# WAF

## LA FORMA MÁS RÁPIDA Y EFICIENTE DE PROTEGER *TU SITIO WEB O E-COMMERCE*

Servicios web disponibles en todo momento de forma fácil y segura.

Junio 2020

www.ciberseguridad.advance-nt.com

# Tabla de contenido.


01 **Introducción**..... (03)

02 **México, el país con mayor número de fraudes en e-commerce.**

E-Commerce en México frente al COVID-19.....(04)

03 **La importancia de mantener disponible tu portal de negocios.**

Mantén disponible tu portal de negocios .....(06)

¿Cómo proteger tu portal de negocios o e-Commerce? ..... (06)

¿Qué es un WAF y cómo funciona?.....(07)

04 **¿Cómo elegir un WAF?**

Características que debe cumplir un WAF.....(08)

05 **Tipos de WAF**

Algunas fortalezas y debilidades de algúnos WAF en el mercado.....(14)

Radware como una de las empresas líderes en protección de servicios web con WAF..... .. (15)

CloudWAF.....(15)

06 **Casos de éxito.** ..... (16)

07 **Para finalizar** ..... (17)

01

# Introducción

El propósito de este documento electrónico es dar a conocer la problemática de ataques cibernéticos a la cual se están enfrentando hoy en día las empresas que tienen un sitio web o eCommerce como elementos fundamentales de su proceso comercial, así como, la relevancia que adquiere un WAF (Web Application Firewall) para la seguridad informática y la prevención de pérdidas económicas, reputación de marca e información relevante de la compañía y sus clientes.

Iniciaremos exponiendo un panorama general de los eventos de fraude informático llevados a cabo en México, veremos algunas estadísticas a nivel internacional, principalmente en eCommerce, así como, el comportamiento de este fenómeno durante la pandemia del Coronavirus.

Aprenderás qué es un WAF, la importancia de implementarlo en tu empresa, los diferentes tipos que existen, así como, las características esenciales que un WAF debe tener para mantener los niveles más elevados de eficacia en materia de seguridad para una continua disponibilidad de las aplicaciones web de tu empresa.

Por último, te compartiremos nuestra experiencia colaborando con Radware para dar solución a este problema y mencionaremos algunos casos de éxito.

Este eBook ha sido realizado por un grupo de expertos en materia de Ciberseguridad con el fin de apoyar a los objetivos de Tecnología de la Información y Seguridad Informática en las empresas.

Gracias por tu atención.

02

eCommerce 40% al alza en México a partir del COVID-19

# E-Commerce en México frente al COVID-19

En México y el mundo, las medidas para frenar la pandemia del Coronavirus (COVID-19) ha ocasionado gran impacto en las economías, representando una aceleración de la transformación digital en las empresas y beneficiando de manera tajante el uso de plataformas de eCommerce o comercio electrónico. Lo que ha significado para nuestro país un incremento del 40% en las ventas en línea, estimación que es 10% mayor a lo que se había previsto antes de la crisis sanitaria; en base a un escenario de crecimiento real de 24% y 36% por año con una cifra de 621,000 millones de pesos en 2019.

Para 2020 las estimaciones en cifras por estas transacciones pueden alcanzar un valor de 864.000 millones de pesos, de acuerdo a lo expuesto por Oliver Aguilar; Gerente de Investigación, Consumo y Telecomunicaciones de la International Data Corporation (IDC).

De acuerdo a la consultora Nielsen, esto es parte de un proceso de 6 etapas, donde del comportamiento del consumidor se relaciona directamente a preocupaciones con el brote del COVID-19 y la vida restringida donde el eCommerce representa la vía más sencilla para tener acceso a productos esenciales y de entretenimiento. Algo que sin duda dejará huella en los patrones de comportamiento del consumidor, haciendo de esto una nueva normalidad.

# ¿Sabías que México es uno de los países con más fraudes en e-Commerce a nivel mundial?

De acuerdo con *Clearsale*, empresa que emplea Inteligencia artificial para detectar este tipo de problemas, todos los días se realizan miles de transacciones en línea a nivel mundial, pero en México, el riesgo de fraude para las empresas y los usuarios es mayor, pues es el país con mayor número de intentos de vulneración, seguido por Brasil y Rusia.

Al cierre del 2017, las afectaciones generadas provocaron pérdidas por 3,700 millones de pesos, según cifras *Condusef*.

Sumado a esto, la pandemia del Coronavirus (COVID-19) está teniendo un impacto casi incalculable en este sentido, pues a medida que crece el comercio electrónico, aumentan las amenazas de fraude en portales de negocios electrónicos, de los cuales, cuatro de cada 10 tienen éxito. Por otro lado, es importante resaltar que existen infinidad de aplicaciones web que puede acabar con un portal web en cuestión de segundos.

Cifras de Radware, empresa especialista en soluciones de Ciberseguridad, expone que del 100% de las amenazas cibernéticas que existen en internet, el 45% van dirigidas a la interrupción del servicio de web.
¿Cómo se han visto afectadas las empresas?

*Radware, 2018-2019 Global Application and Network Security Report*

- 42% Experiencia negativa del cliente
- 36% Pérdida de reputación de la marca
- 22% Pérdida de clientes

## ¿Has calculado la pérdida económica que tendría tu empresa si cae tu sitio web por unos instantes?

Imagina que tus servicios se ven interrumpidos por escasos 10 minutos, ¿cuánto dinero perderías?. Solo imagina si tu portal de negocios recibe hoy en día 5,000 peticiones de usuarios por minuto para adquirir productos o servicios. Las pérdidas serían millonarias.

Por otro lado, para los usuarios el principal riesgo es que un tercero use los datos de su tarjeta y con ella, se realicen compras en más de 200 portales web de forma simultánea.

03

Un WAF protege tu sitio web o eCommerce , manteniendo su disponibilidad y protegiendo el tráfico de información.

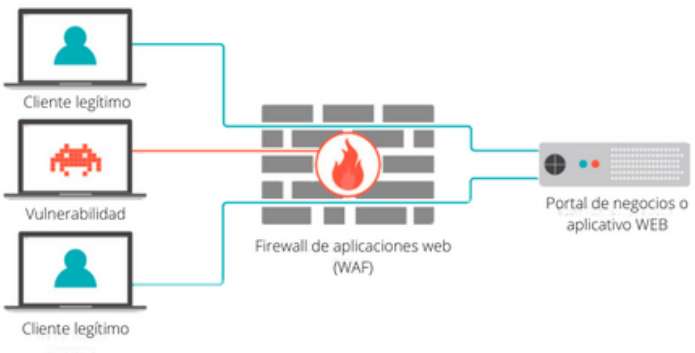
## ¿Cómo proteger tu portal de negocios o eCommerce?

Una medida eficiente y sencilla para proteger tu web, eCommerce o blog (sea cual sea el CMS empleado), ante todo tipo de ataques que van desde la denegación de servicio (DoS) a spambots, es en definitiva, un WAF, que actúa como medida preventiva de seguridad para proteger lo que los firewall tradicionales no serían capaces de detectar.

Un firewall de aplicaciones web o WAF es un sistema de protección que que esta basado en soluciones On-Premise o en la nube dando la capacidad de mantener tus servicios web (portales de negocio, y tiendas en línea) siempre disponibles incluso bajo un ataque cibernético.

Una robusta solución en WAF incluye prevención de intrusiones y entrega de contenido para garantizar la integridad, confidencialidad y la alta disponibilidad de tu portal de negocios web.

## ¿Cómo funciona un WAF?




Un WAF trabaja como intermediario entre usuarios externos (ej. usuarios de Internet) y las aplicaciones web. Esto quiere decir que las peticiones y respuestas son analizadas por el WAF antes de que éstas lleguen a las aplicaciones web o a los usuarios de las aplicaciones.

De no detectarse peticiones web maliciosas o alguna anomalía, entonces las peticiones y respuestas HTTP fluyen con normalidad. Todo el proceso de análisis y protección ocurre de forma transparente para los usuarios, evitando así, interferir con las operaciones normales de las aplicaciones web.

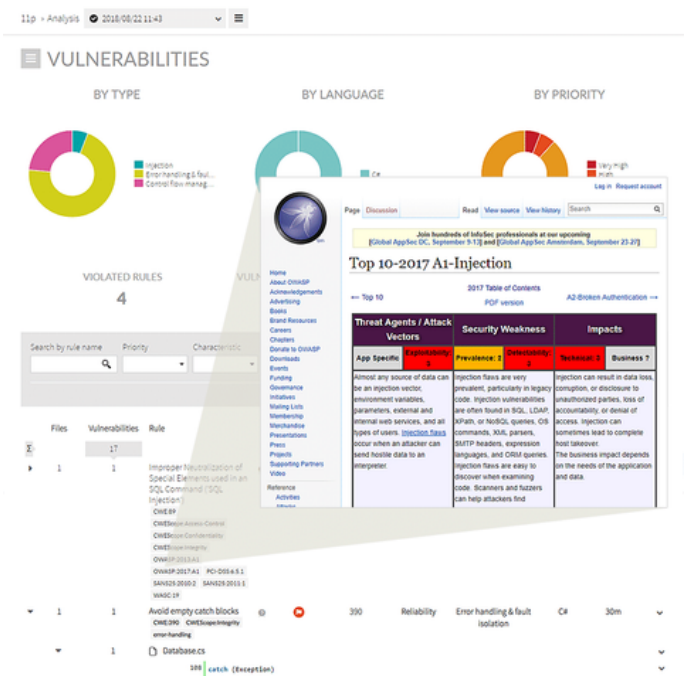
## ¿Cómo elegir el mejor WAF para mi empresa?

Al seleccionar una solución de WAF para proteger tus servicios web, debes priorizar las siguientes características, las cuales se detallan más adelante:

1. Protección contra los 10 principales riesgos según OWASP.
2. Protección con modelo positivo o negativo.
3. Cumplimiento de las normas PCI
4. Alto rendimiento
5. Adminstración desde cualquier punto
6. Prevención contra vulnerabilidades
7. Solución fácil de usar.

# Protección contra los 10 principales riesgos según OWASP

Open Web Application Security Project (OWASP) es una organización internacional sin fines de lucro que analiza, documenta y difunde principios para el desarrollo seguro de aplicaciones web y produce una lista de los principales riesgos críticos de seguridad de las aplicaciones:




1.- Inyección

2.- Pérdida de autenticación

3.- Exposición de datos confidenciales

4.- Ataques de entidades externas (XXE)

5.- Secuencia inyección de comandos maliciosos (XSS)

6.- Configuración incorrecta de seguridad

7.- Ausencia de control de acceso a nivel de las funciones

8.- Redirecciones y reenvíos no válidos

9.- Uso de componentes con vulnerabilidades conocidas

10.- Registro y monitoreo insuficientes

Para obtener más información sobre los riesgos de seguridad de aplicaciones web más importantes de OWASP, puedes consultar la siguiente liga. https://bit.ly/3cOcu7f

## OWASP Top 10 no es suficiente

Si bien el OWASP Top 10 sigue siendo un caso de uso básico, debes esperar que el WAF proporcione protección contra una serie cada vez más amplia de ataques de aplicaciones, incluidos ataques basados en API, en el lado del cliente ataques e incluso bots. Además, la adopción de DevSecOps significa que los WAF deben integrarse con el resto de la infraestructura de seguridad y ayudar a proteger la integridad del portal web.

Es por ello, que te recomendamos contemplar los siguientes aspectos a la hora de elegir un proveedor:

- Los proveedores de WAF deben proporcionar un nuevo enfoque integrado, permitiendo a los usuarios importar archivos de configuración de API en múltiples formatos y detectar encabezados y verificaciones de referencia.

- Protección sólida contra ataques de día cero y amenazas emergentes requiere una amplia función de inteligencia combinada con la capacidad de generar automáticamente políticas de protección. Una buena solución WAF no solo debe ser inteligente ante las amenazas, sino también a la rapidez con que esa inteligencia analiza y protege de las amenazas..

- Busca soluciones que ofrecen múltiples alternativas de integraciones con herramientas DevOps para adaptarse al proceso de implementación en la seguridad de tu portal web.


## Protección en modelo positivo o negativo

El WAF debe admitir tanto un modelo de seguridad positivo como negativo.

**Modelo de Seguridad Negativo**: Se basa en la idea de que todos los accesos a los recursos están permitidos, excepto aquellos que sean prohibidos. Es decir, todo lo que no está prohibido, se le da acceso. En un ejemplo podemos decir que un antivirus permite pasar todos los archivos adjuntos a un correo electrónico excepto aquellos que contienen virus. Algunos WAF emplean esta solución mediante la utilización de listas negras, evitando los ataques conocidos a aplicaciones basadas en web.

**Modelo de Seguridad Positiva**: Consistente en justo la idea contraria del modelo negativo, todo aquello que no está permitido, está prohibido. Un ejemplo muy claro es un firewall de red en el que permitimos el tráfico mediante reglas y denegamos todo lo demás, los mecanismos de autenticación permiten el acceso a aquellos usuarios cuya contraseña es válido y deniegan a todos los demás.

Por otro lado, un WAF debe contar la capacidad de poder frenar ataques de día cero o desconocidos, estos ataques son amenazas que aun no existen y que ningún sistema de protección conoce y pueden afectar de manera significativa al portal web. Los WAF deben tener la capacidad de crear politicas de seguridad en tiempo real para bloquear este tipo de vulnerabilidades

## Cumplimiento de las normas PCI

Los ataques maliciosos diseñados para robar información confidencial están creciendo y se producen a diario cada vez más violaciones a la seguridad y de portales de negocios web o e-commerce.

Si tu portal de e-commerce procesa o almacena información confidencial, debes cumplir con los requisitos de la norma PCI. Debes reforzar tu seguridad, que a menudo constituyen vías sencillas para que los atacantes maliciosos obtengan acceso a los datos confidenciales de tu portal de negocios.

El WAF en el que inviertas debe identificar y bloquear los ataques sofisticados sin afectar las transacciones legítimas de las aplicaciones. Además, el WAF debe ofrecer informes de PCI, que determinen el cumplimiento con las reglamentaciones

De todas las violaciones a la privacidad de los datos investigadas en los últimos diez años, se descubrió que ni una sola empresa cumplía con la norma de PCI al momento de la violación

Verizon
*Informe sobre el cumplimiento de la norma PCI de 2015*

## Alto rendimiento de la solución

A la hora de elegir un WAF, es importante considerar el rendimiento y capacidad del WAF. No debe afectar el funcionamiento de tus servicios ni la eficiencia de las herramientas existentes de tu empresa, incluidos los portales web y aplicaciones.

Los servicios web de tu empresa deben comportarse y funcionar como si el WAF no existiera, el cual deberá ser completamente transparente. Los usuarios no deberán notar ningún cambio en el rendimiento del servicio.

## Administración desde cualquier punto

La administración de la solución WAF deberá ser descentralizada, ya que deberá trabajar con una infraestructura de aplicaciones web que está distribuida en diferentes esquemas (On-premise, nube o híbrida) y en diferentes partes del mundo.

Es de vital importancia administrar un WAF sin tener que conectarse directamente a cada uno por separado.

## Prevención contra vulnerabilidades

Las vulnerabilidades de las aplicaciones web son una de las causas más comunes de violaciones a la privacidad de los datos. Las vulnerabilidades exponen las infraestructuras web de las empresas a los ataques como reescritura de comandos entre sitios, inyecciones SQL, envenenamiento de cookies y finalmente la caída de tus servicios ecommerce.

## Solución fácil de usar

Un WAF no debería ser difícil de implementar y administrar pero, como cualquier otra herramienta, cuanto más completo, más provecho sacarás de del WAF. Deberás buscar la solución que sea capaz de administrarse por sí misma, que requiera la mínima interacción humana y que automáticamente genere políticas de protección para ataques de día cero. Con una simple configuración en pocos pasos y click quede implementada.

advance networks® Video Technology Experience

# 05

# Tipos de WAF

## Basados en la nube completamente administrados

Esta modalidad en WAF permite detener ataques de denegación de servicios (DDoS) de forma rápida y sencilla.

## Basados en la nube autoadministrados

La gran ventaja de manejar solución WAF en la nube es que mantendrás el control de la administración del tráfico y los ajustes de tu política de seguridad.

Al ser autoadministrado, este modelo provoca un grado de complicaciones por parte de tus expertos en seguridad del servicio web, para implementar y crear as políticas de seguridad necesarias.

## WAF basados en solución On-Premise

Esta de una de las soluciones más comunes que hay en el mercado, la gran ventaja es que consta de un equipo físico que se encuentra en las instalaciones de la empresa y eso puede generar hasta cierto punto tranquilidad por tener todo el control de la solución.

La desventaja que tiene una solución On-Premise es que no es una solución tan fácil de implementar en esta etapa critica que vive el mundo. Sin dejar de mencionar que suele ser más costosa que un servicio en la nube.

# Una solución en la nube puede añadir valor a tu negocio.

Estas soluciones tienden a acumular la experiencia de varios clientes. Con las mejores soluciones podremos conocer cuáles son las prácticas óptimas utilizadas en el mercado para nuestro ámbito de negocio. Una solución de este tipo se enriquece continuamente con las necesidades de todos los clientes que la utilicen.

Es muy probable que esto nos permita encontrar formas de optimizar nuestro negocio más allá de lo que originalmente teníamos contemplado.*

En Advance Networks recomendamos ampliamente a nuestros clientes **CloudWAF** de Radware, ya que, al ser implementada en la nube contarás con todas las ventajas anteriormente mencionadas y claro la que brinda su propia naturaleza, la de proteger portales de negocios, los cuáles estarán siempre disponibles para que tus clientes y socios tengan la mejor experiencia de usuario.

***Que la ventaja de tu marca sea tu producto y la productividad, tu portal de negocios.***

A continuación las principales ventajas de usar servicios en la nube

**Menor inversión de capital.** Estas soluciones no requieren invertir en infraestructura o licenciamiento para utilizarse. Prácticamente todo el consumo es bajo la modalidad de renta. Una renta inclusiva que engloba todo lo necesario para utilizar la aplicación y que también la mantiene actualizada en el tiempo.

**Ahorro en los costos internos de las operaciones de TI.** El proveedor se encarga de mantener la solución a punto y de ofrecernos una garantía de disponibilidad mediante un acuerdo de nivel de servicio que estipula un nivel máximo de falla por periodo de tiempo. Internamente no tendremos que preocuparnos por tareas como monitoreo de bases de datos, respaldos, mantenimiento de equipos, almacenamiento, actualizaciones de sistema, etcétera.

**Prueba gratuita:** La mayor parte de los proveedores de soluciones de software en la nube nos permiten probar antes de comprar. Normalmente podremos conocer el funcionamiento de la solución y operar en nuestro negocio con usuarios o funcionalidad limitada por algún tiempo.

# WAF basado en solución híbrida

Esta nueva modalidad, desarrollada principalmente por la empresa Radware, protege todos los elementos de una red desde una única herramienta híbrida. Es capaz de identificar todo tipo de ataques contra los servidores web, los sistemas de almacenamiento y los servicios y aplicaciones Cloud de una empresa, bloquear accesos no autorizados y proteger los sistemas frente a diferentes ataques DDoS (con un mínimo número de falsos positivos y sin repercutir sobre el tráfico real) gracias a sus capas de protección constantemente activas.

## Fortalezas y debilidades entre distintos WAF´s

Akamai ofrece una solución WAF independiente de la nube. El WAF de Akamai, es un conjunto de productos de seguridad que incluye protección DDoS y administración. En un mar de referencias de clientes, Akamai se destacó por la posibilidad de agregar fácilmente otros productos de la marca.

Por otro lado, algunos de los desafíos del cliente al implementar la solución de esta marca se centraron en la comunicación y administración de la solución, falta de transparencia en las operaciones del WAF a limitado a la solución con referencia "sobre cuándo se están realizando cambios".

Imperva Cloud WAF ofrece un conjunto de protecciones de aplicaciones del lado de la implementación, que incluyen WAF, gestión de bots, DDoS y seguridad API. La facilidad de uso es un tema común entre los clientes, quienes calificaron la IU como buena, sin embargo, los bucles de retroalimentación siguen siendo una fuente de frustración para los usuarios de la solución WAF de está marca.

# Advance Networks: Radware, una de las marcas líderes en protección de servicios web con WAF

Radware, una de las empresa líderes en el mercado en entrega de aplicaciones y soluciones en ciberseguridad situado en el cuadrante mágico de Gartner, ofrece protección para servicios web, que maximizan la eficiencia de las áreas TI. El hecho de estar posicionados en el cuadrante de los visionarios, es una validación que demuestra entender el mercado de la seguridad y el compromiso con el cliente cumpliendo con los estándares más sólidos en el tema de soluciones de protección de servicios web.

Ofrece a las empresas seguridad consolidada con múltiples opciones de implementación. **AppWall** como solución On-Premise de Radware se puede implementar como un dispositivo virtual o físico, ya sea de forma independiente o en parte superior del controlador de entrega de aplicaciones (ADC). También ofrece **Cloud WAF** como versión en la nube a nivel mundial e incluir Radware Bot Manager, y **Kubernetes WAF** para aplicaciones nativas de la nube, tiene una fuerte asociación con Microsoft para ejecutar Cloud WAF el único servicio WAF que se ejecuta de forma nativa en Azure.

# CloudWAF

Ofrece protección de seguridad web adaptable y sin igual, basado en el firewall de aplicaciones web líder en el mercado, certificado por ICSA Labs de Radware, el servicio **CloudWAF** proporciona cobertura completa de todos los ataques de los 10 principales de OWASP. El servicio implementa seguridad negativa y positiva. utilizando su capacidad única para adaptarse automáticamente al panorama de amenazas en constante cambio y activos en línea defendibles. Ofrece gran rendimiento y velocidad al disponer de tus servicios web, no requiere de un experto para administrar la solución, la implementación se logra en menos de 2 horas para finalmente ser una solución que no requiere interacción humana. No requiere hardware ni software se activa de manera sencilla con un cambio de DNS's.

Diseñado con el aprendizaje automático de última generación, es un servicio 100% en la nube que detecta y analiza automáticamente las vulnerabilidades potenciales en tu portal web y asigna políticas de protección óptimas.

Monitorea continuamente y analiza patrones de uso de tus servicios web y genera políticas para legitimar el tráfico. Esto permite una detección rápida y mitigación de ataques de día cero. Una de sus grandes características es el uso de huellas digitales, tecnología que permite el diagnóstico automático de fuentes maliciosas tratando de ocultarse detrás de los cambios dinámicos de IP.

# 06

# Casos de éxito

## Manutan implementa WAF de Radware

Manutan, uno de los mayores proveedores de equipo y suministros industriales y de oficina a empresas con sede en Francia, utiliza la solución de Radware para garantizar la alta disponibilidad de sus servicios., seleccionó seguridad que incluye mitigación de ataques SSL, Firewall de aplicaciones web (WAF) basados en la nube.

*Las plataformas de comercio electrónico de Manutan impulsan la mayoría de sus negocios en estos días. Por lo tanto, el negocio de la empresa depende de la disponibilidad de servicios web, así como de teléfonos y fax virtualizados, que siguen siendo herramientas clave para el comercio.*

## Hexatom selecciona a Radware

Hexatom recurrió a Radware porque necesitaba una solución propia, integral y automatizada que consistiera en tecnología de firmas en tiempo real basada en el comportamiento protegido por patente que detecta y mitiga con precisión los ataques de red emergentes, todo ello, sin la necesidad de intervención humana y sin bloquear el tráfico legítimo de usuarios.

*"Queríamos una solución local para complementar la protección que ya teníamos con nuestros operadores", dijo Emmanuel Vannier, Hexatom. "Seleccionamos Radware debido a sus capacidades únicas de detección y mitigación, la protección integral contra ataques DDoS, SSL y basados en la Web, y el costo total de propiedad".*

# Gracias!

Hoy en día las amenazas en la red son cada vez mayores, a causa de la contingencia internacional la forma de hacer negocios de las empresas ha evolucionado, el comercio electrónico es hoy la ruta donde muchas empresas siguen el camino. Por esta razón, tus servicios web deben siempre estar disponibles y esto te puede ayudar a incrementar y transformar tu empresa.

En Advance Networks nos preocupamos por mantener segura, íntegra y disponible la información de tu empresa. Por esta razón, te ofrecemos las mejores soluciones en ciberseguridad gracias a una de nuestras alianzas estratégicas en México, Advance Networks - Radware, manejando tecnología de última generación de origen israelí.