasi-experimental pretest–postest para evaluar los resultados de las fases: aprendizaje, ajuste y protección. Uno de los principales logros fue la reducción del 78,40% en la clasificación de eventos del OWASP Top 10 descartando falsos positivos entre las fases de aprendizaje y ajuste del modelo. En la fase de protección el WAF contuvo el 15,97% del tráfico por presentar comportamiento anómalo y permitió el 84,03 % restante sin generar ningún tipo de degradación de los servicios. Se concluyó que el modelo constituyó una solución eficaz para fortalecer la seguridad de la capa de aplicación en entornos productivos.

Palabras claves: *OWASP Top 10, Web Application Firewall, ciberseguridad.*

ABSTRACT

The aim of this study was to implement a vulnerability mitigation model for the OWASP Top 10 using an optimized Web Application Firewall (WAF) within DISPROVEF's production services. The research was grounded in quantitative data drawn directly from real traffic on internet-exposed services, where each request was inspected by the WAF and generated a measurable, classifiable, and comparable event. A quasi-experimental pretest–posttest design was applied to evaluate the outcomes across three phases: learning, tuning, and protection.

One of the key achievements was a 78.40% reduction in OWASP Top 10 event classifications after discarding false positives between the learning and tuning phases. During the protection phase, the model flagged and contained 15.97% of the traffic due to anomalous behavior, while allowing the remaining 84.03% to pass through without causing any service degradation whatsoever.

It was concluded that the model proved to be an effective solution for strengthening application-layer security in production environments.

Keywords: OWASP Top 10, Web Application Firewall, cybersecurity.

INTRODUCCIÓN

La creciente dependencia de aplicaciones y servicios accesibles desde Internet ha ampliado la superficie susceptible de ataques de las organizaciones y ha incrementado la explotación de vulnerabilidades como mecanismo de acceso inicial. El reporte de investigaciones de brechas de seguridad del 2025 determinó que la explotación de vulnerabilidades representó el 20% de los vectores iniciales de acceso identificados en las brechas analizadas, lo que evidenció un crecimiento sostenido de este mecanismo de intrusión (Verizon, 2025). Esta tendencia se intensificó durante 2025, período en el que la explotación de vulnerabilidades se convirtió en el principal vector de ataque y estuvo presente en el 40% de los incidentes observados por IBM X-Force (IBM, 2026). Estos resultados reflejan una realidad conocida y que ocurre cada día: los servicios expuestos son un imán para los atacantes, especialmente cuando carecen de controles a nivel de aplicación (WAF) lo que incrementa el riesgo de exposición en caso de tener fallas de autenticación, control de acceso, configuraciones inseguras o componentes vulnerables.

La transformación digital ha ampliado la superficie de ataque de las organizaciones al incrementar su dependencia de aplicaciones web, convirtiendo la exposición a Internet en un factor crítico de riesgo frente a vulnerabilidades identificadas en el marco OWASP Top 10 (Alaoui & Nfaoui, 2022). En organizaciones como DISPROVEF, cuyos servicios de misión crítica son publicados mediante firewalls tradicionales sin capacidades avanzadas de inspección en la capa de aplicación, esta situación incrementa la probabilidad de explotación, evidenciando la necesidad de implementar estrategias de defensa especializadas (Baviskar et al., 2025).

El modelo de mitigación constituye el eje central de la investigación y se enmarca como un conjunto integrado de controles, políticas de seguridad y procedimientos

orientados a reducir la probabilidad de explotación de vulnerabilidades y limitar su impacto potencial sobre los activos digitales (Tadavarti & Babu, 2024). Por lo tanto a diferencia de remediar, lo que implicaría cambios directamente al código fuente de una determinada aplicación o sistema, El modelo actúa como un mecanismo compensatorio y adaptable permitiendo adicionar controles para minimizar el riesgo de manera continua mediante la inspección profunda y el filtrado del tráfico en tiempo real, esta característica permite fortalecer la capacidad de respuesta frente a amenazas en la capa de aplicación, contribuyendo a la protección de los servicios expuestos sin alterar la operación.

En Latinoamérica, las pequeñas y medianas empresas (PYMEs) enfrentan dificultades para implementar controles de seguridad que realmente corresponda a su nivel de exposición en Internet. Muchas de estas empresas no cuentan con personal especializado en ciberseguridad y operan con presupuestos ajustados, esto conlleva en muchos casos a usar configuraciones por defecto. Como consecuencia es muy común encontrar servicios críticos expuestos a Internet sin controles de inspección profunda del tráfico ni validaciones en la capa de aplicación. Esta realidad incrementa la probabilidad de explotación de vulnerabilidades asociadas a fallos de control de acceso, inyección de código, configuraciones inseguras y deficiencias en los mecanismos de autenticación, lo que evidencia la necesidad de implementar soluciones de protección especializadas como los Web Application Firewall (WAF) en estos entornos (Baviskar et al., 2025).

En este escenario se enmarca DISPROVEF, empresa ecuatoriana dedicada a la importación y distribución de insumos, medicamentos y equipos veterinarios, cuya operación diaria depende de múltiples servicios web productivos. Plataformas como el sistema administrativo y comercial, el repositorio documental, el correo institucional, la

gestión de soporte interno y la administración de dispositivos móviles se encuentran expuestas a Internet y resultan fundamentales para garantizar la continuidad operativa del negocio. No obstante, dichos servicios son publicados actualmente mediante un firewall tradicional, sin capacidades avanzadas de inspección semántica del tráfico HTTP/HTTPS, lo que incrementa la superficie de riesgo frente a vulnerabilidades OWASP Top 10.

Los WAF son herramientas diseñadas para mitigar este tipo de amenazas, la eficacia de este tipo de soluciones depende en cómo son configurados, ajustados y la precisión con el comportamiento real de las aplicaciones que son protegidas. Adoptar un WAF con configuraciones genéricas o limitarse a firmas estáticas no solo compromete la reducción real del riesgo, sino que en otros casos puede derivar en bloqueos indebidos que afecten negativamente a la operación de los negocios. La literatura técnica advierte que los sistemas tradicionales, al operar bajo configuraciones genéricas o firmas estáticas, suelen presentar una frecuencia elevada de falsos positivos, lo que puede derivar en la interrupción de tráfico legítimo y afectar significativamente la disponibilidad de los servicios (Baviskar et al., 2025). En este contexto, se vuelve necesario contar con un modelo metodológico que permita traducir las recomendaciones del OWASP Top 10 en configuraciones técnicas optimizadas, aplicables y sostenibles en entornos productivos reales, incorporando mecanismos de aprendizaje que ajusten dinámicamente las políticas de seguridad (Tadavarti & Babu, 2024).

Los servicios web expuestos a internet reciben todo tipo de tráfico, desde conexiones legitimas de usuarios pertenecientes a la organización hasta conexiones malintencionadas que buscan una brecha de seguridad para llegar afectar un servicio o

inyectar código malicioso. Por lo cual es necesario mecanismos que puedan analizar todo el tráfico en busca de comportamientos anómalos. Los modelos de mitigación proporcionan una salida practica reduciendo la superficie de exposición por medio de controles técnicos que analizan cada solicitud y la clasifican basado en comportamiento para determinar si puede ser enviado hacia los recursos internos o si este debe ser filtrado en el perímetro. Su verdadera utilidad está en que aprenden y se ajustan con el tiempo. Mientras que la remediación definitiva corrige el fallo directamente en el código fuente, el modelo de mitigación no elimina la vulnerabilidad, sino que funciona como una barrera compensatoria y adaptativa. Este esquema permite gestionar el riesgo en tiempo real mediante la inspección profunda y el filtrado de tráfico, traduciendo marcos de referencia internacionales en configuraciones técnicas ejecutables en entornos productivos

El enfoque adoptado es de carácter aplicado y se desarrolla directamente sobre la infraestructura en operación, permitiendo evaluar la eficacia del modelo en condiciones reales de uso, sin comprometer la disponibilidad ni la estabilidad de los sistemas críticos.

La mayoría de las guías de ciberseguridad inclusive el propio OWASP top 10 están escritas asumiendo que quien las implementa cuenta con una formación especializada, tiempo y un equipo dedicado. La realidad de muchas empresas latinoamericanas es distinta ya que la seguridad recae en una o dos personas que además de esto también son las encargadas de administrar los servidores de las principales plataformas CORE del negocio, conectividad, soporte técnico, asistencia de incidencias entre otros. DISPROVEF representa un caso donde la dependencia de los servicios web forma parte de la operación diaria del negocio, pero carece de un modelo de mitigación ajustado a su infraestructura y aplicaciones.

El aporte del estudio no está en proponer un modelo más, sino en haberlo validado en condiciones reales, partiendo de un modelo metodológico y tecnológico orientado a mejorar protección de organizaciones que dependen de servicios web para la operación de sus actividades. El objetivo no fue diseñar un modelo desde cero, sino integrar dos piezas que suelen tratarse por separado: el marco de riesgos OWASP Top 10 y un Web Application Firewall en un esquema metodológico y técnico que pudiera ser operado con los recursos humanos y tecnológicos existentes. Los resultados obtenidos permiten establecer criterios técnicos y operativos que pueden ser considerados por otras empresas de características similares al momento de implementar mecanismos de mitigación frente a amenazas dirigidas a aplicaciones web.

El trabajo se organiza en 3 capítulos, El primer capítulo establece los fundamentos teóricos y el marco OWASP Top 10, identificando los supuestos técnicos que dificultan su aplicación en entornos limitados. El segundo capítulo describe la metodología que fue aplicada, el diseño de la investigación y su aplicación, así como los métodos, técnicas e instrumentos que fueron utilizados para la recolección y análisis de la información. Finalmente, el tercer capítulo presenta los resultados obtenidos, la discusión correspondiente y la propuesta metodológica y tecnológica validada, concluyendo con las conclusiones y recomendaciones derivadas del estudio.

Planteamiento de la investigación

La operación diaria de DISPROVEF depende de múltiples servicios web productivos que son fundamentales para sostener sus procesos administrativos, logísticos y técnicos. No obstante, estos sistemas operan actualmente mediante firewalls tradicionales sin capacidades avanzadas de inspección semántica en la capa de aplicación,

lo que incrementa la superficie de exposición frente a amenazas asociadas a las vulnerabilidades identificadas en el marco OWASP Top 10.

En DISPROVEF se evidenció que los controles existentes no cubrían adecuadamente las necesidades de inspección y filtrado del tráfico entrante, por lo cual las solicitudes maliciosas recibidas podían llegar directamente a los servidores que soportaban la operación del servicio. En DISPROVEF se evidenció que los controles existentes no cubrían adecuadamente las necesidades de inspección y filtrado del tráfico entrante, por lo cual las solicitudes maliciosas podían llegar directamente a los servidores que soportaban la operación de los servicios. Esta condición incrementaba el riesgo de explotación de vulnerabilidades relacionadas con fallas de control de acceso, inyección, configuraciones inseguras y otros riesgos contemplados en el marco OWASP Top 10, con posibles consecuencias sobre la confidencialidad, integridad y disponibilidad de la información.

En organizaciones con recursos limitados, donde no siempre es posible corregir de inmediato las vulnerabilidades identificadas, esta situación aumenta la exposición a incidentes que pueden afectar tanto la continuidad de los sistemas como la información que estos procesan. Frente a este escenario surgió la necesidad de diseñar e implementar un modelo de mitigación basado en un Web Application Firewall que actuara como una barrera intermedia para inspeccionar y filtrar el tráfico malicioso antes de que alcanzara los servidores reales.

El modelo propuesto utiliza el WAF como un punto de inspección del tráfico HTTP/HTTPS entre internet y los servicios publicados con la capacidad de detectar y bloquear solicitudes maliciosas antes de que lleguen a los servidores reales además

funciona como un control compensatorio para reducir la probabilidad de explotación de vulnerabilidades del TOP 10 de OWASP sin realizar cambios directamente en las aplicaciones o servicios.

Formulación del problema de investigación

¿De qué manera la aplicación de un modelo de WAF optimizado mediante fases de aprendizaje y ajuste técnico reduce los eventos de seguridad asociados a vulnerabilidades OWASP Top 10 en los servicios web críticos de DISPROVEF, y qué nivel de eficacia de mitigación alcanza sin comprometer la continuidad operativa?

Objetivo general:

Implementar un modelo de mitigación de vulnerabilidades OWASP Top 10 mediante un Web Application Firewall configurado de manera optimizada, aplicado a los servicios productivos expuestos a Internet de DISPROVEF, con el fin de fortalecer su seguridad y garantizar la continuidad operativa.

Objetivos específicos:

- Identificar las vulnerabilidades del marco OWASP Top 10 presentes o potenciales en los servicios productivos de DISPROVEF, considerando su nivel de exposición y criticidad operativa.
- Configurar y desplegar una implementación piloto del Web Application Firewall, estableciendo parámetros de aprendizaje y criterios para su optimización progresiva en un entorno productivo.

- Evaluar el impacto del modelo propuesto mediante la comparación del nivel de exposición antes y después de la implementación, analizando la eficacia de mitigación y la estabilidad operativa.
- Establecer lineamientos técnicos y operativos que permitan la replicación, mantenimiento y sostenibilidad del modelo en organizaciones con infraestructura similar.

Planteamiento hipotético

Configurar de forma optimizada un Web Application Firewall, dentro de un modelo de mitigación ejecutado diversas fases disminuirá la exposición de los servicios productivos de DISPROVEF a las vulnerabilidades del OWASP Top 10 sin afectar la eficacia ni la continuidad operativa.

Hipótesis de investigación

(H_1) La implementación de un modelo de mitigación basado en un Web Application Firewall permitirá, mediante el afinamiento técnico de sus firmas y la personalización de sus reglas de seguridad, reducir significativamente la exposición a vulnerabilidades OWASP Top 10 en los servicios productivos de DISPROVEF, sin afectar negativamente la continuidad operativa ni el desempeño de los sistemas.

(H_0) La implementación del modelo de mitigación basado en Web Application Firewall no produce una reducción significativa en el nivel de exposición a vulnerabilidades OWASP Top 10 en los servicios de DISPROVEF, o genera una degradación significativa en su continuidad operativa.

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

1.1 Revisión de literatura

La protección de aplicaciones web expuestas a Internet ha sido ampliamente abordada en la literatura científica reciente, especialmente en el contexto del incremento sostenido de ataques dirigidos a la capa de aplicación. ENISA (2021), en su informe "Ciberseguridad para las pymes: retos y recomendaciones" tuvo como objetivo analizar las principales amenazas que enfrentan las pequeñas y medianas empresas europeas. Advirtiendo que las organizaciones enfrentan un panorama crítico donde la gran mayoría de las intrusiones exitosas aprovechan debilidades de seguridad ya documentadas. La investigación subraya que la vulnerabilidad no reside únicamente en la falta de herramientas, sino en la carencia de controles específicos en la capa de aplicación (Capa 7), factor que facilita la explotación de servicios web en empresas con recursos técnicos limitados.

OWASP Foundation (2021), en el documento "OWASP Top 10: Los diez riesgos de seguridad más críticos en aplicaciones web" presentó una actualización del marco de vulnerabilidades más relevantes a nivel global. OWASP es uno de los marcos de referencia para clasificar riesgos de seguridad en aplicaciones basados en dos criterios: frecuencia de explotación y su impacto. Entre ellas, los problemas relacionados con la inyección de código y las fallas en el control de acceso continúan ocupando posiciones relevantes debido a su frecuencia de explotación y a las consecuencias que pueden generar sobre los sistemas afectados. En consecuencia, se vuelve imperativo adoptar mecanismos de mitigación activa que permitan interceptar estas solicitudes maliciosas antes de que alcancen la infraestructura interna de la organización.

Román-Gallego, López y Ramírez (2023), en el artículo científico “Firewall de aplicaciones web con inteligencia artificial para la detección avanzada de ataques de inyección web” tuvieron como objetivo evaluar la eficacia de modelos de WAF basados en inteligencia artificial para la detección de ataques de inyección. Bajo un enfoque experimental el autor contrasto la eficacia de los modelos tradicionales contra los modelos que hacen uso de aprendizaje automático. El análisis se centró en tres indicadores: tasa de detección, tasa de falsos positivos y latencia obteniendo como resultado mejoras superiores al 30 % en la detección de ataques, aunque con un incremento significativo en la complejidad operativa implicando intervención frecuente para el ajuste de los parámetros, lo que limita su adopción en PYMEs.

Alotaibi y Vassilakis (2023), en “Hacia un firewall de aplicaciones web basado en SDN” evaluaron como optimizar la respuesta de WAF frente a ataques de inyección SQL en arquitecturas basadas en redes definidas por software. El estudio se desarrolló mediante simulaciones y pruebas controladas, utilizando tráfico sintético y real. El procesamiento de datos se centró en la adaptabilidad dinámica de políticas y tiempos de respuesta. Como conclusión, los autores destacan que la efectividad del WAF depende menos de la tecnología subyacente y más de la capacidad de ajuste de las políticas según el comportamiento del tráfico.

Cárdenas Rosero, Guevara Vega y Landeta-López (2025), en la tesis “Protección de sitios web: una evaluación del firewall de aplicaciones web” analizaron la efectividad de los WAF en entornos empresariales de Latinoamérica. Su trabajo midió la reducción de exposición de riesgos tras la aplicación de políticas ajustadas combinando el análisis cuantitativo de eventos de seguridad con evaluación cualitativa de estabilidad operativa,

Sus hallazgos respaldan la necesidad de optimizar correctamente las políticas de seguridad de los WAF para reducir la exposición a ataques de una organización.

Notoma (2025) en la tesis “Un enfoque integral para la gestión de riesgos de ciberseguridad y el cumplimiento normativo en la nube: recomendaciones para el desarrollo de un marco fácil de usar para pequeñas empresas” señala que las pequeñas y medianas empresas (PYMEs) constituyen el 99% del tejido empresarial mundial y sufren del 43 % de los ciberataques, esta desprotección no es aislada deriva directamente de la escasez de expertos en seguridad y de las marcadas restricciones presupuestarias de muchas organizaciones de este sector. En virtud de esta problemática, el autor sugiere un marco de gestión de riesgos que sea escalable y económico para entornos de nube, tras la validación empleada durante la investigación mostró una reducción del 38% de los incidentes y un retorno de inversión (ROI) en seguridad del 200 % en el primer año. Bajo esta perspectiva, se justifica la urgente necesidad de establecer controles técnicos sin exigir inversiones inmanejables permitiendo a las organizaciones más pequeñas mejorar su protección sin comprometer su viabilidad financiera.

Celik (2025) resalta en el reporte de industria de KuppingerCole que el mercado de Protección de Aplicaciones Web y APIs (WAAP) atraviesa una fase de expansión estratégica en América Latina donde la migración del WAF tradicional hacia modelos adaptativos está impulsada por la necesidad regional de enfrentar amenazas sofisticadas que afectan tanto infraestructuras tradicionales como a microservicios esto convierte a la región latinoamericana en un foco prioritario para la adopción de tecnologías WAAP con inteligencia de amenazas en tiempo real y automatización para salvaguardar la integridad de los activos digitales en ecosistemas empresariales distribuidos.

Altamirano Rodríguez et al. (2026) presentan a través de su investigación experimental la efectividad de implementaciones de soluciones Web Application Firewall (WAF) para detectar y mitigar ataques dirigidos a API REST a través de un ambiente controlado realizado en Quito, Ecuador, el estudio empleó el uso de herramientas comerciales en nube y de código abierto implementados localmente (*on-premise*) esto permitió tener una respuesta adecuada frente a diferentes tipos de ataques, Los resultados mostraron mejora en la efectividad del WAF cuando las reglas o firmas de seguridad son ajustadas en base a las características del ambiente y de la aplicación que será protegida actuando como un control de seguridad adicionales. Esta investigación aporta evidencia obtenida en Ecuador y respalda la utilización de modelos de protección como el propuesto para DISPROVEF, relacionando la protección de APIs con la resiliencia operativa del negocio.

Sameh y Selim (2024) proponen un WAF adaptativo de doble capa (ADL-WAF) basado en aprendizaje automático para resolver las limitaciones de los sistemas tradicionales basados en firmas. De acuerdo con los autores la integración de algoritmos de *Machine Learning* permitió alcanzar un 99,83% de precisión en la detección de amenazas en entornos reales, logrando la reducción significativa de falsos positivos a cero al combinar capas de detección de anomalías y amenazas específicas. Estos resultados sugieren que las optimizaciones tecnológicas efectuadas en los equipos de seguridad perimetral como el WAF resulta determinante para la eficiencia operativa de las PYMEs en Latinoamérica, permitiendo una mitigación automatizada y precisa, disminuyendo gradualmente la carga operativa de trabajo de los equipos de seguridad de las compañías

que de por sí ya gestionan grandes volúmenes de tráfico legítimo evitando de esta manera que lleguen a saturarse.

La integración de estos referentes bibliográficos, proporciona una base técnica y regional sólida para el desarrollo del modelo propuesto. Los estudios revisados aportan evidencia obtenida en entornos empresariales respaldando el uso de mecanismos de protección como el WAF para el aseguramiento de aplicaciones que por operación de negocio deben estar expuestos a internet. Es importante mencionar que métricas de retorno de inversión (ROI) en PYMEs y los avances en precisión y detección de falsos positivos mediante aprendizaje automático refuerzan la necesidad de implementar un modelo de mitigación ajustado a las condiciones operativas de DISPROVEF. La literatura analizada confirma que la protección proactiva en la capa de aplicación es la estrategia más viable y efectiva para salvaguardar el patrimonio digital de las organizaciones en el ecosistema empresarial latinoamericano actual.

1.2 Desarrollo teórico y conceptual

La ciberseguridad en entornos empresariales modernos se ha convertido en un componente esencial para la sostenibilidad operativa de las organizaciones que dependen de servicios digitales. A medida que los procesos administrativos, logísticos y comerciales se digitalizan, las aplicaciones web quedan más expuestas y se vuelven blanco frecuente de obre todo en empresas medianas donde los controles de seguridad no evolucionan al mismo ritmo que la dependencia tecnológica por eso la ciberseguridad no puede limitarse al perímetro: tiene que abarcar la prevención, detección y mitigación de amenazas dirigidas a las aplicaciones y a los datos que manejan.

Este planteamiento coincide con lo que organismos como ENISA (2023) denominan resiliencia digital, no la ausencia de incidentes, sino la capacidad de detectarlos y mitigarlos antes de que comprometan los servicios para lo cual se establecen una combinación de controles técnicos, procesos operativos y monitoreo continuo para mantener un fortalecimiento perimetral robusto. El modelo propuesto integra tres componentes que ENISA identifica como necesarios: el ASM de F5 como control técnico, la revisión manual de reglas como proceso operativo, y los logs del WAF como mecanismo de monitoreo continuo.

En este marco el Top 10 de la OWASP sirve de referencia para identificar riesgos de seguridad en las aplicaciones web en lugar de imponer soluciones específicas, ofrece una clasificación de las vulnerabilidades basada en datos estadísticos de incidencia e impacto recolectados a nivel global para guiar a la toma de decisiones en términos de seguridad. Entre ellas destacan problemas relacionados con la inyección de código, las fallas en el control de acceso y las configuraciones inseguras, cuya presencia puede comprometer la confidencialidad, integridad y disponibilidad de los sistemas.

Los firewalls tradicionales operan en las capas de red o transporte mientras que el WAF proporciona controles específicos en la capa de aplicación permitiendo un análisis profundo del tráfico HTTP/HTTPS para identificar comportamientos maliciosos (Baviskar et al., 2025). El firewall de aplicaciones web (WAF) funciona como un proxy reverso que inspecciona cada solicitud antes de que alcance la infraestructura backend (Durmuşkaya & Bayraklı, 2025). En DISPROVEF, esa es precisamente la función del F5 BIG-IP Advanced WAF (ASM) para fortalecer el nivel de seguridad de las aplicaciones expuestas. Esta capacidad lo convierte en una herramienta idónea para traducir los riesgos

identificados por OWASP en controles operativos concretos. No obstante, su efectividad depende de la correcta configuración y del ajuste continuo de sus políticas.

Los parámetros más relevantes que analiza el WAF de F5 dentro de cada solicitud son los siguientes:

1. Encabezados HTTP

   User-Agent: detecta bots o herramientas automatizadas.

   Host: verifica que la solicitud esté dirigida al dominio correcto.

   Referer: identifica si la solicitud proviene de una fuente legítima.

   Content-Type: valida que el tipo de contenido sea el esperado (ej. application/json, text/html).

2. Métodos HTTP

   GET, POST, PUT, DELETE, etc.

   El WAF puede bloquear métodos no permitidos o sospechosos.

3. Cadenas de consulta (Query Strings)

   Parámetros en la URL como ?id=123&action=edit

   Se validan contra patrones de inyección SQL, XSS, etc.

4. Cuerpo de la solicitud (Payload)

   En solicitudes POST o PUT, el WAF analiza el contenido enviado.

   Detecta inyecciones, scripts maliciosos, datos binarios no esperados.

5. Cookies

   Verifica que las cookies no estén manipuladas o contengan datos maliciosos.

   Protege contra ataques como session hijacking o cookie poisoning.

6. Parámetros personalizados

Campos de formularios como username, password, email, etc.

Se validan contra reglas de formato, longitud, codificación y contenido.

7. Dirección IP y geolocalización

Puede bloquear IPs de mala reputación o regiones específicas.

Se usa para aplicar políticas de acceso geográfico.

8. Tasa de solicitudes (Rate Limiting)

Número de solicitudes por segundo (RPS/TPS).

Detecta patrones de abuso o ataques DoS.

9. Tamaño de la solicitud

Solicitudes excesivamente grandes pueden ser bloqueadas.

Previene ataques de buffer overflow o payloads maliciosos.

El proceso de optimización del WAF se ejecutó mediante una metodología iterativa que comprendió el aprendizaje, la calibración y la validación técnica. En la etapa inicial, se configuró el sistema para monitorear el tráfico legítimo, lo que permitió establecer una línea base de las operaciones normales en los servicios de DISPROVEF. En la segunda etapa las políticas generadas automáticamente se revisaron de forma manual para desactivar aquellas que producían falsos positivos sobre el tráfico real reforzando la seguridad de las aplicaciones sin afectar la disponibilidad de los servicios ni la experiencia de los usuarios.

El modelo de mitigación propuesto combina tres componentes: El OWASP Top 10 utilizado para identificar y priorizar los riesgos de seguridad más relevantes, aplicación

de controles técnicos a través de un WAF encargado de inspeccionar y filtrar el tráfico dirigido a las aplicaciones web y la validación empírica en un entorno productivo real. Esta articulación permite construir un modelo replicable, alineado tanto con las buenas prácticas internacionales como con las limitaciones operativas propias de organizaciones como DISPROVEF.

1.3 OWASP Top 10

El OWASP Top 10 constituye un referente internacional para la identificación y priorización de riesgos en aplicaciones web. La versión 2021 reorganiza las categorías con base en datos empíricos recopilados globalmente, integrando frecuencia, impacto y explotabilidad de vulnerabilidades.

Tabla 1

Principales categorías del OWASP Top 10

Código	Categoría	Descripción resumida
A01	Broken Access Control	Fallas en restricciones de acceso a recursos
A02	Cryptographic Failures	Exposición de datos por uso inadecuado de criptografía
A03	Injection	Inserción de comandos o consultas maliciosas
A04	Insecure Design	Deficiencias estructurales en el diseño de seguridad
A05	Security Misconfiguration	Configuración insegura de componentes
A06	Vulnerable and Outdated Components	Uso de componentes desactualizados o vulnerables

A07	Identification and Authentication Failures	Fallas en autenticación e identidad
A08	Software and Data Integrity Failures	Alteraciones en procesos o integridad de datos
A09	Security Logging and Monitoring Failures	Insuficiente registro y monitoreo
A10	Server-Side Request Forgery (SSRF)	Solicitudes forzadas desde el servidor hacia recursos internos

Nota. Adaptado de *"OWASP Top 10: los diez riesgos de seguridad más críticos para las aplicaciones web"* (OWASP Foundation, 2021).

CAPÍTULO 2. METODOLOGÍA

2.1 Contexto de la investigación

La presente investigación se desarrolló en una empresa privada ecuatoriana dedicada a la importación, distribución y comercialización de insumos veterinarios, cuya operación dependía de manera crítica de servicios web utilizados en procesos administrativos, logísticos y técnicos. La organización mantenía presencia operativa en distintas regiones del país, lo que demandaba una infraestructura tecnológica centralizada capaz de soportar múltiples sedes y garantizar la disponibilidad continua de sus sistemas.

Los servicios web estaban desplegados en la infraestructura on-premise de DISPROVEF accesible para usuarios internos y externos a través de Internet dejando a las aplicaciones vulnerables los vectores de ataque contempladas dentro del OWASP Top 10. Dentro la arquitectura perimetral existía un firewall este solo brindaba protección en las capas 3 y 4 del modelo OSI realizando únicamente filtrado básico de puertos y direcciones IP además de carecer de una inspección profunda de los paquetes. Se implementó un F5 BIG IP VE con su módulo se seguridad ASM sobre alternativas de código abierto (*open source*) como ModSecurity o Coraza para suplir esta exposición dado que el mismo fue incorporado dentro del flujo de comunicación como un proxy evitando grandes cambios a nivel de arquitectura de manera que pueda inspeccionar el tráfico y aumentar los niveles de control. Esta decisión se fundamentó en tres pilares estratégicos para la infraestructura de DISPROVEF:

1. Capacidad de aprendizaje dinámico: A diferencia de las reglas estáticas que caracterizan a las soluciones abiertas, F5 integra un motor de Learning Mode que permite construir políticas de seguridad positiva basadas en el comportamiento real y dinámico de las aplicaciones protegidas.

2. Administración unificada: F5 en su consola de administración permite gestionar los módulos ASM y LTM, reduciendo la necesidad de gestionar herramientas independientes y favorece una operación más eficiente, especialmente en organizaciones como las PYMEs que disponen de recursos humanos y presupuestos limitados para actividades de ciberseguridad.
3. Soporte Técnico especializado: A diferencia de las alternativas de código abierto evaluadas ModSecurity y Coraza, la plataforma F5 BIG-IP cuenta con respaldo directo del fabricante, procedimientos de actualización y documentación técnica publicada. Más allá de la disponibilidad de asistencia ante incidencias, el soporte especializado contribuye a reducir los riesgos asociados a actualizaciones de firmas, incompatibilidades entre componentes de la infraestructura o falsos positivos que requieran análisis y corrección, situaciones que podrían afectar la protección de los servicios si debieran resolverse exclusivamente con recursos internos

En este contexto, se implementó un Web Application Firewall (WAF) F5 BIG-IP en modalidad virtual (VE), integrado a la infraestructura tecnológica existente y desplegado dentro de una zona desmilitarizada (DMZ) con el objetivo de centralizar la inspección del tráfico antes de su llegada a los servicios backend. Esta arquitectura permite realizar análisis en la capa de aplicación, incluyendo la inspección de solicitudes HTTP/HTTPS, la detección de patrones maliciosos y la mitigación de amenazas comunes, complementando las capacidades de los firewalls tradicionales que operan en capas inferiores (F5, 2026). Se configuró el WAF como punto de inspección de tráfico

HTTP/HTTPS dirigido a los servicios productivos de DISPROVEF permitiendo analizar, clasificar y gestionar cada una de las solicitudes recibidas.

El modelo se desarrolló durante el primer trimestre del 2026 (1 enero hasta 31 marzo), donde se implementó el modelo en tres fases: aprendizaje, ajuste y protección. Este enfoque permitió evaluar de manera progresiva el comportamiento del sistema, optimizar las políticas de seguridad para la reducción de falsos positivos y habilitar mecanismos de mitigación activa mediante el bloqueo de eventos identificados como maliciosos.

En este sentido, el contexto de la investigación se caracterizó por la intervención directa sobre una infraestructura productiva real, con servicios web expuestos a internet y tráfico operativo genuino, lo que constituyó un escenario idóneo para la implementación, evaluación y validación empírica del modelo de mitigación en la capa de aplicación propuesto en el presente estudio.

2.1.1 Procedimiento de revisión y selección de fuentes (PRISMA)

La revisión de literatura que sustentó el marco teórico y técnico de la investigación se realizó mediante un procedimiento estructurado de identificación, selección y depuración de fuentes, basado en los lineamientos de la declaración PRISMA. Este procedimiento permitió asegurar la rigurosidad metodológica en la selección de fuentes académicas y técnicas relacionadas con seguridad de aplicaciones web, OWASP y Web Application Firewalls.

El proceso se desarrolló en cuatro fases: Primero la fase de identificación donde se recopilaron fuentes de libros académicos, artículos científicos, tesis de posgrado y documentación técnica en seguridad de aplicaciones web. El cribado eliminó duplicados,

fuentes no alineadas con el tema mediante revisión de títulos, resúmenes y palabras clave. Los documentos que superaron ese filtro pasaron a la fase de elegibilidad donde se leyeron completamente para evaluar su rigor técnico, vigencia y alineación con el top 10 de OWASP y soluciones basadas en WAF. En la fase de inclusión solo se conservaron aquellos con fundamentos teóricos, técnicos o evidencia relevante para el modelo de mitigación propuesto para DISPROVEF.

Este proceso conformó una base depurada de fuentes que sirvió de apoyo para la construcción del marco teórico, el diseño del modelo de mitigación y la interpretación de los resultados.

Tabla 2

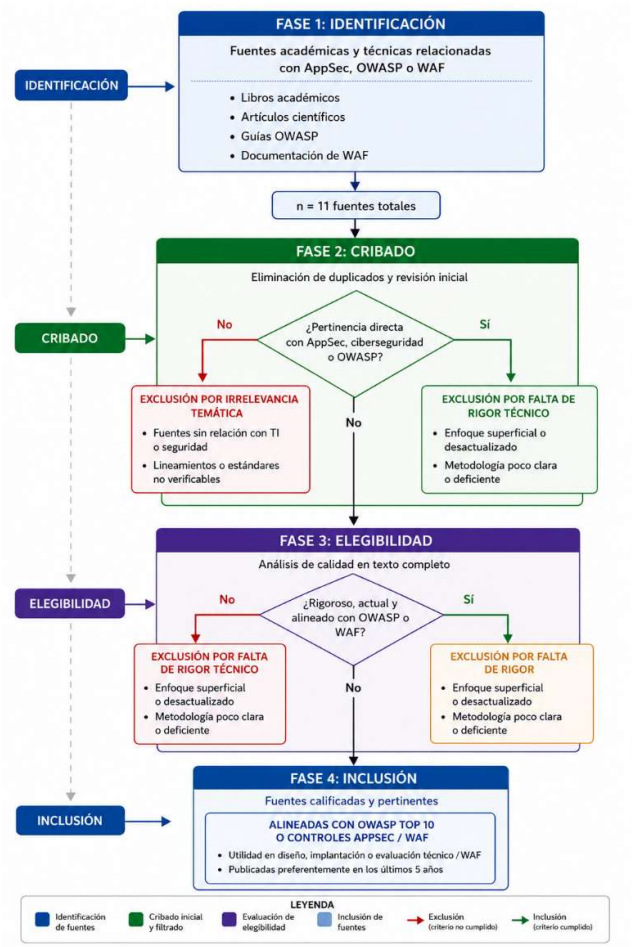
Síntesis de aportes técnicos de la revisión de literatura más relevantes

Recurso	Contenido
Arévalo Ipiales (2024)	• Implementación de WAF sobre Rocky Linux con Nginx y ModSecurity.• Aplicación del OWASP Core Rule Set (CRS) como mecanismo de defensa proactiva.• Mitigación de vulnerabilidades de capa 7 como SQL Injection y XSS.• Uso de registros de auditoría para análisis de tráfico y comportamiento.• Validación de seguridad mediante pruebas de penetración con Kali Linux.
Macías Mendoza et al. (2025)	Construye un laboratorio replicable con VirtualBox y Docker, aplicando OWASP ZAP y Burp Suite para identificar y validar vulnerabilidades antes y después de las mitigaciones. • Aplica buenas prácticas de desarrollo seguro: parametrización de consultas, validación de entradas, cabeceras HTTP de endurecimiento, control de CORS y manejo seguro de errores. • Parametrización de consultas, validación de entradas, cabeceras HTTP endurecidas, control de CORS y manejo seguro de errores. • Observa una reducción promedio del 67,3% en el nivel de riesgo y la eliminación de hallazgos críticos, evidenciando la eficiencia de la integración de seguridades en el SSDLC.
Gamboa Safla (2023)	• Emplea herramientas que facilitan la ejecución de pruebas de penetración en aplicaciones web. • Implementa métodos orientados a resolución y mitigación de vulnerabilidades. • Utiliza guías de prueba de ataques a sitios web, basadas en herramientas de código abierto. • Ofrece diferentes perspectivas para el análisis de vulnerabilidades en entornos web basados en OWASP.

Álava Zambrano et al. (2022)	• Define la seguridad informática como el área encargada de proponer reglas, procedimientos, métodos y técnicas para garantizar que el sistema de información sea seguro • Presenta la tabla de los 10 riesgos de seguridad OWASP Top 10 2021 • Documenta casos reales de empresas afectadas por estas vulnerabilidades • Concluye que OWASP apuesta por implementar la seguridad desde cero, que las vulnerabilidades representan amenazas potenciales cuyo nivel de riesgo varía según su tipo.
Cárdenas Rosero et al. (2025)	• Evalúa que tan efectivo es un WAF utilizando la metodología OWASP para determinar si puede detectar y mitigar con éxito los ataques en el servidor web de la Universidad Técnica del Norte. • Define a OWASP como una de las guías más completas para analizar vulnerabilidades en aplicaciones web y se enfoca en localizar, clasificar y abordar las deficiencias de seguridad • Implementa una capa adicional de seguridad en el servidor web y categoriza los principales tipos de ataques detectados por el WAF. • Determina la eficacia del firewall mediante pruebas de penetración OWASP además del uso de la herramienta OWASP ZAP como escáner de vulnerabilidades
Cárdenas Rosero (2023)	• Fundamenta que la Guía de Pruebas de OWASP (WSTG) es la metodología más completa para pruebas de penetración en aplicaciones web, seguida de ISSAF, OSSTMM, PTES y NIST SP 800-115. • Implementa el WAF de Fortinet (FortiWeb) resguardando diversos sitios críticos del campus universitario. • Recomienda fortalecer el recurso humano en el área de seguridad informática con al menos 2 profesionales especializados. • Identifica al personal gran parte del personal operativo no está familiarizado con los controles mínimos de seguridad por lo que es necesario efectuar capacitaciones constantes.
Shaheed & Kurdy (2022)	• Diseño de WAF basado en aprendizaje automático. • Extracción de características para detección de ataques web.• Uso de Naive Bayes y SVM con precisión de hasta 99,6%.• Análisis de URL, payload y cabeceras HTTP.

Figura 1

Criterios de selección de fuentes (PRISMA)



Nota. La figura muestra el proceso de identificación, cribado, elegibilidad e inclusión de fuentes para la revisión de literatura, aplicado al contexto de seguridad de aplicaciones web, OWASP y WAF. Elaboración propia, basada en la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) (Page et al., 2021).

2.2 Diseño y alcance de la investigación

Esta investigación se planteó como un estudio aplicado y un diseño cuasiexperimental sin grupo de control sobre la infraestructura productiva de DISPROVEF para atender un problema de seguridad en la capa de aplicación. El análisis

se realizó en condiciones reales de operación recibiendo tráfico de clientes y usuarios en los diferentes servicios sin tener manipulación de variables externas ni en un entorno aislado dado que el negocio carece del mismo.

Metodológicamente se utilizó un esquema comparativo de tipo pretest–postest, este diseño permitió contrastar el comportamiento del sistema antes y después de implementar el WAF, tomando como parte crucial del análisis cada uno de los eventos registrados por la herramienta cuando los usuarios realizaban un consumo a los servicios expuestos de manera que se pueda evaluar el impacto de la intervención tecnológica en un entorno productivo activo. Además, se incorporó una dimensión longitudinal ya que el modelo se desplegó mediante las fases de aprendizaje, ajuste y protección y su evolución a lo largo del tiempo. A través de estas etapas se observó la evolución del sistema desde un escenario inicial de monitoreo del tráfico hasta la aplicación progresiva de mitigación activa basados en políticas de seguridad optimizadas.

El análisis de la información combinó enfoques descriptivo, analítico y comparativo, el descriptivo fue útil para definir el estado inicial de la arquitectura, los servicios web y el comportamiento del tráfico durante la fase de aprendizaje. El analítico se aplicó sobre los eventos capturados por el WAF, examinando severidad, recurrencia y patrones usando como base las categorías del OWASP Top 10. Como punto final el comparativo permitió medir la evolución entre fases evidenciando la reducción de eventos alertados, la precisión de detección y la contención mediante la activación del modo de bloqueo.

En cuanto al alcance comprendió el diseño e implementación de una zona desmilitarizada (DMZ), la integración del WAF F5 BIG-IP VE dentro de la arquitectura

existente, listado de los principales servicios, parámetros sensibles y el ajuste paulatino de las políticas de protección. También incluyo el análisis comparativo de resultados y se elaboró la documentación técnica de referencia para la administración de la solución.

La validación se enfocó en la capacidad de detección y respuesta del WAF frente al tráfico productivo real por este motivo no se ejecutaron pruebas de penetración ofensivas posteriores a la implementación. En un entorno como DISPROVEF donde los servicios web son críticos para la operación diaria y no existe infraestructura redundante de respaldo, someter la plataforma a ejercicios de explotación controlada habría introducido un riesgo innecesario de indisponibilidad o degradación de los servicios. En su lugar, la eficacia se validó mediante el análisis exhaustivo de registros (*logs*) y el contraste cuantitativo de eventos en las fases de ajuste y protección.

2.3 Tipo y métodos de investigación

La investigación se clasificó como aplicada, dado que su propósito fue abordar un problema real de seguridad en la capa de aplicación dentro del entorno tecnológico de DISPROVEF, mediante la implementación, ajuste y evaluación de un modelo OWASP–WAF en condiciones operativas reales. Trabajar sobre el tráfico productivo de DISPROVEF implicó que los resultados reflejaran las condiciones reales de uso de los servicios, con sus picos, sus patrones y sus restricciones operativas.

Se adoptó un enfoque mixto combinando dos perspectivas: cualitativas y cuantitativos. La cualitativa se centró en el comportamiento de los servicios web, patrones de uso, los eventos registrados por el WAF y las incidencias detectadas durante el proceso de ajuste de políticas, esto permitió entender de mejor manera los eventos y su relación con el funcionamiento de las aplicaciones. Por su parte el cuantitativo midió alertas

generadas, tráfico permitido, eventos bloqueados y ocurrencia de falsos positivos registradas por el WAF, estas métricas permitieron evaluar la efectividad y precisión del modelo durante las fases de aprendizaje, ajuste y protección.

El análisis de los datos utilizo métodos de investigación complementarios, el método descriptivo permitió establecer la línea base y el comportamiento inicial del sistema. Este método de análisis se centró tanto en los registros creados por el WAF como en los patrones encontrados durante la investigación, las comparaciones realizadas entre las distintas etapas ayudaron a entender la evolución de los eventos y los cambios obtenidos a medida que se aplicaban gradualmente las políticas de protección. El ajuste progresivo de las políticas de seguridad mediante el método inductivo-operacional se basó en la observación del tráfico real, creando un modelo alineado con las condiciones operativas de DISPROVEF.

2.4 Población y muestra

La población de estudio estuvo constituida por los servicios web productivos que DISPROVEF mantuvo expuestos a internet durante el período de ejecución de la investigación. Estos servicios formaban parte de los procesos administrativos, logísticos y técnicos de la organización, requerían alta disponibilidad y representaban la superficie real de exposición a riesgos en la capa de aplicación.

El análisis comprendió la totalidad de los servicios identificados, correspondientes a las aplicaciones Nextcloud, Zimbra, Zlibra ERP, Soporte y Athena MDM, las cuales fueron publicadas a través de la zona desmilitarizada (DMZ) implementada por la organización e inspeccionadas mediante un Web Application Firewall (WAF) durante la ejecución del modelo OWASP–WAF.

La muestra se definió mediante un enfoque censal técnico y estuvo constituida por la totalidad de los eventos de seguridad generados por el tráfico HTTP/HTTPS dirigido hacia los servicios web analizados durante el período comprendido entre el 1 de enero y el 31 de marzo de 2026 donde se registraron 12.846 eventos durante la fase de aprendizaje y 2.775 eventos en la fase de protección.

Trabajar con la totalidad del tráfico y no con una muestra fue una decisión práctica, no solo metodológica. En DISPROVEF, el tráfico HTTP/HTTPS variaba según la hora del día y el tipo de usuario, y algunos eventos relevantes como ciertos falsos positivos o intentos de inyección SQL espaciados en el tiempo ocurrían con baja frecuencia. Un muestreo probabilístico podría haberlos omitido, dejando fuera del ajuste de políticas precisamente los casos que más interesaba capturar.

Bajo esta perspectiva evaluativa, el análisis integral de los eventos permitió que la optimización del modelo OWASP–WAF se sustentara en la observación efectiva del comportamiento operativo del entorno analizado y no únicamente en aproximaciones estadísticas parciales. Este criterio favoreció la trazabilidad integral del comportamiento del sistema y fortaleció la consistencia técnica de los ajustes aplicados sobre las firmas y reglas de mitigación implementadas en la infraestructura de DISPROVEF.

Se analizaron todos los eventos registrados a partir de la inspección del tráfico HTTP/HTTPS generado por el WAF sobre los publicados en la DMZ, fueron y utilizados la clasificación de alertas el tráfico permitido y los eventos bloqueados durante las fases de aprendizaje, ajuste y protección.

2.5 Técnicas e instrumentos de recolección de datos

La recolección de datos se realizó durante el proceso de implementación, ajuste y puesta en protección del Web Application Firewall (WAF) F5 BIG-IP VE, el cual inspeccionó el tráfico real generado por los clientes hacia los diferentes servicios web productivos de DISPROVEF dentro de la red DMZ. A medida que el WAF entró en operación, se generaron registros detallados relacionados con patrones de uso, solicitudes anómalas, violaciones OWASP, coincidencias de firmas y comportamientos que requirieron intervención técnica. Esta información constituyó la base para el análisis del comportamiento de las aplicaciones y para el ajuste progresivo de las políticas de seguridad, garantizando que la protección aplicada no afectara la continuidad operativa de los servicios críticos. Para la recopilación de información se emplearon las siguientes técnicas:

a) Observación directa del comportamiento del WAF, esta técnica consistió en el monitoreo continuo del procesamiento de solicitudes entrantes hacia los servicios web. Las alertas se observaron en tiempo real con el panel de monitoreo del WAF así como tendencias de tráfico y métricas, esta información se usó para determinar patrones de uso, las solicitudes y comportamientos anormales que hacían necesario ajustar las políticas de seguridad.

b) Análisis técnico de registros (logs), los logs del WAF ofrecieron un análisis de las solicitudes y un resumen de los eventos de seguridad y los clasifico en niveles de riesgo según OWASP top 10.

Cada evento se examinó según su severidad, el origen del tráfico, los métodos HTTP empleados y los parámetros enviados permitiendo separar el tráfico legítimo de

los falsos positivos y de solicitudes potencialmente maliciosas. A partir de estos registros fue posible identificar patrones de comportamiento, intentos de explotación y anomalías que alimentaron la correlación de eventos y el análisis de incidentes durante las tres fases del modelo. Asimismo, el uso de mecanismos de registro robustos fortaleció la trazabilidad de las actividades detectadas, constituyendo un elemento clave para el análisis forense y la respuesta ante incidentes en entornos productivos (Abu Laila et al., 2026; Fortinet, 2025).

c) Validación funcional con el equipo de TI, después de cada ajuste aplicado a las políticas del WAF, se realizó una validación funcional conjunta con el personal de TI de DISPROVEF para confirmar que no hubieran existido novedades u afectación de servicios además de verificar flujos de trabajo como: autenticación, acceso a plataformas, carga de documentos y consultas operativas en las aplicaciones protegidas.

d) Comparación por fases operativas, se documentó el comportamiento del tráfico web en tres etapas: antes de la implementación del WAF, durante la fase de aprendizaje y tras la activación de la política optimizada. Esta técnica permitió identificar la evolución de las violaciones OWASP, los cambios en el volumen de alertas y la estabilidad alcanzada por los servicios luego de los ajustes aplicados.

Los instrumentos utilizados incluyeron los registros de eventos de seguridad del WAF (Application Security Events), el panel de monitoreo con métricas en tiempo real, una bitácora técnica de ajustes donde se documentaron cronológicamente las modificaciones realizadas, y un checklist de validación operativa elaborado con base en la documentación del fabricante y buenas prácticas de seguridad. Asimismo, se

emplearon revisiones técnicas conjuntas con el personal de DISPROVEF para validar comportamientos específicos y excepciones necesarias.

2.6 Matriz de operacionalización de variables

Con el propósito de garantizar coherencia entre el marco teórico, las técnicas de recolección y el análisis empírico, se elaboró una matriz de operacionalización de variables. Esta matriz permitió desagregar las variables de estudio en dimensiones e indicadores medibles, asegurando trazabilidad entre los objetivos específicos y los datos obtenidos a partir de los registros del WAF.

Tabla 3

Matriz de operacionalización de variables

Variable	Dimensión	Indicador	Técnica	Instrumento
Implementación del modelo OWASP–WAF	Configuración y ajuste de políticas	Nivel de personalización de reglas	Observación directa	Panel de monitoreo WAF
Eficacia de mitigación	Reducción de amenazas	Disminución porcentual de violaciones OWASP	Análisis de logs	Application Security Events
Eficacia de mitigación	Precisión de detección	Número de falsos positivos identificados	Análisis técnico	Registros de eventos
Eficacia operativa	Continuidad del servicio	Incidentes funcionales posteriores a ajustes	Validación funcional	Checklist operativo

Nota. La tabla presenta la matriz de operacionalización de variables utilizada para relacionar las variables de estudio con sus dimensiones, indicadores, técnicas e instrumentos de recolección de datos.

2.7 Criterios de clasificación de eventos OWASP

La clasificación de los eventos de seguridad detectados por el Web Application Firewall se realizó tomando como referencia las categorías establecidas en el OWASP Top 10 (2021). No obstante, para efectos del análisis empírico se operacionalizaron únicamente aquellas tipologías efectivamente observadas en los registros del entorno productivo de DISPROVEF, garantizando coherencia entre el marco conceptual y los datos recolectados.

Tabla 4

Clasificación operativa de eventos detectados por el WAF

Categoría OWASP 2021	Tipo específico detectado en logs	Nivel de severidad	Acción configurada en WAF	Uso en el análisis
A01: Fallo en el control de acceso	Intentos de acceso a recursos restringidos	Crítico / Alto	Bloqueo	Cálculo de reducción de accesos indebidos
A03: Inyección	Inyección SQL / Comandos	Crítico	Bloqueo	Medición de mitigación efectiva
A05: Configuración de seguridad incorrecta	Acceso a rutas administrativas expuestas	Alto	Bloqueo / Alerta	Evaluación de endurecimiento

A07: Fallas de identificación y autenticación.	Intentos de fuerza bruta	Alto / Medio	Limite de rango / Alerta	Análisis de patrones anómalos
A10: SSRF	Solicitudes internas no autorizadas	Crítico	Bloqueo	Evaluación de protección perimetral
A03 / A05	Cross-Site Scripting (XSS)	Alto / Medio	Bloqueo / Alerta	Reducción de violaciones OWASP

Nota. La tabla presenta la clasificación adaptada de los eventos de seguridad detectados por el WAF en función de las categorías del OWASP Top 10 (OWASP Foundation, 2021).

La Tabla 4 recoge la clasificación operativa de los eventos y facilitar su interpretación técnica, Para complementarla, se presentan a continuación ejemplos de logs y payloads representativos de las categorías del OWASP Top 10. Estos ejemplos muestran las clases de peticiones y tendencias que el cortafuegos de aplicaciones web puede reconocer durante la revisión del tráfico, permitiendo comprender de manera práctica los criterios utilizados para la detección, clasificación y análisis de los eventos registrados.

Tabla 5

Ejemplos representativos de eventos clasificados por categoría OWASP

Categoría OWASP 2021	**Tipo específico detectado en logs**	**Ejemplo representativo de log o payload**
A01: Fallo en el control de acceso	Intentos de acceso a recursos restringidos	Intento de acceso a recursos protegidos sin autorización. “ GET /admin/users HTTP/1.1”
A03: Inyección	Inyección SQL / Comandos	Expresión usada para intentos de manipulación de consultas mediante inyección de código malicioso. “ id=1' OR '1'='1”
A05: Configuración de seguridad incorrecta	Acceso a rutas administrativas expuestas	GET /phpmyadmin/ → Exploración de rutas administrativas utilizada en procesos de reconocimiento y enumeración de servicios..
A07: Fallas de identificación y autenticación.	Intentos de fuerza bruta	Múltiples solicitudes POST hacia los portales con un /login desde un mismo origen.
A10: SSRF	Solicitudes internas no autorizadas	Prueba de acceso a recursos internos o metadatos mediante redirección url=http://169.254.169.254/latest/meta-data/
A03 / A05	Cross-Site Scripting (XSS)	<script>alert('XSS')</script> → Inserción de código JavaScript en parámetros de entrada con el objetivo

	de ejecutar contenido no autorizado en el navegador del usuario.

Nota. Los ejemplos mostrados ilustran patrones de tráfico y payloads utilizados para la clasificación de eventos de seguridad por parte del WAF, no corresponden a información sensible del entorno productivo.

2.8 Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información.

Los eventos generados durante el análisis del tráfico de DISPROVEF fueron organizados según su severidad, riesgo en base al OWASP y tipo de respuesta del WAF (alerta, permitido o bloqueado) permitiendo evaluar la efectividad y nivel de mitigación alcanzado por el modelo tras el afinamiento de las políticas de control.

2.9 Procesamiento de datos

Una vez implementadas las políticas de seguridad del WAF sobre los servicios web de DISPROVEF, arrancó un proceso iterativo de ajuste con el objetivo de bajar los falsos positivos sin tocar la operación de las aplicaciones. Inicialmente, las aplicaciones fueron publicadas bajo la protección del WAF en modo de aprendizaje y monitoreo, dejando que la plataforma registrara eventos bajo condiciones normales de uso. Periódicamente se revisaban las alertas acumuladas para separar las que respondían a amenazas reales de las que disparaba el tráfico legítimo. Cada hallazgo fue validado conjuntamente con el personal responsable de los servicios y en función de eso se decidía si correspondía ajustar una firma o abrir una excepción. Después de cada modificación además de su registro en bitácora se realizaron pruebas funcionales para verificar que las aplicaciones mantuvieran su funcionamiento esperado. Este proceso se repitió hasta

obtener una política optimizada que redujera los falsos positivos sin comprometer la capacidad de detección ni la continuidad de los servicios.

Uno de los factores clave dentro del desarrollo del modelo fue el análisis y procesamiento de los registros de eventos generados por el firewall (logs) ya que fue el principal insumo en cada una de las fases del modelo: aprendizaje, ajuste y protección permitiendo la detección/descarte de falsos positivos y el afinamiento de reglas de control como resultado de esto se logró: una disminución de eventos que fue cuantificable a través de las métricas de eventos, efectividad del modelo en base al etiquetado de las respuestas (permitido, alertado, bloqueado), análisis del tráfico bajo políticas de seguridad optimizadas y su comportamiento.

El análisis se centró en cuatro aspectos: reducción de eventos recurrentes, identificación y tratamiento de falsos positivos, estabilidad operativa tras los ajustes y comportamiento del tráfico bajo las políticas configuradas.

Se definió como unidad de medición los eventos registrados por el WAF durante la inspección del tráfico HTTP/HTTPS con el propósito de garantizar la trazabilidad cuantitativa del análisis. Como se trabajó con un enfoque censal no se aplicaron técnicas de muestreo ya que se analizó la totalidad de los eventos generados en cada fase, durante la fase de aprendizaje en la que no se aplicaron acciones de bloqueo, se registraron 12.846 eventos de seguridad.

En la fase de protección se registró un total de 2.775 eventos, incluyendo tráfico permitido, alertado y bloqueado bajo políticas optimizadas. Este enfoque corresponde a un análisis censal técnico, dado que se consideró la totalidad de los eventos generados en

el entorno productivo, garantizando la representatividad completa del comportamiento del sistema y la consistencia del análisis comparativo entre fases.

2.9.1 Análisis estadístico

El análisis cuantitativo de la eficacia del modelo se realizó mediante estadística descriptiva comparando las frecuencias absolutas y relativas de los eventos registrados por el ASM de F5 en cada fase permitiendo comparar la evolución de alertas, eventos bloqueados y tráfico permitido conforme se incorporaban las políticas de seguridad. La reducción porcentual de la exposición a vulnerabilidades OWASP se calculó mediante la siguiente expresión:

$$Reducción\ (\%)\ =\ \left(\frac{Einicial - Efinal}{Einicial}\right)\ \times\ 100$$

Donde:

- $E_{inicial}$ número de eventos registrados en la fase de aprendizaje (12.846)
- E_{final} número de eventos registrados en la fase de protección (2.775)

Sustituyendo los valores obtenidos:

$$Reducción\ (\%)\ =\ \left(\frac{12.846 - 2.775}{12.846}\right)\ \times\ 100 = 78{,}40\%$$

Este procedimiento permitió cuantificar la mejora relativa en la capacidad de mitigación del sistema, evidenciando una reducción significativa en la exposición a vulnerabilidades de capa de aplicación bajo condiciones operativas reales.

2.10 Validez de los instrumentos

La validez de los instrumentos se sustentó en la correspondencia entre los datos recopilados y los objetivos de la investigación, considerando que los eventos de seguridad registrados reflejan el comportamiento real del tráfico en los servicios web productivos

de DISPROVEF. Los criterios de análisis se basaron en las categorías de riesgo definidas por OWASP Top 10 (2021), en las guías técnicas del fabricante F5 Networks y en buenas prácticas de seguridad en aplicaciones web. Se evaluó la validez de contenido ‘mediante el método de juicio de expertos donde se contó con la participación de cuatro (4) especialistas con experiencia en implementación de controles de seguridad en capa de aplicación y ciberseguridad. Para este proceso se entregó a los expertos un conjunto estructurado de instrumentos del estudio (Anexo A) donde se incluyó: la matriz de operacionalización de variables, checklist de validación operativa y criterios de clasificación de eventos OWASP además de la ficha de evaluación para la valoración técnica y coherencia metodológica.

Se utilizo una escala ordinal de cuatro niveles (1 = deficiente, 4 = excelente), las calificaciones obtenidas fueron promediadas y posteriormente expresadas como porcentaje del valor máximo posible. El promedio global fue 3,75 sobre 4 equivalente al 93,75%, por encima del umbral mínimo de aceptación del 80% establecido para la aceptación de los instrumentos. Las fichas de validación y observaciones técnicas se presentan en los anexos correspondientes.

De forma complementaria, se realizaron revisiones técnicas con el personal de TI de DISPROVEF, con el propósito de verificar que los eventos registrados correspondieran a situaciones reales de operación y que las políticas aplicadas mantuvieran la funcionalidad de los servicios sin generar afectaciones en su desempeño.

2.11 Confiabilidad de los instrumentos

Esta investigación se fundamenta en el análisis de registros generados por el Web Application Firewall (WAF) vistos desde un enfoque técnico-operativo considerando el

tipo de instrumentos empleados y la naturaleza de los datos a diferencia de lo que ocurre en investigaciones con encuestas o escalas de percepción donde se aplican coeficientes de consistencia interna como el Alfa de Cronbach

En este contexto, la confiabilidad no se evaluó mediante métodos estadísticos tradicionales de consistencia interna, debido a que los instrumentos no corresponden a mediciones subjetivas, sino a eventos técnicos generados automáticamente durante la inspección del tráfico HTTP/HTTPS en un entorno productivo real. A continuación de detallan los para la evaluación de confiabilidad de los datos:

a) Trazabilidad de eventos: Todos los registros incluyen fecha y hora (timestamps) para facilitar el seguimiento de eventos verificando su secuencia cronológica a fin de contrastarlo con cada fase del modelo.
b) Integridad de la información: Cada una de las conexiones recibidas por el WAF generan eventos únicos (Support ID) permitiendo su análisis individual.
c) Capacidad de verificación: Permite replicar eventos a partir de los eventos recolectados, los mismos eventos pueden volver a analizarse utilizando los mismos criterios y obtener resultados consistentes.
d) Estabilidad del sistema de medición: Clasificación de eventos según las categorías del OWASP Top 10 manteniendo condiciones operativas similares a lo largo de las tres fases.

Se uso un análisis de concordancia inter-observador como complemento a los criterios anteriores para la clasificación de eventos donde se seleccionó de forma intencional una muestra intencional de 50 eventos que cubrían todas las categorías

operativas definidas en el estudio: 28 falsos positivos, 13 casos de tráfico benigno atípico y 9 eventos potencialmente maliciosos (Tabla 6) de manera que la validación de la confiabilidad contemple el tráfico claramente malicioso como las solicitudes legítimas complejas que suelen generar ambigüedad técnica.

Tabla 6

Matriz de concordancia inter-observador

Clasificación Analista A / Analista B	Falso positivo	Benigno atípico	Potencialmente malicioso	Total
Falso positivo	26	2	0	28
Benigno atípico	3	9	1	13
Potencialmente malicioso	0	2	7	9
Total	29	13	8	50

Nota. La tabla presenta matriz de resultados de los 50 eventos.

A continuación, se describe el proceso efectuado para la evaluación de la confiabilidad de la clasificación de los eventos realizada por los dos analistas técnicos sobre la muestra de 50 eventos:

1. Cálculo del Acuerdo Observado (P_0): Representa la proporción de casos en los que ambos analistas coincidieron.

$$P_0 = \frac{Total\ de\ acuerdos}{Total\ de\ eventos} = \frac{26 + 9 + 7}{50} = \frac{42}{50} = 0{,}8400$$

2. Cálculo del Acuerdo Esperado (P_e)

$$P_e = \frac{(28 \times 29) + (13 \times 13) + (9 \times 8)}{50^2} = \frac{812 + 169 + 72}{2500}$$

$$P_e = \frac{1053}{2500} = 0{,}4212$$

3. Aplicación de la fórmula de Kappa (κ)

$$Kappa = \frac{P_0 - P_e}{1 - P_e} = \frac{0{,}84 - 0{,}4212}{1 - 0{,}4212}$$

$$Kappa = \frac{0{,}4188}{0{,}5788} = 0{,}7235$$

Sobre los 50 eventos evaluados se identificaron 42 coincidencias equivalente a un acuerdo observado del 84%. El análisis de concordancia mediante el coeficiente Kappa de Cohen arrojó un valor de $\kappa = 0{,}7235$ asociado a un nivel de acuerdo sustancial lo que evidencia consistencia en el proceso de clasificación y respalda la confiabilidad de los instrumentos.

La muestra de eventos utilizada se presenta en el Anexo C y se incluyen extractos representativos de los registros analizados. Es importante mencionar que se contó con una participación activa del equipo de TI de DISPROVEF quienes efectuaron validaciones de servicios y descartaron problemas o degradación de los servicios posterior al afinamiento de las políticas de control WAF en el F5. Considerando todos los criterios aplicados los instrumentos demostraron un alto nivel de confiabilidad técnica, comparable al de estudios empíricos basados en monitoreo automatizado y análisis de eventos de seguridad en entornos reales.

2.12 Consideraciones éticas y de datos

La presente investigación se desarrolla dentro de la infraestructura tecnológica de DISPROVEF y se orienta estrictamente a fortalecer la seguridad de sus servicios web mediante la implementación, ajuste y validación operativa de un Web Application

Firewall (WAF). Por ello, se mantiene un cumplimiento riguroso de los principios éticos, legales y de protección de datos vigentes en el Ecuador.

El análisis se limitó a los registros técnicos generados por el ASM tales como violaciones OWASP, patrones de tráfico, coincidencias de firmas y solicitudes clasificadas como anómalas. Los logs contienen metadatos con todo tipo de información crucial para la inspección de seguridad sin dejar de lado la confidencialidad de los datos sin exponer contenido de documentos, correos, archivos, credenciales ni información asociada a usuarios internos o externos.

La criticidad de los servicios de DISPROVEF fue la prioridad en todo momento por ello no se ejecutaron ataques ofensivos, pruebas destructivas, accesos no autorizados ni actividades que puedan comprometer la disponibilidad, integridad o confidencialidad de los sistemas centrándonos en la mejora de los controles existentes y los nuevos propuestos por el modelo. Por ello previo a cada ajuste realizado en las políticas del WAF se revisó en conjunto con el equipo de tecnología a fin de no interferir con la ejecución de procesos del negocio.

Desde el punto de vista legal, el estudio se alinea con el marco normativo ecuatoriano. El Código Orgánico Integral Penal (COIP) sanciona una serie de actividades relacionadas con el acceso no autorizado, manipulación o interferencia en sistemas informáticos. Entre ellas destacan:

- **Artículo 229: Acceso no consentido a sistemas informáticos** sanciona el acceso o la interferencia sin autorización previa.

- **Artículo 230: Ataques a la integridad de sistemas informáticos** penaliza la alteración, destrucción o perturbación de sistemas, datos o servicios.
- **Artículo 231: Interceptación ilícita de datos** prohíbe obtener información sin consentimiento.
- **Artículo 232: Ataques a la disponibilidad** sanciona acciones que generen interrupciones o afectaciones operativas.

DISPROVEF autorizó expresamente el desarrollo del modelo (anexo F). A partir de ahí el trabajo se limitó a instalar y configurar el ASM de F5 como herramienta de protección en la capa de aplicación para el tráfico HTTP/HTTPS sin interferir en la operación de los sistemas incorporándolo a la arquitectura actual actuando como un escudo adicional en nivel de seguridad, este esquema implementado no modifico datos de las aplicaciones sino que más bien fue un intermediario centrándose solo en la inspección y control de tráfico mas no en la manipulación de la información propia de cada aplicación constituyendo una medida legítima y necesaria para la gestión de riesgos tecnológicos. El estudio se desarrolló conforme a los principios de ética profesional en ciberseguridad y a la normativa legal vigente en Ecuador y se trataron bajo criterios de confidencialidad, integridad y trazabilidad, con fines exclusivamente académicos y operativos, sin divulgación a terceros.

CAPÍTULO 3. RESULTADOS Y DISCUSIÓN

La implementación del modelo de mitigación en la arquitectura de DISPROVEF tuvo que cumplir una serie de prerrequisitos técnicos: infraestructura, red, seguridad, acceso administrativo y configuración básica del entorno para garantizar la correcta operación del WAF F5 BIG-IP VE, la estabilidad del tráfico y la continuidad de los servicios críticos.

a) Requerimientos de infraestructura

- Hipervisor: VMware ESXi o Hyper-V dado que se consideró para el modelo una máquina virtual F5 VE.
- **Recursos mínimos dedicados al WAF:** Infraestructura mínima necesaria para la correcta operación de la máquina virtual: 4 vCPU, 16 GB de memoria y 100GB de almacenamiento para logs y eventos. también es necesario contar con un direcciona de la red de administración aislada para acceso al portal de configuración (TMUI) y CLI.

b) Requerimientos de red y direccionamiento

- Subred DMZ: Debe contar con direccionamiento exclusivo para la inspección y publicación de servicios web.
- Direcciones IP internas para el enrutamiento entre WAF/servidores y direcciones IP públicas de los servicios publicados hacia internet.
- Enrutamiento: Permitir el reenvío del tráfico entrante hacia el WAF y de este hacia los servidores internos respetando rutas de retorno y NAT.

c) Requerimientos de seguridad

- Certificados SSL válidos para todos los servicios expuestos en formato PEM o PFX, habilitar TLS versión 1.2 o superior para negociación SSL entre cliente y F5.
- Políticas de firewall (reglas de acceso):
    - Redireccionar el tráfico entrante HTTP/HTTPS para las IP públicas de los servicios hacia la red DMZ gestionada por el WAF.
    - Comunicación interna WAF → Servidores (puertos 80, 443, 9095 y otros según el servicio) requerido para monitoreo de salud/estado de los servicios a ser expuestos.
- Red DMZ: el WAF debe quedar en un segmento lógico separado gestionado desde el firewall perimetral y garantizar que todo el tráfico se encamine hacia F5 cerrando todo tipo de bypass que intente saltear la protección.

d) Requerimientos del WAF

- Licenciamiento F5 activo y provisionamiento de los módulos LTM + ASM.
- configuración de Políticas base de inspección HTTP/HTTPS para la protección de tráfico web.
- Capacidad de operación en diferentes modos de operación aprendizaje (Learning Mode) o bloqueo (Blocking) para el afinamiento de las políticas de seguridad.

- Soporte para firmas de seguridad, parámetros, métodos HTTP, control de cabeceras y verificación de integridad para el afinamiento de las políticas en la fase de ajuste.
- Capacidad de almacenamiento y envió de logs de eventos ASM (Application Security Manager) necesarios para el análisis de incidentes.

e) Requerimientos de acceso administrativo

- Acceso seguro a la consola de administración a través del protocolo HTTPS (https://IP-mgmt:443) y SSH para el acceso por consola CLI.
- Capacidad de segregación de Roles de usuarios:
    - Administrador del WAF "Administrator"
    - Validador técnico para lectura y revisión de eventos "operator"
- Configuración de parámetros mínimos de complejidad de contraseñas, el sistema debe parametrizar controles específicos para longitud, y uso de caracteres especiales como numéricos obligatorios y vigencia de contraseñas.
- Registro de auditoría habilitado para acciones de configuración, se debe logear todos los cambios efectuados por todos los usuarios.

f) Requerimientos de soporte y operación

- Disponibilidad del equipo de TI en DISPROVEF para validaciones funcionales posteriores a los ajustes.
- Registro diario de eventos críticos durante la fase inicial.

- Procedimiento mínimo de respaldo de configuraciones.

3.1 Arquitectura actual y arquitectura propuesta

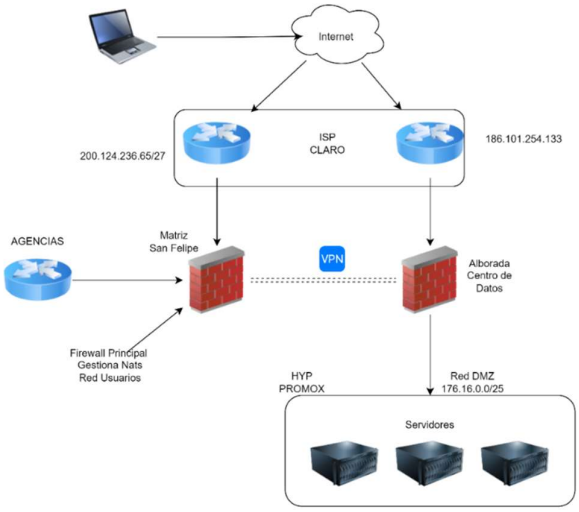
La arquitectura tecnológica involucrada en este proyecto se compone de dos estados claramente diferenciados: la arquitectura actual de publicación de servicios web utilizada por DISPROVEF y la arquitectura propuesta, en la cual se integra el Web Application Firewall (WAF) F5 BIG-IP VE como nueva capa de inspección y protección dentro de una DMZ dedicada. Esta sección describe de forma detallada ambos escenarios para contextualizar el funcionamiento previo y los cambios introducidos con la implementación del modelo OWASP–WAF.

3.2 Arquitectura actual

En el estado actual, los servicios web de DISPROVEF son expuestos directamente a Internet mediante reglas de firewall y NAT configuradas sobre el equipo perimetral (Mikrotik). Cada servicio Nextcloud, Zlibra ERP (Planificacion de recursos empresariales), Soporte, Zimbra y Athena MDM (Mobile Device Management) se publica desde su respectiva IP interna hacia una IP pública específica, permitiendo acceso directo desde el exterior sin un mecanismo avanzado de inspección de capa 7.

Figura 2

Diagrama de conectividad inicial de DISPROVEF



Nota. La figura muestra la arquitectura de red actual de DISPROVEF, en la que los servicios internos se encuentran conectados mediante infraestructura perimetral y un túnel VPN sitio a sitio, sin incorporar un mecanismo especializado de inspección en la capa de aplicación.

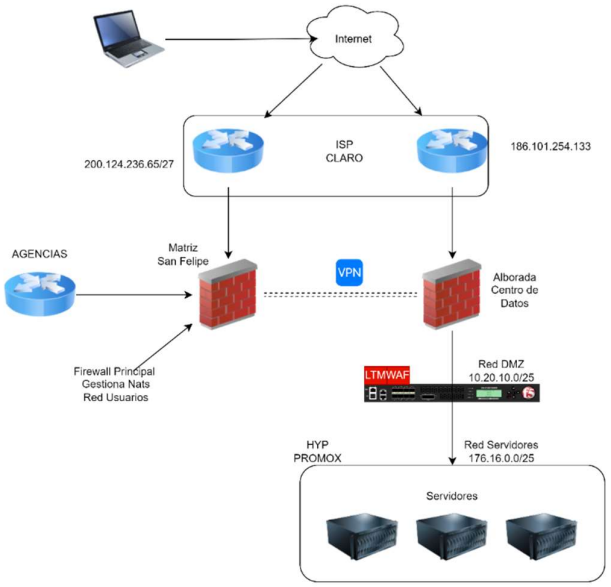
El tráfico entrante atraviesa únicamente el firewall perimetral, que realiza funciones básicas de filtrado y control de puertos, pero no ejecuta inspección profunda, verificación de parámetros HTTP, detección de prácticas OWASP ni validación dinámica del comportamiento de las solicitudes. Este diseño implica que cualquier solicitud HTTP/HTTPS llega directamente a los servidores internos, incrementando la exposición a amenazas como inyecciones, manipulación de cabeceras, desbordamientos, intentos de evasión, fuerza bruta, explotación de vulnerabilidades conocidas y otras categorías del OWASP Top 10

3.3 Arquitectura propuesta

La arquitectura propuesta introduce una DMZ especializada y un WAF F5 BIG-IP VE como punto central de inspección, protección y control de los servicios web expuestos. F5 BIG-IP opera bajo una arquitectura Full Proxy estableciendo sesiones independientes entre el cliente/f5 y F5/servidores por ende en la nueva arquitectura el tráfico que antes llegaba directamente hacia los servidores reales ahora pasa primero por el WAF el cual recibe el tráfico, lo inspecciona y decide si lo deja pasar hacia los servidores internos o lo bloquea en función de firmas, políticas OWASP, validaciones de parámetros, reputación, patrones anómalos y reglas adaptadas a cada servicio. Adicionalmente, gestiona certificados SSL, normaliza tráfico, protege contra ataques de inyección, identifica solicitudes manipuladas y bloquea comportamientos maliciosos sin afectar la continuidad operativa.

Figura 3

Arquitectura de red propuesta con implementación de WAF



Nota. Se incorpora el F5 BIG-IP (LTM + WAF) para la inspección y protección del tráfico hacia los servidores internos.

Cada servicio es redirigido por rutas hacia la DMZ, lo que permite que F5 pueda aplicar políticas de seguridad específicas para cada aplicación, de esta forma el WAF puede diferenciar parámetros propios de los servicios protegidos: ERP, flujos documentales de Nextcloud, sincronización de Zimbra, operaciones del soporte técnico y tráfico del MDM. Esto garantiza una adaptación precisa a las necesidades operativas de DISPROVEF.

La implementación del WAF no altera el direccionamiento interno de los servidores ni la estructura de las aplicaciones; únicamente modifica el punto de publicación, lo que facilita una integración controlada y sin interrupciones. Esta arquitectura estará acompañada por una imagen esquemática que representa el flujo de tráfico antes y después del WAF.

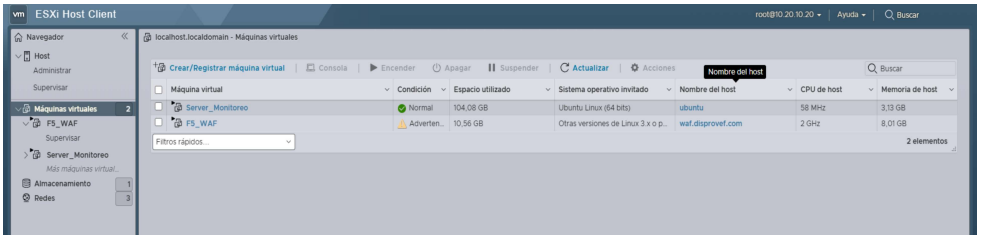
3.4 Fases metodológicas del despliegue del modelo OWASP–WAF

La implementación del modelo se desarrolló en cinco fases metodológicas progresivas que permitieron incorporar, ajustar y validar los mecanismos de protección sin afectar la operación normal de los servicios publicados de DISPROVEF.

Fase 1: Preparación y adecuación del entorno: En esta primera etapa se realizó la revisión completa del direccionamiento actual, la verificación de conectividad, la creación de la nueva DMZ (10.20.10.0/24) y la preparación del entorno de virtualización donde operará el WAF F5 [Esxi + F5 VE].

Figura 4

Entorno virtual y despliegue del F5 BIG-IP VE



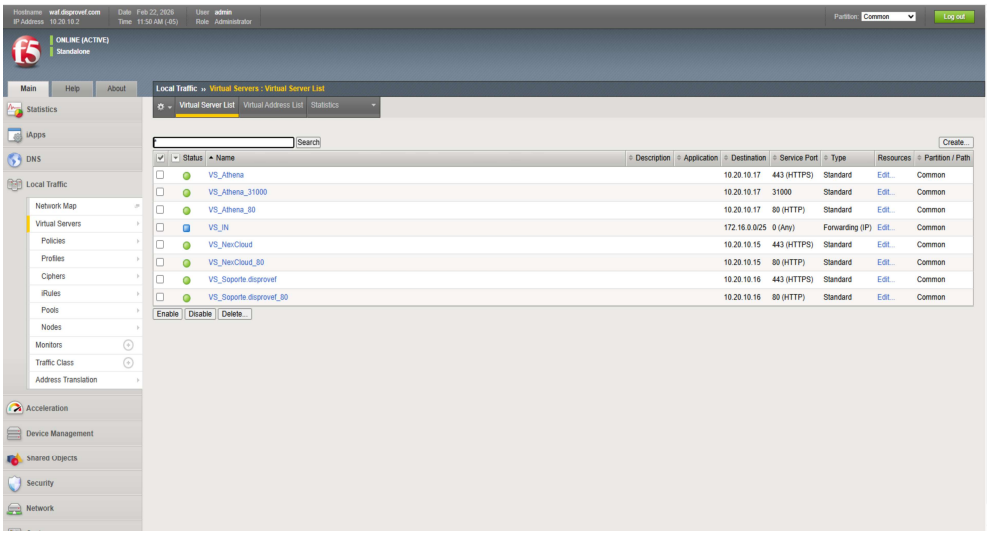
Nota. La figura muestra el entorno de virtualización donde se implementa el F5 BIG-IP VE como Web Application Firewall dentro de la arquitectura propuesta, permitiendo la inspección del tráfico antes de su llegada a los servicios internos.

Se definieron las rutas internas, los servicios que fueron publicados, los certificados SSL necesarios y las reglas mínimas de firewall requeridas para permitir el flujo de tráfico hacia el WAF. Asimismo, se estableció los accesos administrativos y se habilitaron los logs para asegurar trazabilidad durante todo el proceso.

Fase 2: Publicación inicial y modo de aprendizaje (Learning Mode): Una vez preparado el entorno, los servicios web de DISPROVEF se redirigieron hacia el WAF en modo de aprendizaje.

Figura 5

Virtual Servers configurados en F5 BIG-IP VE

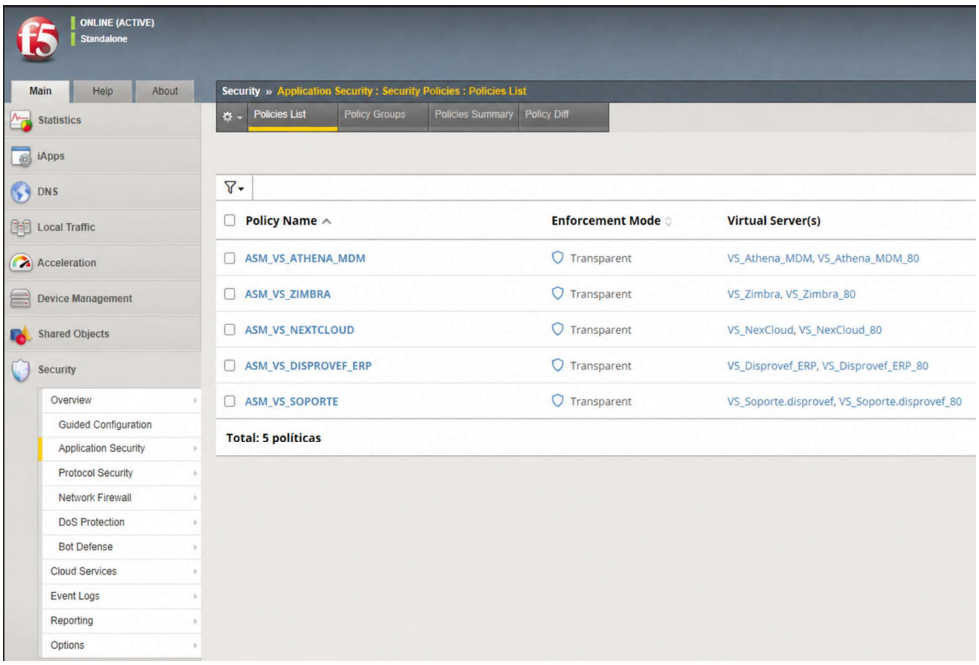


Nota. La figura muestra la configuración de los Virtual Servers en el F5 BIG-IP VE, utilizados para la publicación y gestión del tráfico HTTP/HTTPS hacia los servicios web de DISPROVEF, permitiendo su inspección y control a través del WAF.

En esta fase, el WAF inspecciona todo el tráfico real sin aplicar bloqueos, permitiendo identificar parámetros legítimos, rutas de uso frecuente, métodos HTTP válidos, variaciones de carga, patrones de sincronización y comportamientos específicos de cada aplicación (ERP, Nextcloud, Zimbra, Soporte y Athena MDM).

Figura 6

Políticas de seguridad WAF en modo de aprendizaje (Transparent)

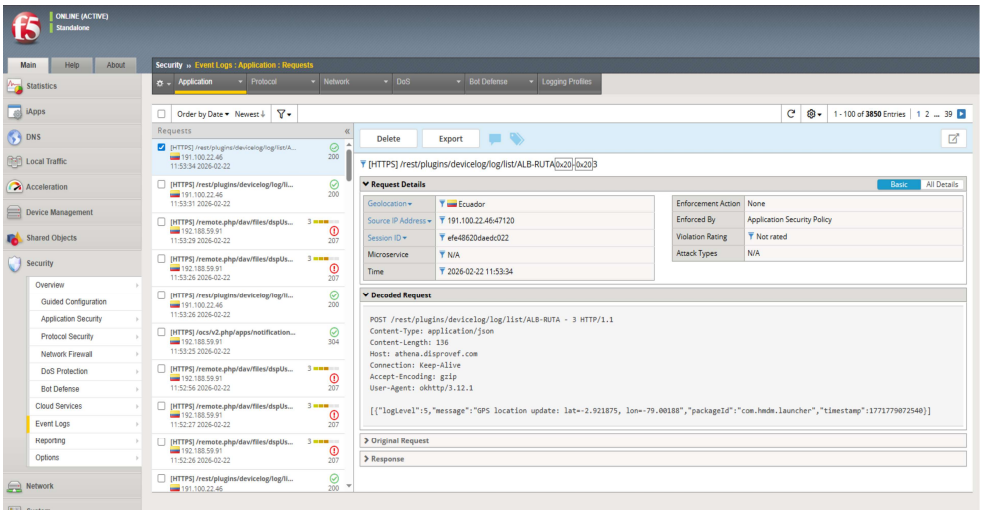


Nota. El modo aprendizaje de las políticas permitirá el monitoreo del tráfico y la identificación de eventos sin aplicar bloqueos.

Fase 3: Ajuste y calibración de políticas: Las políticas fueron ajustadas en base a la mediante la información recopilada en la fase de aprendizaje lo que permitió la habilitación gradual de firmas OWASP, parámetros, control de cabeceras y excepciones justificadas en caso de falsos positivos. Cada ajuste se valida internamente junto con el personal de TI de DISPROVEF para asegurar que las aplicaciones continúen funcionando de manera estable. En esta fase se corrigen falsos positivos, se documentan rutas sensibles y se consolida la configuración base del modelo.

Figura 7

Registro de eventos de seguridad para análisis y ajuste de políticas



Nota. Eventos de seguridad registrados F5 utilizados para el análisis, identificación de anomalías y ajuste de las políticas de seguridad del WAF.

Fase 4: Activación del modo de protección: Con las políticas ajustadas y validadas, se activó el bloqueo de forma progresiva: primero en las aplicaciones menos sensibles y luego en las más críticas. A partir de esto el WAF comienzo a bloquear solicitudes maliciosas, patrones anómalos, intentos de inyección, manipulación de parámetros y categorías OWASP previamente identificadas, durante todo el proceso se mantuvo monitoreo constante para verificar que el bloqueo no interfiriera en la continuidad del servicio.

Fase 5: Documentación, monitoreo continuo y sostenibilidad: Se consolidó una memoria técnica con el razonamiento detrás de cada decisión, ajustes de sensibilidad, excepciones justificadas y criterios para equilibrar la protección con

la operación de servicios como Nextcloud, Zimbra, Zlibra y Athena MDM. Este documento se recoge en el Anexo E. Adicionalmente se explicó al equipo de TI de DISPROVEF la estructura de las políticas, cómo interpretar los eventos del ASM y qué necesita el sistema para mantenerse operativo sin depender de un especialista externo. Esta transferencia se limita a guías y recomendaciones prácticas sin requerir la generación de manuales extensos o documentación adicional fuera del alcance del proyecto.

3.5 Análisis de riesgos operativos

El despliegue del WAF F5 BIG-IP VE en el entorno productivo de DISPROVEF implica riesgos operativos que deben gestionarse para garantizar la continuidad de los servicios críticos. La siguiente tabla resume los principales riesgos identificados, su probabilidad, su impacto y las medidas de mitigación previstas:

Tabla 7

Identificación y control de riesgos operativos del modelo OWASP–WAF

Riesgo	Descripción	Medida de mitigación	Mecanismo de monitoreo	Evidencia / indicador
Falsos positivos	Clasificación incorrecta de tráfico legítimo como malicioso	Ajuste progresivo de políticas y validación en fase de ajuste	Revisión de logs del WAF	Reducción del 78,40 % de eventos alertados
Sobrecarga del WAF	Saturación de recursos por alto volumen de tráfico o reglas complejas	Optimización de políticas y control de tráfico	Alertas en F5 BIG-IP (CPU, memoria, TMM)	Ausencia de eventos críticos de CPU (starvation, overload)
Consumo elevado de memoria	Uso excesivo de memoria por	Ajuste de configuraciones	Alertas de memoria (OOM,	Sin registros de eventos

	procesamiento de reglas	y monitoreo de recursos	swap high, malloc failed)	críticos de memoria
Saturación de almacenamiento	Uso excesivo de disco por logs o procesos internos	Gestión de logs y monitoreo de particiones	Alertas de disco (warning y critical)	Sin eventos de disco en estado crítico
Degradación del rendimiento	Disminución en capacidad de respuesta del sistema	Implementación progresiva y validación en entorno productivo	Monitoreo general del sistema	Operación estable sin interrupciones

Nota. La tabla presenta la identificación de los riesgos operativos asociados a la implementación del modelo OWASP–WAF, junto con sus medidas de mitigación, mecanismos de monitoreo y evidencia observada durante la fase de protección en el entorno productivo de DISPROVEF.

Durante la fase de protección, los riesgos operativos asociados a la sobrecarga del WAF y a la degradación del rendimiento fueron gestionados mediante la configuración de alertas específicas en la plataforma F5 BIG-IP, orientadas a la detección temprana de condiciones críticas a nivel de recursos. Se implementaron reglas de monitoreo para CPU (starvation, overload y scheduler delay) , memoria (out of memory, malloc failed y uso elevado de swap) y almacenamiento con umbrales de ocupación de particiones, estado crítico o falta de espacio disponible. El envió de alertas se realizó a través de traps SNMP y al correo electrónico institucional, permitiendo la generación de eventos automáticos el escalamiento de incidentes hacia el equipo de soporte técnico. A partir del seguimiento realizado, no se registraron eventos críticos asociados a saturación de CPU, agotamiento de memoria ni condiciones de almacenamiento que comprometieran la estabilidad del sistema. El WAF operó sin afectar la disponibilidad ni el rendimiento de los servicios protegidos. La configuración detallada de las alertas implementadas se presenta en el Anexo D.

Finalmente, como mecanismo de alta disponibilidad y salvaguarda técnica ante contingencias críticas imprevistas se ha formalizado un Plan de Reversión Inmediata. Este contingente aplicaría en situaciones en las que el F5 BIG-IP VE presente algún tipo de anomalía u estado de indisponibilidad parcial o completa que genere intermitencias o degradaciones en el servicio por el ende el protocolo operativo definido dispone la ejecución de un bypass lógico del dispositivo desde el firewall perimetral a través de la reconfiguración de las políticas NATs con la finalidad de restituir el flujo directo hacia los servidores internos en menos de cinco minutos. Esta medida prioriza la continuidad de negocio de DISPROVEF asegurando que la seguridad en la capa de aplicación no se convierta en un punto único de fallo para la organización.

3.6 Validación operativa

La validación operativa se realizó utilizando el siguiente checklist, que permite confirmar que los servicios continúan funcionando correctamente tras la publicación en el WAF y que las políticas configuradas no generan afectaciones sobre la operación de DISPROVEF.

Tabla 8

Checklist de validación operativa de los servicios web tras la implementación del WAF

Elemento a validar	Descripción de la verificación	Responsable	Resultado esperado
Acceso a cada servicio web publicado	Confirmar que Nextcloud, Zimbra, Zlibra ERP, Soporte y Athena MDM cargan	TI DISPROVEF / Administrador WAF	Acceso exitoso sin errores.

	correctamente detrás del WAF.		
Autenticación de usuarios	Validación de login y sesiones activas en todas las plataformas.	TI DISPROVEF	Inicio de sesión correcto.
Carga y descarga de archivos	Verificar operaciones en Nextcloud y plataformas que intercambian documentos.	TI / Validación operativa	Sin bloqueos ni interrupciones.
Sincronización de correo (Zimbra)	Validación de acceso webmail y sincronización básica.	TI	Funcionamiento normal.
Flujos críticos del ERP (Zlibra)	Validar consultas, formularios y transacciones frecuentes.	TI / Usuario clave	Operación estable y sin bloqueos.
Operación de Soporte	Prueba de servicios mediante la generación de nuevos tickets, navegación y acciones internas de usuarios.	TI / Área técnica	Plataforma operativa.
Operación de Athena MDM	Prueba de acceso y monitoreo de funciones básicas de dispositivos moviles	TI	Operación normal.

Certificados SSL	Carga correcta de certificados y ausencia de advertencias.	Administrador WAF	HTTPS funcional y confiable.
Eventos del WAF en tiempo real	Revisión de eventos ASM	Administrador WAF	Eventos consistentes con la operación.
Detección de falsos positivos	Revisar solicitudes marcadas como violación y descartar que se corresponda a una petición permitida	TI / Administrador WAF	Identificación o descarte de falsos positivos.
Excepciones aplicadas	Verificar que cualquier excepción aplicada está documentada.	Administrador WAF	Excepciones justificadas.
Rutas internas y NAT	Confirmar que los flujos desde el WAF hacia los servidores internos funcionan correctamente.	Redes / TI	Tráfico estable y sin pérdidas.
Bitácora técnica	Registro de cada cambio realizado en la configuración.	Administrador WAF	Bitácora actualizada.

Nota. La tabla muestra el proceso de validación operativa aplicado a los servicios web, mediante un checklist estructurado que permite confirmar la continuidad del servicio y la correcta aplicación de las políticas de seguridad del WAF.

3.7 Roles operativos y sostenibilidad del modelo

Para asegurar la continuidad y correcta operación del modelo OWASP–WAF en DISPROVEF, se definen dos roles operativos centrales, cuya participación es clave para mantener la protección, el monitoreo y la estabilidad de los servicios expuestos. Estos roles se integran dentro de la memoria técnica del proyecto y no requieren la generación de manuales adicionales, sino únicamente el cumplimiento de lineamientos básicos de buenas prácticas.

Administrador: responsable técnico del F5 BIG-IP VE y del modelo de seguridad implementado, entre sus funciones se incluyen:

- Revisar y analizar los eventos generados por el WAF diferenciando amenazas reales de falsos positivos.
- Aplicar ajustes o excepciones en las políticas de control cuando sean necesarios basado en el análisis de los eventos.
- Gestión de certificados SSL a fin de mantenerlos actualizados y cargados correctamente en los perfiles cliente o servidor para su uso en la gestión de tráfico o administración.
- Mantener actualizadas las firmas de seguridad conforme a las liberaciones de fábrica y su revisión periódica.
- Documentar cualquier modificación en la bitácora técnica, así como la confirmación de logs de auditoria propias del equipo.

- Coordinar pruebas de servicios con el equipo de tecnología de DISPROVEF antes y después de que se realicen ajustes en las políticas a fin de asegurar que los cambios aplicados no afecten la operación de los servicios protegidos o generen algún tipo de degradación de los mismos.

Perfil requerido: Conocimientos en redes, seguridad en capa de aplicación y operación del WAF.

Operador: responsable del seguimiento diario de la operación del modelo, su responsabilidad es identificar anomalías, incrementos inusuales en alertas o posibles falsos positivos y comunicar oportunamente cualquier situación al Administrador para su revisión o solución dependiendo del caso. Entre sus actividades están:

- Monitorear alertas y tendencias de tráfico y eventos registrados por el WAF.
- Revisar logs para identificar patrones inusuales o repetitivos.
- Verificar la estabilidad después de aplicar cambios en las políticas.
- Reportar incidentes operativos o comportamientos inesperados.

Perfil requerido: seguridad en capa de aplicación y operación del WAF, este rol no requiere modificar configuraciones, solo supervisar y reportar.

3.8 Limitaciones del estudio

Las limitaciones del modelo están asociadas a su diseño metodológico y al contexto de aplicación. En primer lugar, no se contó con un grupo de control limitando la capacidad de atribuir los resultados exclusivamente a la intervención sin considerar

factores externos. No obstante, el diseño cuasi-experimental permitió comparar el antes y el después dentro del mismo entorno.

La segunda es que los resultados reflejan un entorno concreto DISPROVEF, con su infraestructura, su volumen de tráfico y sus servicios, por lo que su aplicación en otros escenarios puede requerir un proceso previo de adaptación. Una limitación adicional fue la ausencia de pruebas de penetración posteriores a la implementación, esta decisión fue producto de una evaluación de costo-beneficio y gestión de riesgos basada en los siguientes factores:

1. Restricciones de Recursos y Presupuesto: El proyecto se ejecutó bajo un presupuesto optimizado (ver Tabla 8), priorizando la adquisición y el afinamiento técnico de la solución, La ejecución de pruebas de penetración ofensivas adicionales habría demandado una inversión económica y de tiempo que excedía los límites establecidos para esta etapa de fortalecimiento institucional.
2. Carencia de Entorno Mirror (Staging): Debido a limitaciones de infraestructura, la investigación se realizó directamente sobre el entorno productivo real de DISPROVEF. Sin un entorno espejo para pruebas destructivas, el riesgo de generar una degradación del servicio o corrupción de datos en sistemas críticos como el ERP Zlibra o el MDM Athena era técnicamente inaceptable.
3. Riesgos en el Flujo Operativo y Comunicaciones: Someter a estos componentes (firewalls perimetrales, hipervisores, switches entre otros) a ráfagas de ataques simulados podría haber causado latencias imprevistas o fallos de hardware en dispositivos que no fueron dimensionados originalmente para soportar

validaciones ofensivas de alta intensidad en paralelo con la carga operativa normal.

La validación se limitó al enfoque defensivo sobre tráfico real. Las pruebas ofensivas quedan como una línea de trabajo futura abierta, viable si se dispone de un entorno de pruebas aislado, sería útil replicar el modelo en otras organizaciones con infraestructuras distintas y comparar resultados con un grupo de control.

3.9 Sostenibilidad del modelo

El modelo de mitigación requiere actividades periódicas orientadas al mantenimiento de las políticas de seguridad y al seguimiento del comportamiento del tráfico, integrándose como parte de las buenas prácticas para la operación del sistema:

- Revisión periódica: verificar que las políticas reflejan el tráfico real y no falsos positivos.
- Actualización de firmas de seguridad: según las recomendaciones del fabricante y aparición de nuevas amenazas.
- Gestión de certificados SSL, manteniéndolos actualizados y cargados correctamente en los perfiles cliente o servidor.
- Revisión de excepciones: para confirmar que siguen justificadas y no representen un riesgo.
- Validación de servicios: Confirmar operatividad se servicios mediante pruebas controladas a fin de garantizar que los servicios operan con normalidad.
- Documentar ajustes: mantener trazabilidad sobre los cambios y facilitar procesos de auditorías o plan de reversión.

La ejecución periódica de estas actividades permite mantener actualizadas las políticas implementadas y verificar su comportamiento frente a cambios en el tráfico o en los servicios publicados. Para dar seguimiento a la operación del modelo se definieron métricas como: volumen de eventos alertados, porcentaje de tráfico bloqueado, cantidad de falsos positivos y la estabilidad de los servicios después de aplicar algún ajuste.

Durante el primer mes de operación se recomienda realizar un monitoreo constante, así como la evaluación de los indicadores al menos una vez a la semana posteriormente con la evolución del modelo se puede cambiar la frecuencia a mensual, esto permitirá identificar cambios en el comportamiento del tráfico y aplicar ajustes oportunos en las políticas de seguridad garantizando la sostenibilidad del modelo en el tiempo manteniendo un equilibrio adecuado entre seguridad y continuidad operativa

3.10 Impacto directo previsto

La implementación del modelo en DISPROVEF generará impactos directos sobre la seguridad, estabilidad y continuidad de sus servicios críticos al integrarse un Web Application Firewall en la nueva DMZ se obtendrán beneficios medibles derivados del análisis y filtrado del tráfico real que actualmente llega a los servidores internos sin mecanismos avanzados de inspección. Entre los principales tenemos:

1. Mitigación inmediata: mediante el bloqueo de solicitudes maliciosas asociadas a las categorías OWASP TOP 10 por ejemplo: ellas inyección, manipulación de parámetros, abuso de métodos HTTP entre otras.
2. Estabilidad Operativa: Las solicitudes inválidas o malformadas son contenidas por el WAF evitando que lleguen a los servidores internos.

3. Visibilidad de amenazas, los registros ASM del WAF identificaron patrones anómalos, rutas sensibles y comportamientos repetitivos que no eran visibles en el firewall.
4. Reducción del riesgo, con la aplicación del modelo las violaciones críticas se detectan antes de que lleguen a los servidores internos.
5. Fortalecimiento de la ciberresiliencia, el modelo sigue OWASP y las prácticas recomendadas por F5 permitiendo anticipar incidentes y disminuir su probabilidad de éxito.

Estos impactos serán evidenciados de la comparación entre el estado de protección previo y el comportamiento de la solución posterior a la activación del bloqueo y ajuste de las políticas.

3.11 Plan de despliegue de la solución

El despliegue del modelo en DISPROVEF se realizó de forma progresiva y controlada garantizando la continuidad operativa de los servicios productivos en cada etapa. A continuación, se detallan las actividades necesarias para implementar, ajustar y validar la solución con la mínima afectación posible en la arquitectura actual.

Preparación del entorno (Semana 1)

- Implementación de la red DMZ destinada alojar el direccionamiento que usara F5 para la publicación de los servicios manteniendo una separación lógica contra el resto de la red corporativa.

- Configuración de direccionamiento, NAT y rutas hacia los servidores internos para permitir el flujo de comunicación entre F5 (tráfico controlado) y los servidores encargados de los servicios.
- Verificación de certificados SSL para tráfico operativo y accesos al portal de administración y para la publicación de los servicios a través del protocolo seguro HTTPS.
- Pruebas iniciales de conectividad extremo a extremo previo a la puesta en producción de la arquitectura.

WAF en modo aprendizaje (Semanas 2–3)

- Redirección de los servicios al WAF mediante Nats en el firewall perimetral.
- Registro de comportamiento del tráfico real y análisis previo.
- Detección de parámetros, rutas y métodos HTTP propios de cada aplicación.

Ajuste de políticas de seguridad (Semanas 3–4)

- Activación progresiva de firmas de seguridad para que coincidan con los patrones observados.
- Detección de parámetros, rutas y métodos HTTP propios de cada aplicación.
- Pruebas funcionales en conjunto con el equipo de TI de DISPROVEF.

Activación de modo Protección (Semanas 5–6)

- Paso a modo bloqueo por tandas de servicios empezando por los de menor impacto operativo.
- Seguimiento continuo de los eventos bloqueados y de los posibles falsos positivos.
- Correcciones puntuales hasta dejar las políticas listas para todos los servicios.

Cierre técnico y transferencia de conocimientos (Semana 6)

- Documentación y entrega de las configuraciones aplicadas y de los criterios de ajuste en las políticas.
- Revisión conjunta del modelo final.
- Transferencia de conocimiento al administrador y operador.
- Recomendar a la empresa la evaluación post-proyecto para adquisición definitiva de licenciamiento.

3.12 Presupuesto del proyecto

El presupuesto incluye los costos estimados asociados a la eventual adopción del modelo de mitigación con F5 BIG-IP Virtual Edition (VE) como parte de la arquitectura de seguridad de DISPROVEF. Se utilizaron licencias de evaluación (trial) provistas por F5 Networks esto permitió habilitar temporalmente los módulos LTM (Administrador de tráfico local) y ASM (Administrador de seguridad de aplicaciones) con todas sus funciones para el desarrollo investigativo y de resultados del modelo.

Una vez concluido el estudio y presentados los resultados, será decisión de DISPROVEF determinar si procede con la adquisición formal de licenciamiento y soporte técnico. Por esta razón, los costos presentados corresponden a valores referenciales de mercado, y representan el gasto esperado en caso de que la empresa decida continuar con la solución de forma permanente.

Tabla 9

Presupuesto estimado para la implementación del modelo OWASP–WAF

Categoría / Rubro	Descripción	Tipo de Gasto	Costo Estimado (USD)
Implementación técnica del proyecto	Instalación, configuración, tuning y validación técnica (uso de licencia trial durante el estudio).	Inversión inicial	1.000 – 1.500
Validación operativa	Pruebas funcionales realizadas por el personal técnico de DISPROVEF.	Inversión inicial	0 (costo interno)
Contingencias	Posibles ajustes, cambios menores o soporte complementario durante el despliegue.	Inversión inicial	300 – 500
Infraestructura	Uso de recursos existentes (ESXi/Hyper-V). No implica desembolsos adicionales.	Inversión inicial	0 (recursos existentes)
Licencia F5 BIG-IP VE (LTM + ASM)	Suscripción anual VE (25–200 Mbps). Valor referencial para futura adopción definitiva.	Recurrente	4.000 – 6.000 / año
Soporte & Updates (F5 Standard)	Soporte 8x5, actualizaciones de firmas ASM y parches de seguridad críticos.	Recurrente	800 – 1.200
Certificados SSL	Renovación o adquisición anual de certificados comerciales.	Recurrente	60 – 120
TOTAL ESTIMADO (AÑO 1)	**Suma de inversión inicial + recurrente**		**6.160 – 9.320 USD**

Nota. Durante el proyecto se emplearán licencias de evaluación proporcionadas por F5 Networks. Los costos presentados corresponden únicamente al escenario de adopción futura e implican valores referenciales basados en precios públicos de F5 VE (F5, 2024; WorldTech IT, 2024; GuidePoint Security, 2024).

La estimación presentada permite relacionar el presupuesto de implementación con el costo operativo potencial de no adoptar el modelo OWASP–WAF. Aunque el estudio no contempló un cálculo financiero del retorno de inversión, la evidencia reportada por IBM Security (2023) señala que los incidentes de seguridad pueden implicar costos elevados y tiempos prolongados de detección y contención.

Tabla 10

Referencia de impacto económico y operativo de incidentes de seguridad

Métrica	Valor reportado	Implicación para el estudio
Costo promedio por brecha de seguridad	USD 4,45 millones	Un incidente puede generar pérdidas económicas significativamente superiores al costo de implementación del WAF
Tiempo promedio de detección y contención	277 días	La permanencia del incidente sin control incrementa el impacto operativo
Incremento de costos por detección tardía	Hasta 30 % adicional	La ausencia de mecanismos de mitigación temprana aumenta el costo total del incidente
Vectores frecuentes de ataque	Aplicaciones web y credenciales comprometidas	Los servicios web expuestos representan puntos críticos de entrada

Nota. Datos adaptados de IBM Security (2023), *Cost of a Data Breach Report*.

En DISPROVEF, una caída de la plataforma web arrastra consigo la operación comercial, la gestión de documentos, el correo institucional, el soporte técnico y el control de los dispositivos móviles ya que no son servicios aislados, comparten infraestructura y dependen del mismo flujo de tráfico. El WAF se planteó como una forma de blindar los servicios y reducir la probabilidad de incidentes que pudieran afectar la disponibilidad de las aplicaciones, antes de que una violación obligara a remediar sobre la marcha con los costos operativos y de reputación que eso implica.

Esta relación resulta relevante para la adopción futura del modelo, en la medida en que vincula el costo de implementación con la reducción del riesgo sobre servicios críticos del negocio.

3.13 Resultados del diagnóstico inicial del entorno productivo de DISPROVEF

El diagnóstico inicial del entorno productivo de DISPROVEF permitió identificar las condiciones reales bajo las cuales se encontraban expuestos los servicios web institucionales antes de la implementación del Web Application Firewall. A partir del análisis de la arquitectura tecnológica existente, se evidenció que la publicación de los servicios se realizaba directamente hacia Internet mediante reglas de firewall y NAT configuradas sobre el equipo perimetral, sin la incorporación de una capa dedicada de inspección y protección a nivel de aplicación.

Durante la revisión de la arquitectura se identificó que el Firewall ejecutaba funciones básicas de filtrado por direcciones IP y puertos sin contar algún tipo de inspección profunda de paquetes y era el encargado de la publicación de los diversos servicios de DISPROVEF por ejemplo: Nextcloud, Zlibra ERP, Soporte, Zimbra y Athena MDM. Debido a las limitantes propias de este equipo el tráfico HTTP/HTTPS llegaba directamente a los servidores internos sin que nadie las detuviera y sin validaciones de capa de aplicaciones asociadas al OWASP Top 10 por listar algunas: inyecciones de código, manipulación de parámetros, explotación de vulnerabilidades conocidas, ataques de fuerza bruta y técnicas de evasión.

DISPROVEF no contaba con procedimientos regulares para evaluar la seguridad de las aplicaciones publicadas ni con herramientas que facilitaran el análisis de eventos específicos de la capa de aplicación de las solicitudes recibidas. Como consecuencia, gran

parte del comportamiento del tráfico HTTP/HTTPS quedaba fuera del alcance de los mecanismos habituales de supervisión. Estos resultados fundamentaron la necesidad de incorporar una solución de inspección y protección en capa de aplicación, dando paso a la siguiente fase del proyecto, orientada a la implementación y ajuste progresivo del Web Application Firewall.

3.14 Resultados de la fase de aprendizaje del Web Application Firewall

La fase de aprendizaje se ejecutó con el Web Application Firewall F5 BIG-IP ASM operando en modo transparente, con el propósito de observar el comportamiento real del tráfico sin aplicar bloqueos automáticos que pudieran afectar la continuidad operativa. El modo transparente del WAF permitió registrar todas las conexiones de los usuarios recibidas por el WAF bajo un escenario real en la red DMZ y los eventos de seguridad alertados debido a coincidencias de firmas o anomalías permitiendo construcción de una línea base (baseline) del comportamiento de las aplicaciones a partir de la cual se identificaron patrones de uso, parámetros esperados y posibles desviaciones gracias a esto de esto se optimizó el proceso de ajuste de políticas en fases posteriores reduciendo la probabilidad de falsos positivos al alinear las reglas del WAF con el comportamiento real del entorno productivo (Fortinet, 2025).

Durante esta fase, el sistema inspeccionó la totalidad del tráfico HTTP/HTTPS dirigido a las aplicaciones publicadas en el entorno productivo. A diferencia de un muestreo limitado, el análisis se realizó sobre el total del tráfico registrado en el periodo de observación, lo que permitió obtener una caracterización representativa del comportamiento real de las aplicaciones y de su exposición en la capa de aplicación.

En esta fase el volumen total de solicitudes inspeccionadas fue de 1.106.926 eventos, de los cuales 473.863 (42,81%) se clasificaron como tráfico permitido y 633.063 (57,19%) generaron alertas de seguridad. Durante esta etapa no se registraron eventos bloqueados ya que el objetivo en este punto era observar el comportamiento del tráfico y recopilar información que luego se usaría para el ajuste de las políticas, los resultados obtenidos son una proporción esperable en esta fase. El WAF aprende basado en las solicitudes recibidas y tienden a marcar como sospechoso tráfico que en realidad es legítimo debido a su coincidencia con las reglas de detección de la línea base.

En la revisión de los eventos se observó que muchas de estas alertas estaban asociadas a comportamientos legítimos de las aplicaciones publicadas debido a que las políticas implementadas aún no distinguían completamente entre tráfico normal y patrones potencialmente maliciosos hacia los servicios de DISPROVEF. El análisis de esta fase permitió identificar tendencias en el comportamiento del tráfico, rutas de acceso frecuentes, parámetros utilizados por las aplicaciones y tipos de solicitudes que requerían validación más precisa. Esta información constituyó la base para el proceso de optimización de políticas, orientado a reducir falsos positivos y mejorar la capacidad de diferenciación entre tráfico legítimo y eventos potencialmente maliciosos.

Los resultados de esta fase constituyen la línea base del diseño cuasi-experimental, utilizado para evaluar el desempeño del modelo de mitigación, la fase de aprendizaje dejó dos cosas claras: el volumen de alertas era alto porque las reglas aún no estaban calibradas y una parte importante de esas alertas eran falsos positivos. Por esta razón, la fase de aprendizaje tuvo un papel fundamental en la identificación de falsos

positivos y en la posterior adaptación de las reglas al comportamiento real de los servicios protegidos de la siguiente fase.

3.15 Resultados de la configuración optimizada y activación del modo protección

Una vez concluida la fase de aprendizaje y ejecutado el proceso de ajuste de políticas para la reducción de falsos positivos, se activó la política del Web Application Firewall en modo bloqueo. A partir de este momento, las solicitudes que incumplían las reglas de seguridad dejaron de ser únicamente registradas y pasaron a ser bloqueadas antes de alcanzar las aplicaciones publicadas en la zona desmilitarizada. Durante esta etapa no se modificó la infraestructura ni en la publicación de servicios, de modo que las condiciones de evaluación se mantuvieron equivalentes a las fases anteriores.

En la fase de protección se inspeccionaron 2.084.366 solicitudes HTTP/HTTPS. De este total 1.751.497 solicitudes (84,03%) fueron clasificadas como tráfico permitido y 332.869 solicitudes (15,97%) fueron bloqueadas por incumplir las políticas de seguridad configuradas. No se registraron eventos en estado de alerta, las reglas ajustadas permitieron una clasificación entre tráfico legítimo y solicitudes maliciosas.

La evolución entre fases refleja la maduración del modelo, en aprendizaje se obtuvo una gran cantidad de eventos alertados, en la fase de ajuste se redujeron significativamente los falsos positivos gracias a la optimización de las políticas y en la fase de protección las solicitudes que incumplían las políticas de seguridad fueron filtradas automáticamente. Este resultado confirma que el proceso de optimización permitió mejorar la precisión del sistema, evitando la generación de alertas innecesarias y habilitando una respuesta directa frente a eventos identificados como maliciosos.

Desde una perspectiva cuantitativa, la presencia de un 15,97 % de tráfico bloqueado representa la materialización de la capacidad de mitigación del modelo OWASP–WAF en condiciones reales de operación. Este porcentaje no debe interpretarse como incremento de amenazas, sino como la capacidad del sistema para interceptar solicitudes que anteriormente solo eran registradas como alertas en fases previas.

En términos operativos, la activación del modo bloqueo no generó interrupciones ni afectaciones de los servicios de DISPROVEF mediante pruebas controladas se confirmó la correcta operación de los servicios y la continuidad de procesos críticos, evidenciando de esta manera que el ajuste efectuado en las políticas incremento los niveles de seguridad sin comprometer la disponibilidad de los servicios.

Los resultados alcanzados demuestran que el modelo implementado evolucionó desde la observación y análisis de eventos hacia un esquema capaz mitigar activamente eventos en la capa de aplicación.

3.16 Análisis comparativo del estado de exposición y mitigación

La validación de la hipótesis se realizó mediante el análisis comparativo de los eventos registrados en las fases operativas del modelo OWASP–WAF: aprendizaje, ajuste y protección, considerando la evolución en la clasificación del tráfico y la capacidad de mitigación del sistema en un entorno productivo real. Para el cálculo de la reducción de eventos se tomó como referencia la fase de aprendizaje, en la que el WAF operaba sin bloqueo activo, y la fase de protección, donde ya se encontraban aplicadas las políticas optimizadas. La fase de ajuste se utilizó como un periodo intermedio de calibración, en el cual se optimizaron progresivamente las políticas antes de activar el modo de protección. Con el propósito de evaluar el comportamiento del modelo OWASP–WAF

durante las diferentes etapas de implementación, se consolidaron los eventos registrados en cada fase del proceso. La siguiente tabla presenta el resumen de transacciones procesadas, clasificadas como permitidas, alertadas y bloqueadas durante las fases de aprendizaje, ajuste y protección.

Tabla 11

Resumen de conexiones procesadas

Fase	Totales	Permitidos (%)	Alertados (%)	Bloqueados (%)
Aprendizaje (15 días)	1106926	42,81	57,19	0,00
Ajuste (15 días)	1088120	87,44	12,56	0,00
Protección (30 días)	2084366	84,03	0,00	15,97
Total	4279412	74,24%	17,99%	7,78%

Nota. Los resultados validan la eficacia del modelo implementado y su impacto en la seguridad de DISPROVEF.

En la fase de protección el WAF bloqueó 332.869 solicitudes, equivalentes al 15,97 % del tráfico total inspeccionado, ese porcentaje representa las solicitudes que el ASM interceptó de forma proactiva por contener patrones compatibles con las categorías del OWASP Top 10 principalmente asociados a inyección y fallos de control de acceso y que en ausencia de estos controles habrían llegado directamente a los servidores internos. A continuación, se detalla el comportamiento de cada una de las fases y como su progresión permitió consolidar una postura de defensa activa sin afectar el desempeño de los servicios de DISPROVEF.

En la fase de aprendizaje se registró e inspecciono 1.106.926 solicitudes de las cuales 633.063 (57,19%) se clasificaron alertados y 473.863 (42,81%) como tráfico

permitido. Constituyendo la línea base caracterizada por una alta proporción de eventos etiquetados como anómalos o falsos positivos debido a la ausencia de políticas ajustadas.

Durante la fase de ajuste se evidenció una mejora significativa en la clasificación del tráfico. De un total de 1.088.120 solicitudes, 951.463 (87,44 %) fueron clasificadas como permitidas y 136.657 (12,56 %) como alertadas. Esta variación refleja el efecto directo del proceso de optimización de políticas, orientado a la reducción de falsos positivos y a la mejora en la precisión del sistema. En esta fase se observó una disminución progresiva de eventos alertados, al pasar de 633.063 a 136.657, lo que representó una disminución del 78,40%; Este comportamiento evidenció el efecto del ajuste de políticas sobre la clasificación del tráfico; sin embargo, correspondió a un periodo de ajuste de reglas previo a la activación del modo de protección, por lo que no se consideró como estado final del sistema.

En la fase de protección, el modelo operó en modo bloqueo, registrando un total de 2.084.366 solicitudes inspeccionadas, de las cuales 1.751.497 (84,03 %) fueron permitidas y 332.869 (15,97 %) fueron bloqueadas por incumplimiento de las políticas de seguridad. En esta etapa no se generaron eventos en estado de alerta, lo que indica que el sistema alcanzó un nivel de madurez suficiente para clasificar y gestionar el tráfico de manera directa.

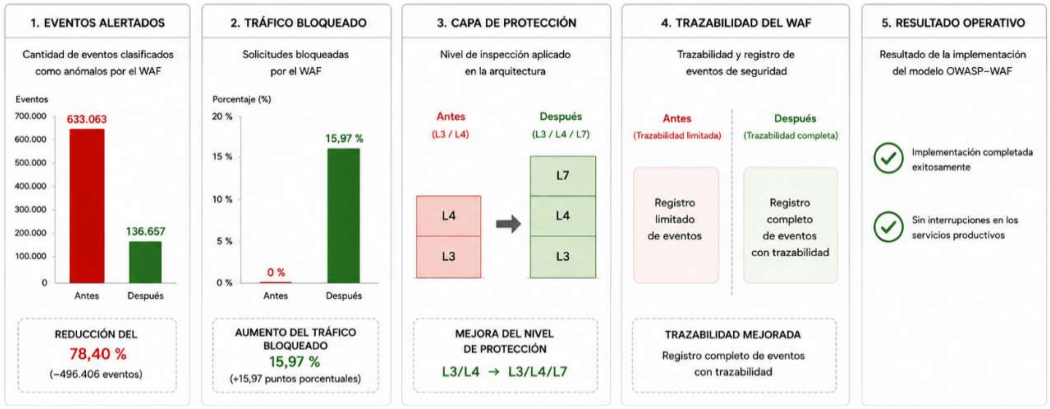
La comparación entre las fases de aprendizaje y ajuste mostró una reducción del 78,40% de eventos alertados pasando de 633.063 a solo 136.657. Esa disminución es resultado de un proceso de revisión de reglas, eliminación de firmas que generaban falsos positivos sobre el tráfico legítimo de DISPROVEF, el modelo pasó de señalar como sospechoso más de la mitad del tráfico inspeccionado a generar alertas solo sobre eventos

que presentaban un comportamiento anómalo contra lo esperado, antes de efectuar el bloqueo fue indispensable efectuar esta depuración ya que un volumen excesivo de alertas habría saturado al equipo de TI y dificultado distinguir las amenazas reales del ruido de fondo. Durante este proceso y como parte de la perspectiva operativa, la implementación del modelo no generó interrupciones ni afectaciones en los servicios productivos demostrando que se logró incrementar la seguridad en la capa de aplicación sin comprometer la disponibilidad de los sistemas.

Con el propósito de sintetizar los hallazgos más relevantes obtenidos durante la implementación del modelo, se realizó una comparación de los indicadores más representativos antes y después de la intervención presentados en la Figura 8.

Figura 8

Comparación de los indicadores de mejora en la implementación del modelo

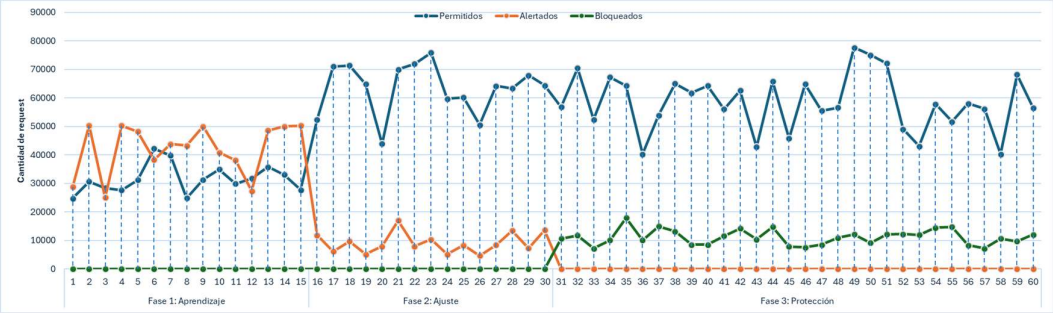


En consecuencia, los resultados obtenidos permiten aceptar la hipótesis planteada, al evidenciar que la implementación del modelo OWASP–WAF redujo significativamente los eventos inicialmente clasificados como anómalos, mejoró la precisión del sistema y permitió establecer mecanismos efectivos de mitigación en la capa de aplicación bajo condiciones reales de operación.

La evolución del comportamiento del tráfico a lo largo de las fases del modelo se presenta en la siguiente Figura, en la cual se observa la transición desde un escenario con alta proporción de eventos alertados durante la fase de aprendizaje, hacia una reducción significativa de estos eventos en la fase de ajuste, y finalmente la activación de mecanismos de mitigación mediante bloqueo en la fase de protección.

Figura 9

Evolución del comportamiento del tráfico durante las fases del modelo OWASP–WAF



Nota. La figura muestra la evolución del tráfico web en las fases de aprendizaje, ajuste y protección, evidenciando la reducción de eventos alertados y la activación de mecanismos de mitigación mediante bloqueo, sin afectar la continuidad operativa.

Como se observa en la figura 9, La evolución del tráfico a lo largo de las tres fases muestra el ajuste progresivo del modelo, durante el aprendizaje las alertas representaron el 57,19% de los registros generados, una situación esperable cuando el WAF opera con reglas genéricas proporcionando información para el análisis inicial de las políticas. Tras el proceso de afinamiento de reglas esta proporción descendió al 12,56% validando la precisión alcanzada al depurar los falsos positivos identificados en la fase anterior, la fase de protección incorporó mecanismos de bloqueo sobre las solicitudes que incumplían los criterios definidos, registrándose un 15,97 % de tráfico bloqueado frente a un 84,03 % de tráfico permitido sin generar alertas remanentes.

3.17 Comprobación de la hipótesis de investigación

La hipótesis de investigación (H_1) planteó que la implementación de un modelo basado en un Web Application Firewall configurado de manera optimizada permitiría reducir significativamente los eventos asociados a riesgos del OWASP Top 10 en los servicios productivos de DISPROVEF, sin afectar la continuidad operativa ni el desempeño del sistema. En contraste, la hipótesis nula (H_0) estableció que dicha implementación no generaría una mejora significativa o produciría un impacto negativo en la operación de los servicios.

El análisis comparativo entre fases se resume en tres cifras: 633.063 eventos alertados en aprendizaje, 136.657 eventos alertados en ajuste obteniendo una reducción del 12,56% en relación a la primera fase y como fase final en protección se inspeccionaron 2.084.366 de solicitudes de estos 332.869 (15,97%)eventos se bloquearon de manera automática debido a que las solicitudes coincidieron con los criterios especificados en las firmas de seguridad enmarcado en el OWASP, durante todo este proceso los servicios productivos operaron sin interrupciones ni degradaciones atribuibles al WAF.

Los resultados demuestran que se fortaleció los controles sobre el tráfico a nivel de aplicación HTTP/HTTPS, la reducción de alertas y la activación de bloqueo muestran la capacidad del modelo para filtrar tráfico potencialmente malicioso sin requerir de cambios en el código de las aplicaciones en los servidores reales. A su vez esto no implica que las vulnerabilidades dejen de existir en los servidores, sino que con F5 en la arquitectura se cuenta con un control adicional dedicado a la protección de aplicaciones.

Los resultados respaldan la hipótesis de investigación (H_1) y permiten rechazar la hipótesis nula (H_0) dado que se demostró que la implementación del modelo mejoro de

manera significativa la gestión del tráfico y mitigo eventos asociados a riesgos en aplicaciones web sin comprometer la operatividad de los servicios de DISPROVEF. Esta mejora se interpreta en términos de fortalecimiento de los mecanismos de mitigación en la capa de aplicación y de reducción del riesgo operativo asociado al tráfico web.

3.18 Discusión integral de los resultados y aportes del estudio

Los resultados obtenidos evidencian que la implementación progresiva de un Web Application Firewall configurado de manera optimizada permitió mejorar significativamente la gestión del tráfico y la capacidad de control de eventos asociados a riesgos en la capa de aplicación. La reducción del 78,40 % en los eventos alertados entre la fase de aprendizaje y la fase de ajuste demuestra que el proceso de optimización de políticas se vinculó con la disminución de falsos positivos y a una mejor interpretación del comportamiento legítimo de las aplicaciones. El detalle pormenorizado del razonamiento técnico, las firmas aplicadas y las excepciones justificadas para cada servicio web se encuentra documentado en la Memoria Técnica del Anexo E.

Un WAF con aprendizaje automático propuesto por Durmuşkaya y Bayraklı (2025) alcanzó un 93,27% de exactitud y un 93,13% de F1-score contra ataques XSS, inyección SQL, inclusión de archivos locales y de comandos. A diferencia del modelo evaluado en Disprovef este se desarrolló mediante tráfico híbrido y ataques controlados. Más allá de las cifras, ambos estudios comparten una conclusión: adaptar la detección al comportamiento del tráfico mejora la capacidad del WAF para separar lo legítimo de lo malicioso. Sin embargo, las métricas no son directamente comparables: el artículo evaluó la precisión de un algoritmo; mientras que en este estudio el nivel de protección efectivo tras la aplicación y optimización del modelo donde se logró controlar un 15,97% de

conexiones con comportamiento malicioso. La diferencia es bastante clara: un estudio se basó en ataques controlados contra aplicaciones vulnerables, el otro en tráfico real sobre servicios productivos donde lo prioritario era no interrumpir la operación.

Cujbă et al. (2026) desarrollaron un motor adaptativo de reglas que alcanzó tasas de detección del 98,1% y 98,3% con falsos positivos inferiores al 0,51%. El motor empleado en este estudio puede usarse como un proxy inverso para la inspección del tráfico HTTP en tiempo real e inclusive permite su uso en un entorno fuera de línea para casos de investigaciones forenses. En ambos casos los resultados apuntan a lo mismo a pesar de efectuarse en ambientes diferentes (laboratorio-controlado / entorno productivo real): afinar las reglas es lo que marca la diferencia en la eficacia operativa de un WAF.

Los resultados obtenidos son consistentes con investigaciones recientes sobre protección de aplicaciones web. Altamirano Rodríguez et al. (2026) en su investigación demostró que la implementación de un Web Application Firewall en entornos API REST incremento de forma significativa la capacidad de detección y mitigación de ataques web. Celik (2025) destaca el papel de las soluciones Web Application and API Protection (WAAP) como uno de los mecanismos más efectivos para reducir la exposición frente a las amenazas de aplicaciones. Aunque las investigaciones parten de una infraestructura diferente coinciden en que un WAF configurado de forma progresiva incrementa los niveles de seguridad de los servicios que son expuestos a internet.

Técnicamente, los controles en capa 7 aplicados de forma progresiva disminuyó la cantidad de alertas asociadas a tráfico legítimo (falsos positivos) y mejoró la clasificación de solicitudes inspeccionadas. Este resultado coincide con los principios del marco OWASP Top 10 (2021) establece que la reducción de riesgos en aplicaciones web

expuestas a Internet se apoya en: validación de solicitudes, control de accesos y configuración de servicios. El análisis confirma que la fase de ajuste es un punto crítico dentro del modelo propuesto para lograr una reducción de alertas, optimizar la clasificación de eventos descartando falsos positivos y la preparación para el filtrado de las solicites potencialmente riesgosas en la fase de protección Este resultado respalda enfoques metodológicos basados en la implementación progresiva y el ajuste iterativo de controles en entornos productivos.

La reducción del 78,40 % documentada en esta investigación corresponde estrictamente a la disminución de eventos de seguridad alertados, reflejando la optimización del modelo en la depuración de ruido técnico y en una clasificación más precisa de intentos de explotación asociados al OWASP Top 10. Metodológicamente el WAF mejoró el control sobre el tráfico HTTP/HTTPS y mitigo intentos de vulneración de los servicios expuestos de DISPROVEF actuando como un filtro para la contención de ataques, pero esto no significa que las aplicaciones o servidores dejaron de ser vulnerables, sino que se cuenta con un escudo adicional para la reducir la exposición. La corrección definitiva de las vulnerabilidades subyacentes continúa perteneciendo al ámbito de la remediación segura del software y al ciclo de desarrollo, los cuales constituyen procesos complementarios dentro de una estrategia integral de ciberseguridad.

A fin de profundizar la reducción observada, se efectuó una revisión de los eventos que dejaron de clasificarse como alertas durante la fase de ajuste considerando su comportamiento en el sistema. Este análisis permitió establecer que gran parte de estos eventos correspondía a falsos positivos asociados principalmente a solicitudes legítimas

que durante la fase de aprendizaje no se ajustaban con precisión a las políticas por defecto. Entre estos eventos se identificaron variaciones en parámetros, uso de métodos HTTP y otros patrones propios del funcionamiento de las aplicaciones que fueron mal clasificados.

La fase de ajuste permitió incorporar estos comportamientos dentro del perfil esperado reduciendo la generación de alertas sin afectar la operación normal de los servicios. La disminución de alertas asociadas a eventos de baja severidad no corresponde a una pérdida de sensibilidad del WAF sino a la optimización de los umbrales de detección lo cual mejoro la eficacia del sistema.

El afinamiento de las políticas de WAF redujo considerablemente el número de falsos positivos lo que conllevo a que el personal de TI de DISPROVEF encargado del análisis tenga menos carga operativa a fin de que los recursos se centren en el análisis del tráfico calificado como anómalo o malicioso de esta manera se priorizo los esfuerzos en la mitigación de eventos con mayor criticidad particularmente los relacionados con Injection y Broken Access Control gracias a esto se evidencio una reducción marcada de falsos positivos y no por la desactivación indiscriminada de mecanismos de protección por un mal afinamiento. Se logro la reducción del 78,40% lo que representa una mejora en la capacidad del sistema para discriminar entre tráfico legítimo y eventos potencialmente relevantes, aunque plantea la necesidad de gestionar de forma continua el equilibrio entre la reducción de falsos positivos y la capacidad de detección en entornos productivos.

En la fase de protección se evidencia la consolidación del modelo mediante la activación del bloqueo en las políticas logrando un 15,97 % de eventos bloqueados

confirmando la capacidad del sistema para interceptar solicitudes que infringen las políticas de seguridad llevando a la evolución del modelo desde el monitoreo hacia el control efectivo del tráfico y demuestra que el modelo no solo mejora la visibilidad, sino que habilita acciones concretas de mitigación en tiempo real.

Un análisis complementario de los eventos bloqueados permitió identificar su distribución según categorías alineadas con OWASP Top 10. Se observó que la mayor proporción correspondió a eventos asociados a Injection (166.428 registros), seguida por Broken Access Control (66.561) y Security Misconfiguration (39.929). En menor proporción se registraron eventos relacionados con validación de entradas (39.929) y categorías diversas (20.022). Esta distribución evidencia que el modelo actuó sobre vectores de ataque relevantes y comúnmente explotados en aplicaciones web, confirmando su capacidad para mitigar riesgos específicos y no únicamente tráfico anómalo de forma general.

Desde el plano organizacional el estudio demostró que es posible fortalecer la postura de seguridad sin comprometer la continuidad operativa de los servicios de un negocio u organización. La estabilidad observada durante la fase de protección evidencia que la implementación de controles de seguridad puede realizarse de manera controlada cuando se sustenta en un proceso previo de aprendizaje y ajuste a fin de evitar degradaciones en los servicios.

Seguir la evolución del sistema fase por fase fue posible gracias al diseño cuasi-experimental permitiendo tener trazabilidad y medir cada mejora con los resultados de las clasificaciones del tráfico y la capacidad de respuesta del modelo. Como aporte aplicado el modelo es una guía que puede ser usada para replicar el modelo en

organizaciones de características similares a DISPROVEF siguiendo la misma secuencia: diagnóstico del tráfico, ajuste progresivo de políticas y evaluación comparativa de resultados entre fases convirtiéndolo en un proceso medible, verificable y alineado con buenas prácticas de seguridad en aplicaciones web. Si bien el modelo es replicable su efectividad dependerá del contexto operativo y del nivel de madurez en seguridad de cada organización. Los resultados obtenidos durante la comparación de las fases del modelo confirman que la implementación del WAF optimizado progresivamente constituye una estrategia efectiva para mejorar la protección de los servicios expuestos de una organización.

CONCLUSIONES

Se implementó un modelo de mitigación basado en OWASP Top 10 mediante un Web Application Firewall (WAF) optimizado en los servicios web productivos de DISPROVEF bajo condiciones operativas reales desarrollado en fases de aprendizaje, ajuste y protección, esto permitió adaptar progresivamente las políticas de seguridad al comportamiento legítimo de las aplicaciones y reducir el riesgo sin comprometer la continuidad operativa.

Depuración de Ruido: El modelo logró una reducción del 78,40% de eventos alertados entre la fase de aprendizaje y ajuste confirmando la efectividad del proceso de afinamiento de las políticas de seguridad para eliminar falsos positivos permitiendo que el personal de TI se enfoque en amenazas reales. No implica la eliminación directa de vulnerabilidades OWASP Top 10 presentes en el código fuente de las aplicaciones sino una mejora en la detección, clasificación y mitigación del tráfico malicioso.

Mitigación Activa: Se alcanzó un 15,97% de bloqueo del tráfico durante la fase de protección correspondiente a solicitudes maliciosas asociadas a inyección y fallos de control de acceso, El WAF actuó como un control compensatorio que intercepto el tráfico antes de que llegue a los servidores reales sin afectar al 84,03% de tráfico legítimo necesario para la operación.

El F5 se implementó bajo una arquitectura Full Proxy actuando como punto central de inspección de tráfico HTTP/HTTPS entre la zona desmilitarizada DMZ y la red de servidores a fin de fortalecer la seguridad de aplicaciones expuestas a Internet frente a vulnerabilidades críticas del OWASP Top 10 particularmente en categorías como control de acceso, inyección y configuraciones inseguras.

Como aporte aplicado la investigación dejó un modelo replicable acompañado de lineamientos de despliegue, criterios de ajuste de políticas y una memoria técnica con las configuraciones documentadas de modo que pueda usarse como referencia para organizaciones con características similares que operan servicios web expuestos y requiera mejorar la seguridad en la capa de aplicación.

Los resultados obtenidos están limitados a las condiciones de DISPROVEF expuestas en la sección 3.8, El diseño cuasiexperimental sin grupo de control impide atribuir causalidad absoluta a la intervención es importante mencionar que fue desarrollado bajo la arquitectura de DISPOVEF por lo que replicar el modelo en otra organización exigiría ajustar las políticas al perfil de tráfico local a sus necesidades. Los datos cubren un trimestre sin evidencia sobre cómo evolucionaria la precisión del ASM más allá de ese punto ni sobre la degradación de las reglas si no se mantienen actualizadas.

El modelo es viable técnicamente y operó sin interrupciones y con resultados cuantificables sin embargo debe considerar el análisis costo-beneficio y un presupuesto estimado para licenciamiento, soporte y operación del WAF el cual oscila entre $6.160 y $9.320 siendo necesario para garantizar la sostenibilidad de la solución en el tiempo.

Reducir la exposición a riesgos en aplicaciones web fue posible gracias a una configuración progresiva, contextualizada y basada en tráfico real de DISPROVEF.

La memoria técnica resultante documenta las fases de implementación y las configuraciones aplicadas. Está pensada para que quien opere el WAF después conozca el porqué de cada configuración aplicada y facilitar su replicación en futuras implementaciones.

RECOMENDACIONES

Se recomienda institucionalizar el modelo OWASP–WAF como parte de la estrategia de seguridad de la organización, integrándolo con otros mecanismos de protección como sistemas de monitoreo, gestión de incidentes y controles de acceso, con el fin de fortalecer la postura de ciberseguridad de manera integral.

Mantener una revisión periódica de los eventos generados por el WAF para identificar cambios en el comportamiento del tráfico e identificar oportunamente la necesidad de aplicar ajustes en las políticas de seguridad o excepciones en firmas ya configuradas.

Mantener actualizadas las firmas de seguridad en alineación con las actualizaciones del OWASP Top 10 garantizando que el modelo de mitigación se adapte a nuevas amenazas.

Documentar y estandarizar los procedimientos de ajuste de políticas, validación funcional y gestión de excepciones, con el propósito de facilitar la operación, mantenimiento y replicabilidad del modelo en otros entornos organizacionales.

Replicar la implementación en organizaciones con diferentes arquitecturas de conectividad y seguridad para evaluar el comportamiento y la eficacia de las reglas del WAF a largo plazo con periodos de monitoreo más extendidos y diseños metodológicos más robustos. Además, cuando sea factible incorporar un grupo de control con el propósito de ampliar la evidencia de la efectividad del modelo y fortalecer su aplicabilidad en diversos contextos organizacionales.

Se recomienda que DISPROVEF considere el presupuesto estimado y el análisis costo-beneficio presentados en esta investigación como insumo para planificar futuras

inversiones en la protección de sus aplicaciones web mediante un Web Application Firewall.

Mantener la estrategia del modelo y sus fases de implementación: aprendizaje basada en el comportamiento del tráfico real, ajuste progresivo de las políticas y la activación de los mecanismos de bloqueo. Definir indicadores de desempeño que evalúen de forma continua la operación del modelo y su capacidad de respuesta ante cambios en el tráfico cubriendo al menos la eficiencia del sistema, la gestión de eventos y la actualización de políticas para que sea posible identificar y corregir degradaciones de la plataforma antes de que afecten la protección ver anexo F.

Es importante fortalecer las capacidades técnicas del personal responsable mediante programas de capacitación continua en administración de WAF, análisis de eventos de seguridad y gestión de vulnerabilidades, asegurando la sostenibilidad del modelo implementado. A su vez mantener actualizada la memoria técnica documentada en el Anexo E, registrando de forma sistemática cada ajuste realizado sobre las políticas, firmas, excepciones y parámetros de configuración del WAF para conservar la justificación técnica de los cambios efectuados, con el fin de garantizar la trazabilidad, sostenibilidad y mejoras del modelo de mitigación frente a cambios en las aplicaciones y las amenazas emergentes.

REFERENCIAS

Abu Laila, D., Obeidat, I. M., Aman, M., Altubaishe, B. Z., Odeh, M., & Samara, G. (2026). An intelligent web application firewall fuzzing framework integrated with blockchain technology for secure payload analysis and traceability. Scientific Culture, 12(1). https://doi.org/10.5281/zenodo.18092759

Alaoui, R. L., & Nfaoui, E. H. (2022). Deep Learning for Vulnerability and Attack Detection on Web Applications: A Systematic Literature Review. *Future Internet*, 14(4), 118. https://doi.org/10.3390/fi14040118

Altamirano Rodríguez, B. S., Cepeda Altamirano, C. L., Cadena Paillacho, C. A., y Flores Cruz, G. S. (2026). Diseño e implementación de un entorno de pruebas para evaluar la efectividad de un Web Application Firewall (WAF) en la detección y mitigación de ataques de API REST [Tesis de maestría, Universidad Internacional del Ecuador]. Repositorio Digital UIDE. https://repositorio.uide.edu.ec/handle/37000/8883

Alotaibi, F., & Vassilakis, V. (2023). Toward an SDN-based web application firewall. IEEE Access, 11, 12345–12360.

Álava Zambrano, J., et al. (2022). Análisis del OWASP Top 10 en sistemas web modernos. Revista de Ingeniería Informática, 10(3), 606–635.

Arévalo Ipiales, M. (2024). Implementación de un WAF basado en ModSecurity para la protección de aplicaciones web [Tesis de grado]. Universidad.

Baviskar, D. N., Mane, S. M., Shingan, N. R., Kulkarni, S. S., & Kshirsagar, R. R. (2025). AI-Powered Smart-Shield Web Application Firewall System. *International*

Journal of Engineering Development and Research, 13(1). https://rjwave.org/ijedr/papers/IJEDR2601342.pdf

Cárdenas Rosero, J. (2023). Implementación de FortiWeb para mitigación de vulnerabilidades OWASP Top 10 [Tesis de maestría]. Universidad.

Cárdenas Rosero, J., Guevara Vega, P., & Landeta-López, M. (2025). Website protection: An evaluation of the web application firewall [Tesis de posgrado]. Universidad.

Celik, O. (2025). Leadership Compass: Web Application and API Protection. KuppingerCole Analysts AG.

Chindrus, M., & Caruntu, C. (2025). Deep learning techniques for web application firewall optimization. Journal of Network Security, 18(2), 101–120.

Cujbă, M.-C., Chiru, C.-G., Bica, I., & Țiță, I. (2026). *An adaptive rule-based engine for application-layer security*. **Applied Sciences, 16**(11), 5220. https://doi.org/10.3390/app16115220

Durmuşkaya, M. E., & Bayraklı, S. (2025). Web application firewall based on machine learning models. PeerJ Computer Science, 11, e2975. https://doi.org/10.7717/peerj-cs.2975

European Union Agency for Cybersecurity (ENISA). (2021). Cybersecurity for SMEs: Challenges and recommendations. https://www.enisa.europa.eu

European Union Agency for Cybersecurity (ENISA). (2023). Cybersecurity guidelines and resilience strategies. https://www.enisa.europa.eu

F5 Networks. (2024). BIG-IP Application Security Manager (ASM) documentation. https://www.f5.com

F5, Inc. (2026). BIG-IP advanced WAF. https://www.f5.com/products/big-ip-services/advanced-waf

Flament, B., et al. (2022). Design and implementation of a web application firewall using Apache and ModSecurity. International Journal of Information Security, 21(4), 567–580.

Fortinet. (2025). How WAFs help protect against OWASP threats. https://www.fortinet.com/resources/cyberglossary/owasp-web-application-firewall

GuidePoint Security. (2024). F5 BIG-IP VE pricing and security solutions. https://www.guidepointsecurity.com

IBM. (2026). *2026 X-Force Threat Intelligence Index*. https://www.ibm.com/reports/threat-intelligence

IBM Security. (2023). *Cost of a data breach report 2023: Global analysis*. IBM Corporation. https://www.ibm.com/reports/data-breach

Liu, Y., & Chen, X. (2021). Re-Transformer model for efficient sequence processing. IEEE Transactions on Neural Networks, 32(5), 483–496.

Macías Mendoza, J., et al. (2025). Secure software development lifecycle and risk reduction in web applications. Journal of Software Engineering, 19(4), 519–530.

Notoma, O. K. (2025). A holistic approach to cybersecurity risk management and compliance in the cloud: Recommendations for development of a user-friendly framework for small businesses [Disertación doctoral, Purdue University]. Purdue University Graduate School.

OWASP Foundation. (2021). OWASP Top 10: The ten most critical web application security risks. https://owasp.org/www-project-top-ten/

Román-Gallego, J., López, J., & Ramírez, M. (2023). Artificial intelligence web application firewall for advanced detection of web injection attacks. Journal of Cybersecurity Research, 12(3), 45–60.

Sameh, Ahmed., y Selim, Sahar. (2024). Adaptive Dual-Layer Web Application Firewall (ADL-WAF) Leveraging Machine Learning for Enhanced Anomaly and Threat Detection. arXiv preprint arXiv:2401.16104. https://doi.org/10.48550/arXiv.2401.16104

Shaheed, R., & Kurdy, M. (2022). Machine learning-based web application firewall for attack detection. Computers & Security, 115, 102600.

Tadavarti, L. K., & Babu, A. R. (2024). Improving protection of web applications through a machine learning–based firewall framework. International Journal of Engineering Sciences. https://theaspd.com/index.php/ijes/article/view/11769

Valle, R., & Adachi, K. (2024). Scrubbing centers and DDoS mitigation strategies. Journal of Network Defense, 9(2), 1157–1259.

Verizon Business. (2025). *2025 Data Breach Investigations Report (DBIR).* https://www.verizon.com/business/resources/reports/dbir/

WorldTech IT. (2024). F5 BIG-IP Virtual Edition pricing overview. https://www.worldtechit.com

ANEXOS

Anexo A: Ficha de Validación por Juicio de Expertos

FICHA DE VALIDACIÓN DE INSTRUMENTOS

Título del estudio:

Modelo de mitigación OWASP Top 10 mediante Web Application Firewall optimizado, aplicado a los servicios productivos de DISPROVEF

Instrumentos evaluados:

- Matriz de operacionalización de variables
- Checklist de validación operativa
- Criterios de clasificación de eventos OWASP
- Indicadores de medición de eficacia

Perfil del experto:

Nombre: _____

Formación académica: _____

Años de experiencia en ciberseguridad: _____

Especialidad: _____

INSTRUCCIONES

Valore cada criterio según la siguiente escala:

Valor	Interpretación
1	Deficiente
2	Regular
3	Adecuado

Valor Interpretación

4 Excelente

EVALUACIÓN

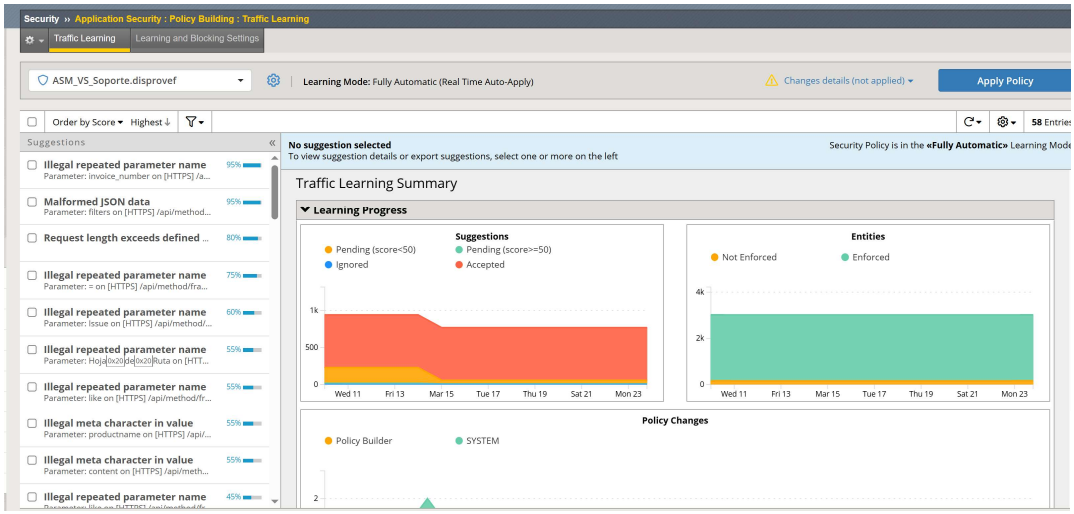
Criterio	**Puntuación (1–4)**
Relevancia del instrumento respecto a los objetivos	___
Coherencia entre variable e indicador	___
Suficiencia de los indicadores	___
Claridad técnica y redacción	___

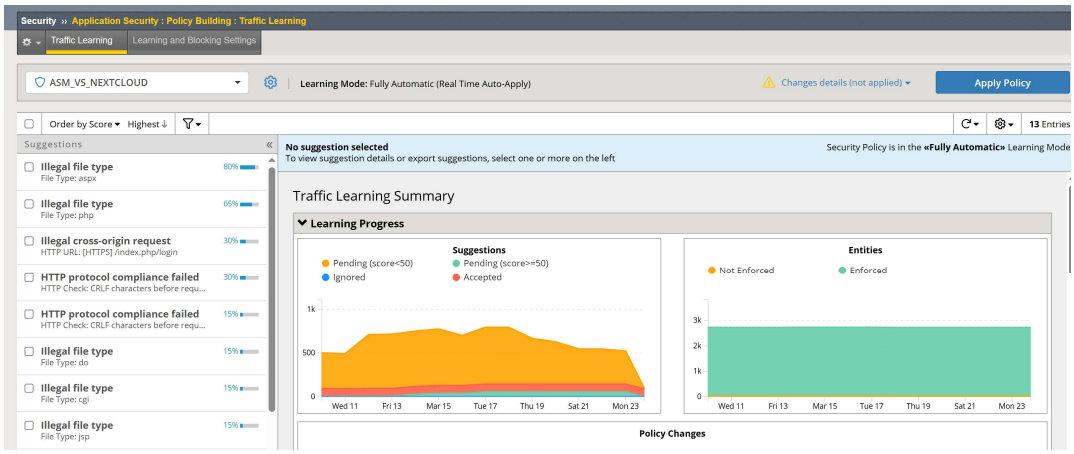
Observaciones del experto:

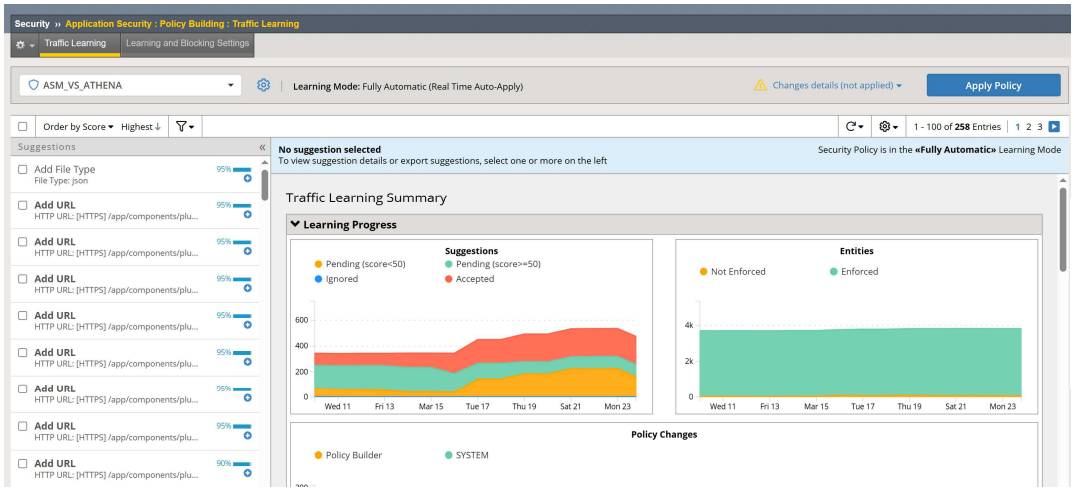
Firma: _____

Fecha: _____

Anexo B: Panel de aprendizaje de tráfico del Web Application Firewall (WAF)






Security ›› Application Security : Policy Building : Traffic Learning
Traffic Learning
Learning and Blocking Settings
ASM_VS_ATHENA
Learning Mode: Fully Automatic (Real Time Auto-Apply)
Changes details (not applied)
Apply Policy
Order by Score
Highest
1 - 100 of 258 Entries 1 2 3
Suggestions
Add File Type
File Type: json
Add URL
HTTP URL: [HTTPS] /app/components/plu...
No suggestion selected
To view suggestion details or export suggestions, select one or more on the left
Security Policy is in the «Fully Automatic» Learning Mode
Traffic Learning Summary
Learning Progress
Suggestions
Pending (score<50)
Pending (score>=50)
Ignored
Accepted
Entities
Not Enforced
Enforced
Wed 11
Fri 13
Mar 15
Tue 17
Thu 19
Sat 21
Mon 23
Policy Changes
Policy Builder
SYSTEM

Anexo C: Evidencia de eventos analizados a partir de logs del WAF

Los siguientes registros corresponden a extractos de logs generados por el Web Application Firewall durante la fase de operación. Se presentan como evidencia del origen real de los eventos utilizados en la evaluación de concordancia inter-observador.

Figura 10

Extracto de logs del WAF utilizados en el análisis

```
Mar 24 13:33:23 waf.disprovef.com ASM:unit_hostname="waf.disprovef.com"
management_ip_address="[redacted]" attack_type="Information Leakage"
violations="Illegal HTTP status in response" support_id="123456789"
request_status="blocked" response_code="500" method="GET"
uri="/index.php/[redacted]/api/v2/notifications"

Mar 24 13:35:10 waf.disprovef.com ASM:unit_hostname="waf.disprovef.com"
request_status="passed" response_code="207" method="PROPFIND"
uri="/remote.php/dav/[redacted]/" user_agent="mirall/3.5.0"

Mar 24 13:36:45 waf.disprovef.com ASM:unit_hostname="waf.disprovef.com"
request_status="passed" method="POST" content_type="application/json"
payload="Unexpected character ('<' (code 60))"
uri="/rest/plugins[redacted]/list/remote"

Mar 24 13:38:02 waf.disprovef.com ASM:unit_hostname="waf.disprovef.com"
request_status="passed" method="GET"
uri="/ocs/v2.php/[redacted]/v2/notifications"
user_agent="Mozilla/5.0"
```

Nota. Extractos de logs del WAF F5 BIG-IP que evidencian eventos clasificados como falsos positivos, tráfico benigno atípico y eventos potencialmente maliciosos durante la fase de operación.

Anexo D: Configuración de alertas de monitoreo en F5 BIG-IP

A continuación, se presenta un extracto de la configuración implementada en la plataforma F5 BIG-IP para la detección de eventos asociados al uso de CPU, memoria y almacenamiento, mediante reglas personalizadas basadas en patrones de registro.

Figura 11

Monitoreo de recursos y envío de alertas

```
alert BIGIP_CPU-ISSUE-CUSTOM "(tmm.*busy|cpu.*starvation|CPU.*starvation|overload|scheduler.*delay|Scheduler.*delay)" {
snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.30";
email toaddress="soporteti@disprovef.com.ec"
fromaddress="alarmainfra@disprovef.com.ec"
body="EN EL EQUIPO F5 ALERTA DE EVENTO RELACIONADO A CPU"
}

alert BIGIP_MEMORY-ISSUE-CUSTOM "(memory.*low|Memory.*low|out of memory|Out of memory|malloc failed|Malloc failed|swap.*high|Swap.*high|oom|OOM)" {
snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.31";
email toaddress="soporteti@disprovef.com.ec"
fromaddress="alarmainfra@disprovef.com.ec"
body="EN EL EQUIPO F5 ALERTA DE EVENTO RELACIONADO A MEMORIA"
}

alert BIGIP_DISK-WARNING-CUSTOM "(Disk partition (.*) (warning|reached|high|exceeded))" {
snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.25";
email toaddress="soporteti@disprovef.com.ec"
fromaddress="alarmainfra@disprovef.com.ec"
body="EN EL EQUIPO F5 ALERTA DE ESPACIO EN DISCO (WARNING)"
}

alert BIGIP_DISK-CRITICAL-CUSTOM "(Disk partition (.*) (critical|full|100%|no space|out of space))" {
snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.26";
email toaddress="soporteti@disprovef.com.ec"
fromaddress="alarmainfra@disprovef.com.ec"
body="EN EL EQUIPO F5 ALERTA CRITICA DE ESPACIO EN DISCO"
}
```

Nota. Se configuro el monitoreo de alertas por OID para consumo de recursos en caso de activación se envía la notificación por correo al personal de soporte para su revisión.

Anexo E: Muestra representativa de eventos utilizados en el análisis de concordancia inter-observador

El proceso de optimización del modelo OWASP–WAF en DISPROVEF permitió transitar de una postura de seguridad genérica a una solución personalizada, equilibrando la protección de la capa de aplicación con la continuidad de los servicios críticos. A continuación, se detalla el razonamiento analítico aplicado en la configuración de excepciones y reglas, agrupado por sus objetivos estratégicos:

1. Garantía de Continuidad Operativa y Flujos de Negocio

Para asegurar que el WAF no se convirtiera en un obstáculo para la operación, se realizaron ajustes específicos en los umbrales de carga y métodos permitidos:

- Gestión de Evidencias (Soporte): Se incrementó el umbral de carga útil (*Request Size*) a 15 MB en el portal de Soporte Técnico. Esta medida fue necesaria para permitir el envío de capturas de pantalla y registros comprimidos fundamentales para la resolución de incidentes, mitigando simultáneamente riesgos de desbordamiento de búfer.
- Sincronización Documental y Correo (Nextcloud y Zimbra): Se habilitó el método PROPFIND en Nextcloud para normalizar el flujo del agente *mirall/3.17.1*, el cual utiliza protocolos WebDAV para la sincronización corporativa. Asimismo, en Zimbra, se ajustó el Rate Limiting a 15 peticiones/segundo para el protocolo ActiveSync, garantizando la disponibilidad del correo en dispositivos móviles frente a ráfagas de tráfico legítimo.
- Plataforma ERP (Zlibra ERP): Se ajustaron los límites de *Payload* para evitar bloqueos "Illegal request length" debido a la alta cantidad de datos procesados en la generación de reportes mensuales y cierres contables ya que interrumpía la facturación masiva.

2. Reducción de Ruido y manejo de Falsos Positivos

El análisis de eventos en la fase de ajuste fue clave en la reducción de alertas de alta severidad alcanzando un 78,40% mediante excepciones granulares:

- Facturación Electrónica (Zlibra ERP): Se aplicaron excepciones a firmas de Inyección SQL (ID: 200000147) en parámetros específicos de los paquetes XML. El ajuste fue vital para no interrumpir el flujo comercial debido a bloqueos por caracteres especiales mal interpretados teniendo gran cantidad de eventos registrados 166.000+.
- Telemetría y Soporte (Athena y Soporte): En Athena MDM, se estandarizaron los valores en parámetros de coordenadas GPS (latitud y longitud) para permitir el uso de decimales y signos negativos esenciales para el rastreo y seguimiento de la flota móvil. En cuanto al portal de soporte se crearon excepciones para firmas de XSS en el campo ticket_description para no generar alertas por una categorización incorrecta y permitir al personal de TI documentar trazas de código y errores técnicos evidenciados con los usuarios.
- Sincronización de Clientes (Nextcloud): Se implementaron excepciones para firmas de Inyección de JavaScript (ID: 200101814), ya que el motor del WAF clasificaba erróneamente la sincronización de archivos .js de configuración del cliente de escritorio.

3. Endurecimiento de la Postura de Seguridad (*Hardening*)

A pesar de las flexibilizaciones operativas, se fortaleció la seguridad mediante controles compensatorios directos donde la remediación del código no era inmediata:

- Exfiltración de datos (Nextcloud y Athena): Se bloqueó el acceso a archivos con extensiones de base de datos local (.sqlite) y copias de seguridad (.bak) y al directorio de desarrollo /.idea/ reduciendo la exposición de información sensible y componentes de las aplicaciones.
- Protección contra Fuerza Bruta: Se configuraron límites de intentos de autenticación en el portal de Soporte para mitigar ataques de *Credential Stuffing*

y evitar accesos no autorizados a la plataforma. Para Athena se activó el bloqueo por longitud de solicitudes “Illegal POST data length” para controlar cargas anómalas que puedan derivar en ataques de denegación de servicio dirigidas a sus APIs.

- Fortalecimiento de sesiones: Se forzó la inyección de atributos Secure y HttpOnly en las cookies de Soporte impidiendo su transmisión por canales no cifrados y su acceso mediante scripts para proteger las sesiones administrativas. También fue configurado el bloqueo hacia las respuestas con errores HTTP 500 en Athena para evitar la fuga de información técnica hacia atacantes externos.

Anexo F: Indicadores de desempeño para la sostenibilidad del modelo

En la Tabla 12 se presentan los principales indicadores propuestos, junto con su método de medición y frecuencia de seguimiento.

Tabla 12

Indicadores de desempeño para la sostenibilidad del modelo OWASP–WAF

Indicador	Descripción	Método de medición	Frecuencia
Tiempo promedio de respuesta a falsos positivos	Tiempo requerido para analizar y resolver eventos clasificados incorrectamente	Revisión de tickets o registros de eventos	Mensual
Frecuencia de revisión de reglas y excepciones	Número de revisiones realizadas sobre políticas del WAF	Historial de configuración del WAF	Trimestral
Tasa de falsos positivos	Proporción de eventos incorrectamente clasificados respecto al total de eventos detectados	Análisis de logs del WAF	Mensual
Tiempo de actualización de políticas	Tiempo transcurrido entre la detección de una nueva amenaza y la aplicación de ajustes en las reglas del WAF	Registro de cambios en la configuración	Trimestral

Anexo G: Autorización para uso de información institucional

DISPROVEF
Prevención y solución

VETEQUIPOS

Guayaquil, 15 de noviembre de 2025

Ingeniero
Adrian Apunte
COORDINADOR DE SISTEMAS, DESARROLLO Y TECNOLOGÍA
DISPROVEF ECUADOR S.A.

Presente.-

Asunto: Solicitud de autorización para uso de información institucional con fines académicos

De mi consideración:

Yo, **John Jairo Apunte Caspi**, estudiante de la Maestría en Ciberseguridad de la Universidad Estatal Península de Santa Elena (UPSE), me permito dirigirme a usted con la finalidad de solicitar la autorización para el uso de información institucional de DISPROVEF ECUADOR S.A., como parte del desarrollo de mi trabajo de titulación denominado **"Modelo de mitigación OWASP Top 10 mediante Web Application Firewall optimizado, aplicado a los servicios productivos de DISPROVEF"**, cuya finalidad es implementar un modelo de mitigación de vulnerabilidades OWASP Top 10 mediante un Web Application Firewall configurado de manera optimizada, aplicado a los servicios productivos expuestos a Internet de DISPROVEF, con el fin de fortalecer su seguridad y garantizar la continuidad operativa.

Para el desarrollo de la investigación podrá ser necesario acceder a información institucional relacionada con el alcance del proyecto, incluyendo diagramas de arquitectura tecnológica, configuraciones de equipos, direccionamientos de red y demás información pertinente para sustentar académicamente el trabajo de titulación.

Por lo expuesto, y con el debido respeto, solicito a usted se sirva autorizar y otorgar su consentimiento para el uso de información institucional estrictamente necesaria para el desarrollo de la investigación, garantizando que dicho tratamiento de datos será realizado con fines exclusivamente académicos, manteniendo en todo momento la confidencialidad, integridad y protección de la información, en estricto cumplimiento de la normativa vigente, especialmente lo establecido en la Ley Orgánica de Protección de Datos Personales (LOPDP). Cabe indicar que la información recopilada será tratada de manera agregada, anonimizada y no será divulgada ni utilizada con fines distintos a los establecidos en el presente estudio, precautelando en todo momento los intereses y la seguridad de la institución.

Agradezco de antemano la atención brindada a la presente solicitud y el apoyo institucional para el desarrollo de esta investigación.
Atentamente,

John Jairo Apunte Caspi
C.C. 092955227-1

Recibido
15 Nov 2025
13:40

DISPROVEF
Prevención y solución

VETEQUIPOS

Guayaquil, 20 de noviembre de 2025

Señor
John Jairo Apunte Caspi
Estudiante de la Maestría en Ciberseguridad
Universidad Estatal Península de Santa Elena – UPSE

Presente.-

Asunto: Autorización para uso de información institucional con fines académicos

De mi consideración:

En atención a su solicitud de fecha 15 de noviembre de 2025, mediante la cual pone en conocimiento que se encuentra cursando la Maestría en Ciberseguridad en la Universidad Estatal Península de Santa Elena (UPSE), y considerando el desarrollo de su trabajo de titulación denominado: **"Modelo de mitigación OWASP Top 10 mediante Web Application Firewall optimizado, aplicado a los servicios productivos de DISPROVEF"**, me permito manifestar lo siguiente:

Esta Coordinación **AUTORIZA** el uso de información institucional estrictamente necesaria para el desarrollo de su investigación académica, siempre y cuando dicho acceso, tratamiento y análisis de la información se realice bajo criterios de confidencialidad, responsabilidad y uso adecuado.

Se deja expresa constancia de que la información deberá ser utilizada exclusivamente con fines académicos, evitando su divulgación, reproducción o uso indebido, en cumplimiento de la normativa vigente, en especial lo dispuesto en la Ley Orgánica de Protección de Datos Personales (LOPDP), así como de las políticas internas de seguridad de la información de DISPROVEF ECUADOR S.A.

Adicionalmente, se dispone que la información sensible o crítica sea debidamente anonimizada o tratada de forma agregada, garantizando la protección de la información institucional y evitando cualquier riesgo que pudiera afectar la integridad, confidencialidad o disponibilidad de los activos de información.

Finalmente, se solicita que una copia del trabajo de titulación y de los resultados obtenidos en el marco de la investigación sea compartida con la organización, a fin de que estos contribuyan al fortalecimiento de la seguridad de la información y a la mejora continua de los servicios tecnológicos institucionales.

Sin otro particular, reitero mi apoyo a las iniciativas académicas que aporten al fortalecimiento de la seguridad de la información y al desarrollo institucional.
Atentamente,

Adrian Apunte
Coordinador de Sistemas, Desarrollo y Tecnología
DISPROVEF ECUADOR S.A.