Ciencia Latina
Revista Multidisciplinar

DOI: https://doi.org/10.37811/cl_rcm.v6i6.3757

Implementación de cortafuego de aplicación en plataformas web y API´s para la contención y mitigación de ciberataques

Fco. Javier Vazquez Pantaleon
fj.vazquez@lcardenas.tecnm.mx
https://orcid.org/0000-0001-8764-0868
Departamento de sistemas y computación del
Instituto Tecnológico de Lázaro Cárdenas
Lázaro Cárdenas, Mich. – México

Gabriel Nava Fombona
gabriel.nava@lcardenas.tecnm.mx
https://orcid.org/0000-0003-2697-8122
Departamento de sistemas y computación del
Instituto Tecnológico de Lázaro Cárdenas
Lázaro Cárdenas, Mich. – México

Jesus Daniel Rojas Cid
jdaniel.rojas@lcardenas.tecnm.mx
https://orcid.org/0000-0003-2183-8163
Departamento de sistemas y computación del
Instituto Tecnológico de Lázaro Cárdenas
Lázaro Cárdenas, Mich. – México

RESUMEN

El objetivo general de la investigación tiene como finalidad implementar un cortafuego de aplicación web mediante application and API protection (WAAP) para poder brindar medios de protección ante los ciberataques, manteniendo la integridad, confidencialidad y disponibilidad de la información dentro de una institución. La investigación mantiene un alcance descriptivo de tipo retrospectivo. Además, contempla un enfoque cualitativo, con diseño no experimental, de corte transversal. En su implementación se aplica la metodología defensa en profundidad que contemplan 7 fases, de la cual, la fase 3 es el aseguramiento de perímetro externo que se desarrolla con la guía denominada Accelerated Implementation Program (AIP) de SAP, consta de preparación de la solución, realización y/o configuración, despliegue. Como resultante se obtuvo la mitigación y contención de los ciberataques principalmente, Vulnerabilidades de día cero, DDOS, SQL Injection, Cross-site scripting, entre otros, de tal modo se garantiza la disponibilidad de la información integra y segura.

Palabras clave: *ciberseguridad; WAAP; mitigación; contención; ciberataque.*

Correspondencia: fj.vazquez@lcardenas.tecnm.mx
Artículo recibido 16 octubre 2022 Aceptado para publicación: 16 noviembre 2022
Conflictos de Interés: Ninguna que declarar

Cómo cita Vazquez Pantaleon, J., Fombona, G. N., & Rojas Cid, J. D. (2022). Implementación de cortafuego de aplicación en plataformas web y API´s para la contención y mitigación de ciberataques. Ciencia Latina Revista Científica Multidisciplinar, 6(6), 4045-4064. https://doi.org/10.37811/cl_rcm.v6i6.3757r

Implementation of web application protection and api for the containment and mitigation of cyberattacks

ABSTRACT

The general objective of the research is to implement a web application firewall through application and API protection (WAAP) in order to provide means of protection against cyberattacks, maintaining the integrity, confidentiality and availability of information within an institution. The research maintains a retrospective descriptive scope. In addition, it contemplates a qualitative approach, with a non-experimental, cross-sectional design. In its implementation, the defense-in-depth methodology is applied, which includes 7 phases, of which phase 3 is the assurance of the external perimeter that is developed with the guide called SAP's Accelerated Implementation Program (AIP), consisting of preparation of the solution, realization and/or configuration, use. As it turned out, the mitigation and containment of cyberattacks was obtained mainly, zero-day vulnerabilities, DDOS, SQL Injection, Cross-site scripting, among others, thus guaranteeing the availability of complete and secure information.

Keywords: *cybersecurity; WAAP; mitigation; containment; cyberattack.*

INTRODUCCIÓN

La tecnología es parte fundamental del día a día de la vida de los seres humanos, en el trabajo, en el hogar por consecuencia al hacer uso de la misma se genera información. La información es el activo digital más valioso que se tiene. En el ámbito organizacional, la información contenida en los aplicativos es parte medular de los procesos estratégicos, y mantener asegurados los sistemas, representa un reto hoy día, debido a los ciberataques que han ido al alza por el uso exponencial de la tecnología, debido a la necesidad de automatización de procesos en las diferentes áreas, en las que hacen uso de Internet de las cosas, Blockchain, Inteligencia artificial, Big Data, Computo en la nube, etc.

Todas las tecnologías mantienen un grado de vulnerabilidad desconocido que ciertos perfiles como los Black Hat Hackers descubren cuando realizan una investigación y del cual se aprovechan (Long, 2012).

La ciberseguridad trata de salvaguardar esas vulnerabilidades que presenta la tecnología o lo que representa un riesgo para los activos informáticos.

> La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes (Kaspersky, 2020, p. 1).

La problemática central que se pretende abordar es la necesidad de salvaguardar de ciberataques a las plataformas web y a las API (Bandera & Villero Contreras, 2021).

ESET Security Report presenta un informe al año de las estadísticas sobre el comportamiento de la seguridad de las empresas en la región de Latinoamérica, y cuyo contenido se basa en el análisis de encuestas realizadas a profesionales de tecnología y datos de la telemetría de ESET.

Dentro de los hallazgos que presentan en su reporte en el año 2021 se tiene:

“Los códigos maliciosos son la principal preocupación (64%) y la primera causa de incidentes de seguridad (34%) en las empresas latinoamericanas” (ESED, 2021, p. 4).

"El número ataques de fuerza bruta a los servicios de acceso remoto como RDP creció 704%, mientras que los registros para usuarios únicos aumentaron 196% durante 2020 en Latinoamérica" (ESED, 2021, p. 4).

"Con base en la telemetría de ESET, las empresas de Brasil (26,4%) fueron las más afectadas por casos de phishing durante 2020, seguidas por las empresas de Perú (22,8%) y México (12%)" (ESED, 2021, p. 4).

Dentro de los hallazgos que presentan en su reporte en el año 2022 se tiene:

"El país con la mayor cantidad de detecciones es Perú (18%), seguido inmediatamente por México (17%), Colombia (12%), Argentina (11%) y Ecuador (9%)" (ESED, 2022, p. 4).

"Dos tercios de los encuestados señaló la infección con códigos maliciosos como la mayor preocupación en materia de ciberseguridad. A esta le sigue la preocupación por el robo de información (62%)" (ESED, 2022, p. 4).

"Las detecciones de vulnerabilidades rompieron un nuevo récord en 2021, con más de 22 mil reportes a lo largo del año. Esto resultó en un promedio de 4100 exploits detectados a diario" (ESED, 2022, p. 4). Los problemas de seguridad en la actualidad van al alza, la dependencia de las tecnologías nos hace más susceptibles a ciberataques (World Economic Forum, 2020).

Marco teórico

Un sistema contempla el conjunto de componentes interrelacionados, con un límite claramente definido, trabajando juntos para lograr un conjunto común de objetivos de manera que acepta entradas y produce salidas (Adorno, 2019). La representación de sistema a través de la informática da vida a las tecnologías que usamos en nuestro día a día en el hogar y en el trabajo.

"Los ciberataques aspiran a dañar o a lograr acceso a documentos importantes y sistemas de una red empresarial o personal o al control de estos" (Microsoft, 2022, p. 1). Dentro de los ciberataques más relevantes tenemos malware, ataques de denegación de servicio distribuido (DDOS), phising, ataques por inyección de código SQL, scripting entre sitios (XSS), redes de robots (Botnets), ransomware (Microsoft, 2022).

Existe una organización llamada proyecto abierto de seguridad de aplicaciones web o por sus siglas en ingles OWASP, que se dedica a determinar o combatir las causas raíces que hacen al software, aplicaciones informáticas, sistemas informáticos inseguros (OWASP,

2022). Cada año suele presentar un estudio sobre las principales amenazas que se relacionan con los ataques antes mencionados. Figura 1.

Firewall

Representa una parte importante para protegerse de los ataques. Es el encargado de monitorear el tráfico de red (entrante y saliente) y toma decisiones que fluye en la red permitiendo o bloqueando, basado en conjunto de reglas predefinidas. Se han constituido como la primera barrera de defensa tanto en redes locales y las externas (CISCO, 2019). Existen diversos tipos de firewalls entre los que destacan:

Un firewall proxy, uno de los pioneros, funciona como puerta de entrada entre dos o más redes para un aplicativo específico. Además, pueden brindar un extra en funcionalidad, como seguridad al permitir analizar inputs y almacenamiento de contenido en caché, restringiendo las peticiones directas desde el exterior de la red (CISCO, 2019).

Firewall de inspección activa, permite o el bloqueo de tráfico en base al estado, puerto y protocolo, realiza la vigilancia de toda la actividad desde el comienzo de la conexión hasta la conclusión. La toma de decisión para el filtrado se rige en base a reglas que define el administrador y el contexto (Dielsa, 2019).

Firewall de administración unificada de amenazas (UTM), es la sinergia de múltiples servicios o funciones de seguridad en un solo lugar, los usuarios de la red están protegidos con filtrado de correo electrónico, antivirus, filtrado de contenido, filtro web, entre otros (Fortinet, 2022).

Firewall de próxima generación (NGFW), preparado para el bloqueo de amenazas modernas como los ataques de capa de aplicación (funciones WAF) y malware (Taeyong, Taewoong, Lee, & Jungsuk, 2021). Tiene todas las características de los firewalls mencionados incluye prevención de intrusos, bloque de aplicativos con alto riesgo de vulnerabilidad, vías de actualización de fuentes para reconocimiento de vulnerabilidades conocidas, autoaprendizaje para afrontar amenazas en constante evolución. Sus funciones van incrementando a medida de su uso (CISCO, 2019).

Firewall de próxima generación centrado en amenazas (NGFW), mantiene las mismas características que el anterior sumando la especialización de estar al tanto de activos con mayor riesgo y reaccionar de manera oportuna a los ataques, incorpora la mejora de tiempos de respuesta significativamente en la detección y eliminación de la amenaza, brinda la facilidad para su administración reduciendo la complejidad (CISCO, 2019).

Los sistemas de contención de ataques de capa 7 o de capa de aplicación (WAF) forman parte esencial como refuerzo para la protección de plataformas web (Neupane, Haddad, & Lei, 2021). En nuestra implementación se hace uso de las características de un firewall de próxima generación centrado en amenazas denominado cloudflare.

Cloudflare es un servicio en la nube que ofrece aceleración en carga del contenido, seguridad y fiabilidad. Dentro de la seguridad se abordan los ciberataques DDoS, inyecciones de código, bots maliciosos, las vulnerabilidades publicadas en CVE de MITRE, OWASP, entre otras (Cloudflare, 2022).

Existen soluciones para la protección a nivel de aplicación que no se brinda como servicio o en la nube, tales como ModSecurity el cual es un complemento que se configura en los servidores web con mayor demanda Apache, IIS, NGinx (Hlaing & Khaing, 2020). El segundo lugar lo tiene IRONBEE que tiene las mismas características que el anterior con la diferencia que va dirigido a orientar el comportamiento de las plataformas web y de usuarios, de esta manera se establecen controles de seguridad resultado del análisis realizado (Méndez, 2022). Por otro lado, se cuenta con los servicios en la nube de Radware WAF, Amazon web services WAF, Cloud armor WAF, Microsoft WAF. Cada uno de ellos cumple con las características de protección de la lista de MITRE, OWASP. Una de las desventajas de poder usar alguno de ellos es el costo. La integración de nuevas técnicas de inteligencia artificial refuerzan la prevención y mitigación de los ataques el uso de modelos de IA cada vez son más comunes (Muhammad Nadeem, 2022).

La implementación de cloudflare se rige con la metodología de defensa en profundidad (DID). Figura 2, en la fase de perímetro, dado que es la parte medular que se pretende reforzar en las plataformas web y api´s, también se basa en las estepas de Accelerated Implementation Program (AIP) de SAP para la implementación (Kratikal, 2020).

El objetivo es proteger de ciberataques a nivel de aplicación a las plataformas web y api´s contenidas dentro de un dominio.

METODOLOGÍA

Defensa en profundidad se denomina a la pila de medidas de seguridad para salvaguardar la información, cubriendo en su plenitud los aspectos empresariales que demandan resguardo (Avast, 2022). Se vulnera una fase de defensa, la otra fase entra en acción para evitar el filtrado de las amenazas. De manera que, se combate a las vulnerabilidades que

inevitablemente conlleva la tecnología, las posiblemente generadas por personal y las originadas por operaciones de una red (Ciberseguridad, 2022). Figura 2.

Fase 1. Se deben de aplicar políticas, procedimientos, alertas, dentro de la organización, deben ser fundamentadas en estándares nacionales o internacionales tales como, MTRE, SANS, ISO, etc.

Fase 2. Se deben de incorporar medios físicos de resguardo como CCTV, guardias, bloqueos, controles de acceso al personal al cuarto de telecomunicaciones, alarmas, etc.

Fase 3. Se debe de incorporar servidores de seguridad, filtrado de tráfico, bloqueos de tráfico, dispositivos de seguimiento, se protege el perímetro de la red.

Fase 4. Se debe de segmentar la red, uso IPSec, NIDS, estructura lan, wan y dmz, gestión general de seguridad en la red interna.

Fase 5. Se aplican reforzamiento a los sistemas operativos, administración de revisiones y/o parches, autenticación, HIDS, uso de certificados desde directorio activo, reglas de huésped.

Fase 6. Se deben de implementar antivirus, aplicación sandbox para impedir la ejecución de código malicioso, manejo de privilegios a nivel de aplicativos.

Fase 7. Datos, cifrado, acl, configuraciones en dispositivos (Rodriguez, Yepez Holgin, Peralta Guaraca, & Ortiz Zambrano, 2018).

La implementación de cloudflare para la protección ante ciberataques recae en la fase 3, que aborda la protección del perímetro externo. Figura 3. Se contempla como medio de referencia la guía denominada Accelerated Implementation Program (AIP) de SAP, la cual indica la forma de cómo implementar de manera rápida un aplicativo, considerando tres elementos esenciales, preparación es la elección del aplicativo para la implementación y recursos, configuración es la parte técnica que se realiza para el correcto funcionamiento, despliegue es el aseguramiento de las funciones e identificar las funciones principales ejercidas por el aplicativo (SAP, 2013). Figura 4

Preparación

Se ingresar a la página oficial de Cloudflare, crear una cuenta si no se tiene una. Figura 5. Al iniciar sesión se solicita proporcionar el dominio que desea asegurar, para este caso el dominio de la institución es itlc.mx, este dominio y sus subdominios son utilizados para la publicación de todas las plataformas web y api´s publicadas. Mencionar que se pueden agregar tantos dominios como se requieran. Figura 6.

En la siguiente ilustración seleccionamos un plan, una de las ventajas que tiene sobre otros servicios de protección en la nube es que ofrece un servicio gratuito con funcionalidades fundamentales como DDoS, Aceleración de contenido, etc. Seleccionamos el plan Pro, que cuenta con todas las características requeridas. Figura 7.

Al seleccionar el plan comienza la sincronización de los registros del dominio y subdominios de manera automática se hace el registro, posteriormente se pueden editar para personalizar alguna configuración extra requerida. Figura 8.

Configuración

En esta etapa ingresamos al portal de administración de nuestro dominio y en el menú de administración de dns, eliminamos los dns registrados y se registran los proporcionados por cloudflare. Cabe mencionar que los registradores pueden tardar entre 24 y 48 horas en procesar las actualizaciones del servidor de nombres. Figura 9.

Se refuerza la configuración inicial con la activación de redirección https, esto para garantizar la comunicación cifrada, momificar archivos y compresión de contenido, Ilustración 4. Hasta este punto todo está en operación y funcionando, el dominio está protegido. Figura 10.

Despliegue

Se consideran las siguientes acciones que conforman el despliegue de la solución.

Rendimiento: CDN, Almacenamiento en caché del contenido estático, Purga completa de caché inmediata, TTL mínimo de vencimiento de la caché, Tamaño máximo de carga (MB), TCP Turbo, Argo Smart Routing, Tiered Caching, Load Balancing, Equilibrio de carga global (enrutamiento basado en geolocalización), Comprobaciones de estado de Load Balancing, Stream. Personalización y optimización: Reglas de página, Enlaces móviles acelerados (AMP), IPv6, HTTP/2, SPDY, WebSockets, Carga asincrónica de JavaScript con Rocket Loader, Optimización de imagen con Polish, Optimización móvil, Redimensionamiento de imágenes, Almacenamiento de pares clave-valor con Workers.

Seguridad: Protección contra DDoS de uso no medido, Implementa soluciones de inteligencia para identificar nuevas amenazas, Protección contra amenazas basada en la reputación, Protección contra spam en comentarios, Protección contra la apropiación de contenido, Alertas DDoS, Protección contra DDoS para SSH, Protección DDoS para

Minecraft. Gestión de certificados: Certificado SSL universal, Cloudflare para SaaS, Administrador de certificados avanzados. Firewall de aplicaciones web (WAF): Reglas WAF, Reglas del bloqueador de agente de usuario, Reglas del bloqueo de zona, Reglas administradas de Cloudflare, Conjuntos de reglas básicas de OWASP, Limitación de velocidad, Reglas de limitación de velocidad, Reglas de encabezado de limitación de velocidad, CAPTCHA/Desafío de JavaScript, Modo Bot Fight, Modo Super Bot Fight.

Fiabilidad: DNS global de Anycast, DNSSEC, Registros DNS comodín, Proxy de registro de DNS comodín. Acceso al panel de control, del usuario y API: Acceso administrativo multiusuario, Acceso a la API de Cloudflare, Integración con Terraform. Información y análisis: Análisis del sitio y DNS, Cache Analytics, Análisis del sitio (resolución), Análisis de DNS (tiempo histórico), Análisis de firewall (tiempo histórico), Análisis de equilibrio de carga (tiempo histórico), Registros de auditoría. Conformidad: ISO 27001. Soporte: Soporte en caso de incidencia.

RESULTADOS Y DISCUSIÓN

Resaltando algunas características tenemos que el tráfico hacia las plataformas es de 109,49 k solicitudes en un periodo 24 horas, de las cuales 15,06 k en cache y 94,44 k no se cacharon. Figura 11.

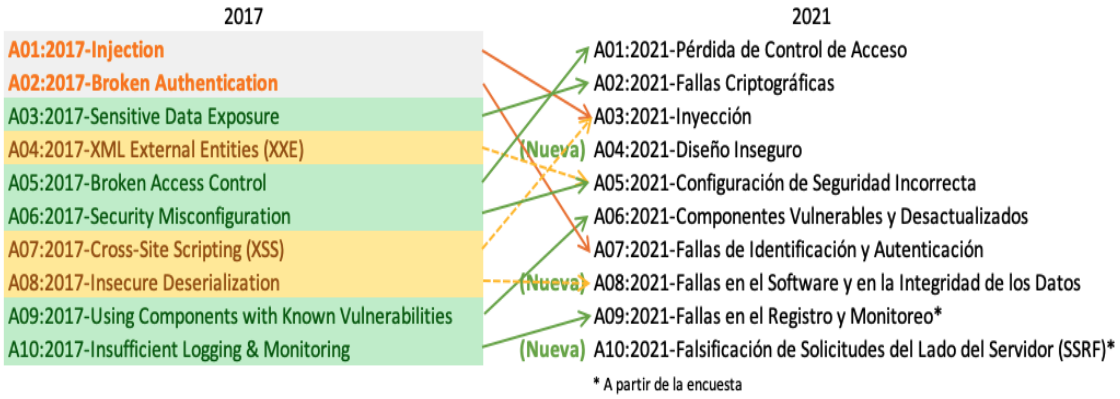
El ahorro de carga de datos corresponde a 33 GB en el último mes, eso significa un beneficio para aumentar el rendimiento de las plataformas web y api´s, además de un 35% del ahorro de ancho de banda. La cantidad de ataques bloqueados corresponde a 4535 correspondiente a las solicitudes citadas con anterioridad. Las principales fuentes de esos ataques provienen de países como China, Taiwan, Rusia, Japón, Alemania, Estados Unidos, Autralia, etc. Figura 12.

La mayoría de las amenazas se realiza con bots, significa que utilizan automatizaciones para los ataques, estos se especializan en buscar vulnerabilidades expuestas y poder aprovecharse de ellas. Además de ataques como inyección SQL, XSS, DDoS, etc. Figura 13.

ILUSTRACIONES, TABLAS, FIGURAS.

Figura 1.

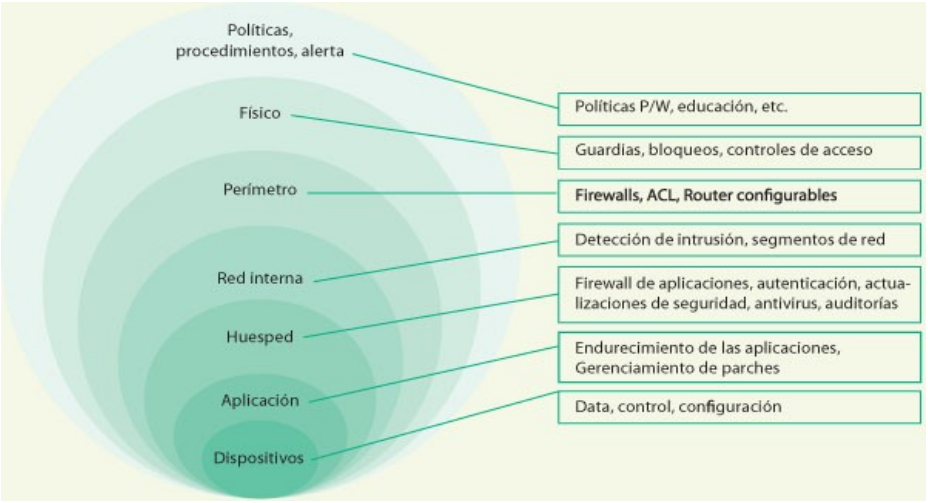
Los 10 principales riesgos de seguridad de las aplicaciones web



Nota. Adaptado de Riesgos de Segurida de las Aplicaciones Web y API´s, por OWASP, 2021, OWASP (https://owasp.org/www-project-top-ten/). CC BY 2.0

Figura 2 .

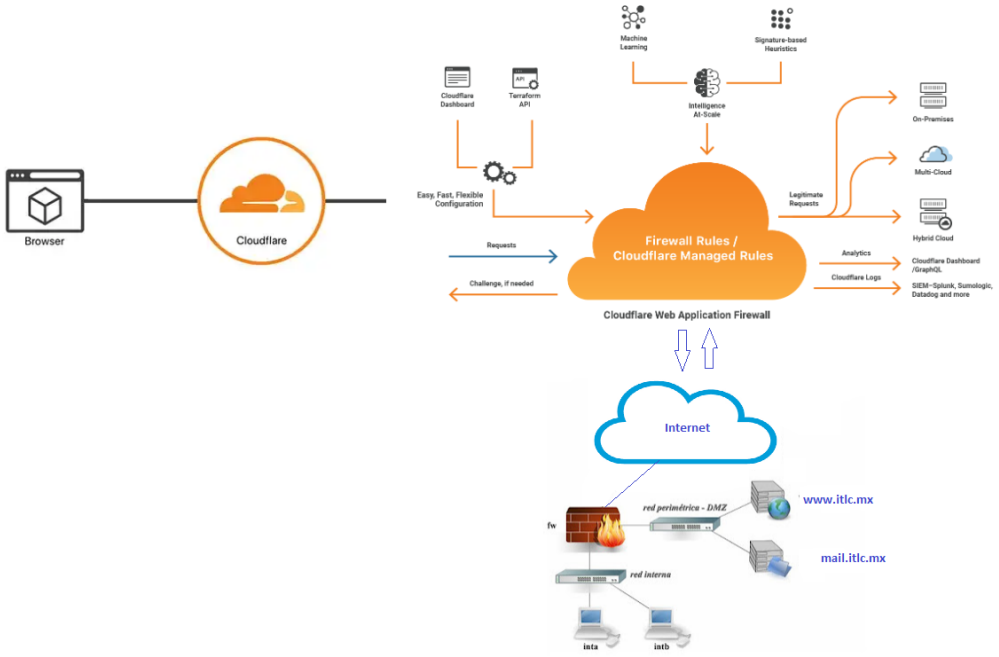
Arquitectura de seguridad que incorpora varios niveles



Nota. Adaptado de Ciberseguridad | Sistemas de detección de intrusión en la red para infraestructuras críticas, por Daniel Paillet, 2017, Editores (https://www.editores-srl.com.ar/revistas/aa/6/paillet_sistemas_de_deteccion). CC BY 2.0

Figura 3.

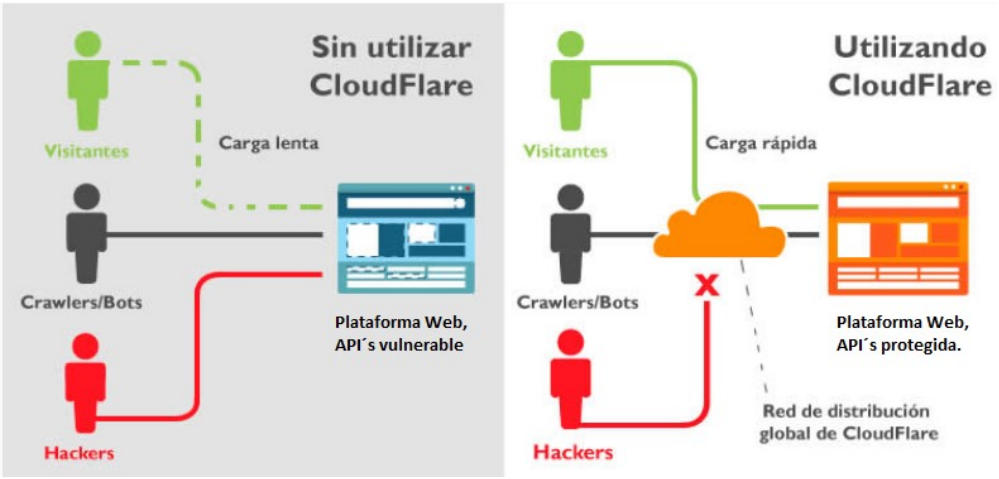
Infraestructura en la nube



Nota. Adaptado de *Cómo funciona Cloudflare con cualquier infraestructura de nube,* por Cloudflare, 2017, Cloudflare (https://www.cloudflare.com/es-es/learning/cloud/cloudflare-and-the-cloud/). CC BY 2.0

Figura 4.

Utilizando Cloudflare vs Sin utilizar Cloudflare



Nota. Adaptado de *Qué es Cloudflare y como funciona,* por HardNET, 2020, HardNET (https://www.hardnet.com.ar/noticias/que-es-cloudflare-y-como-funciona). CC BY 2.0

Figura 5.

Início de sesión

Nota. Adaptado de *Servicio en la nube de Cloudflare,* por Cloudflare, 2022, Cloudflare (https://dash.cloudflare.com/login). CC BY 2.0

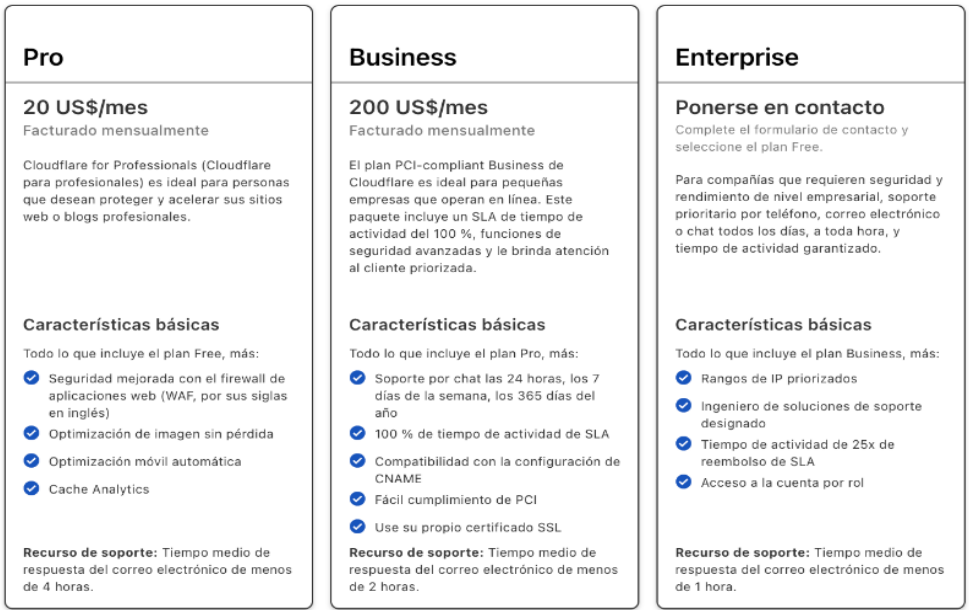
Figura 6.

Domínio para administración

Nota. Adaptado de *Servicio en la nube de Cloudflare,* por Cloudflare, 2022, Cloudflare (https://dash.cloudflare.com/login). CC BY 2.0

Figura 7.

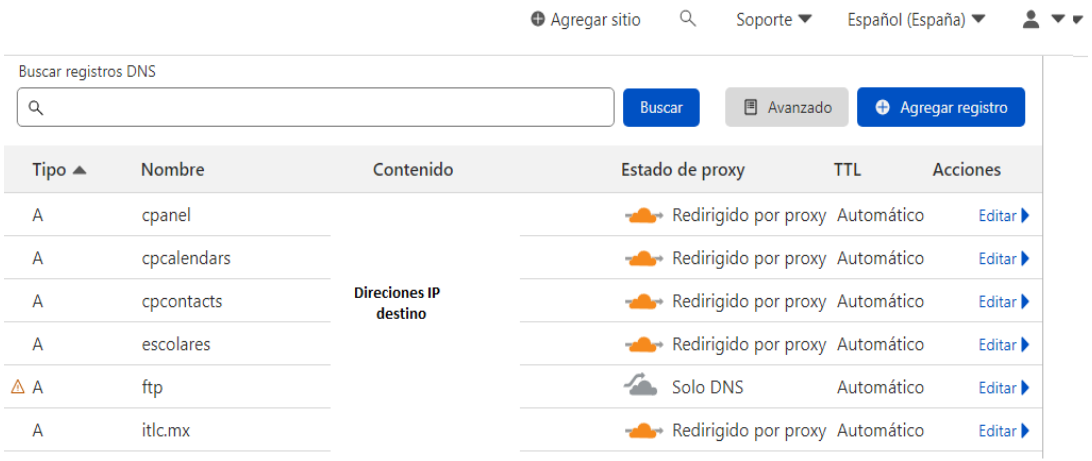
Selección de Plan



Nota. Adaptado de *Servicio em la nube de Cloudflare,* por Cloudflare, 2022, Cloudflare (https://dash.cloudflare.com/login). CC BY 2.0

Figura 8 .

Sincronizacion de registros DNS



Nota. Adaptado de Servicio em la nube de Cloudflare, por Cloudflare, 2022, Cloudflare (https://dash.cloudflare.com/login). CC BY 2.0

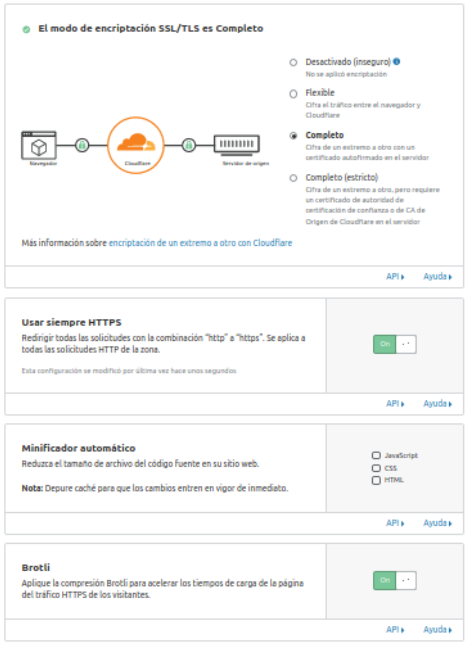
Figura 9

Cambio de administrador de registros DNS

Nota. *Adaptado de* Servicio em la nube de Cloudflare, *por Cloudflare, 2022, Cloudflare (*https://dash.cloudflare.com/login*). CC BY 2.0*

Figura 10

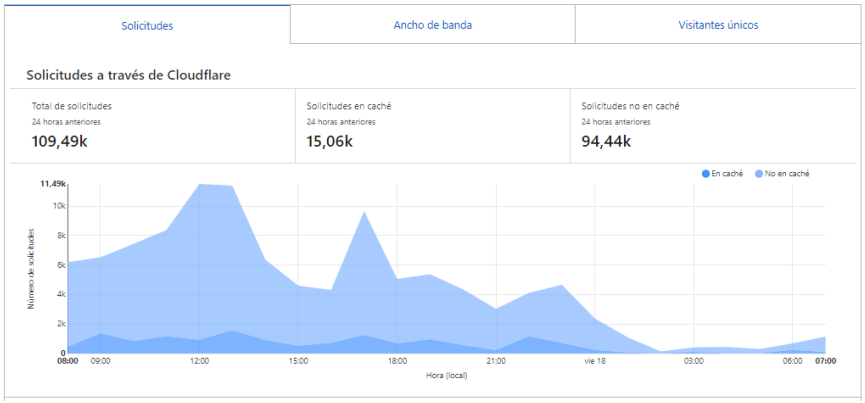
Activación de servicios de protección



Nota. Adaptado de *Servicio en la nube de Cloudflare,* por Cloudflare, 2022, Cloudflare (https://dash.cloudflare.com/login). CC BY 2.0

Figura 11

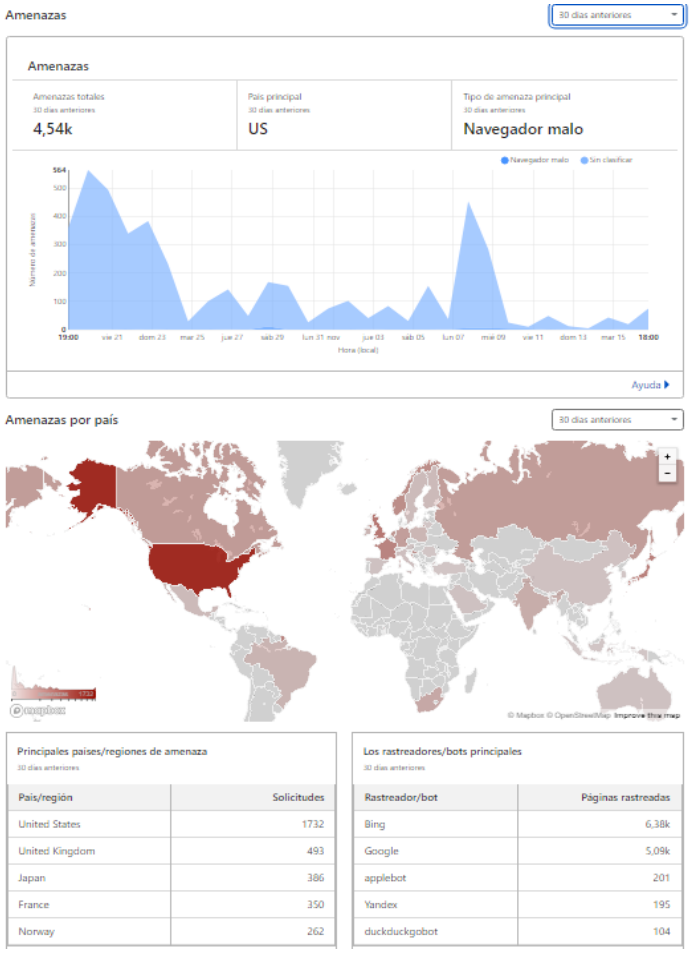
Tráfico hacia plataformas web y API´s



Nota. Adaptado de *Servicio en la nube de Cloudflare,* por Cloudflare, 2022, Cloudflare (https://dash.cloudflare.com/login). CC BY 2.0

Figura 12

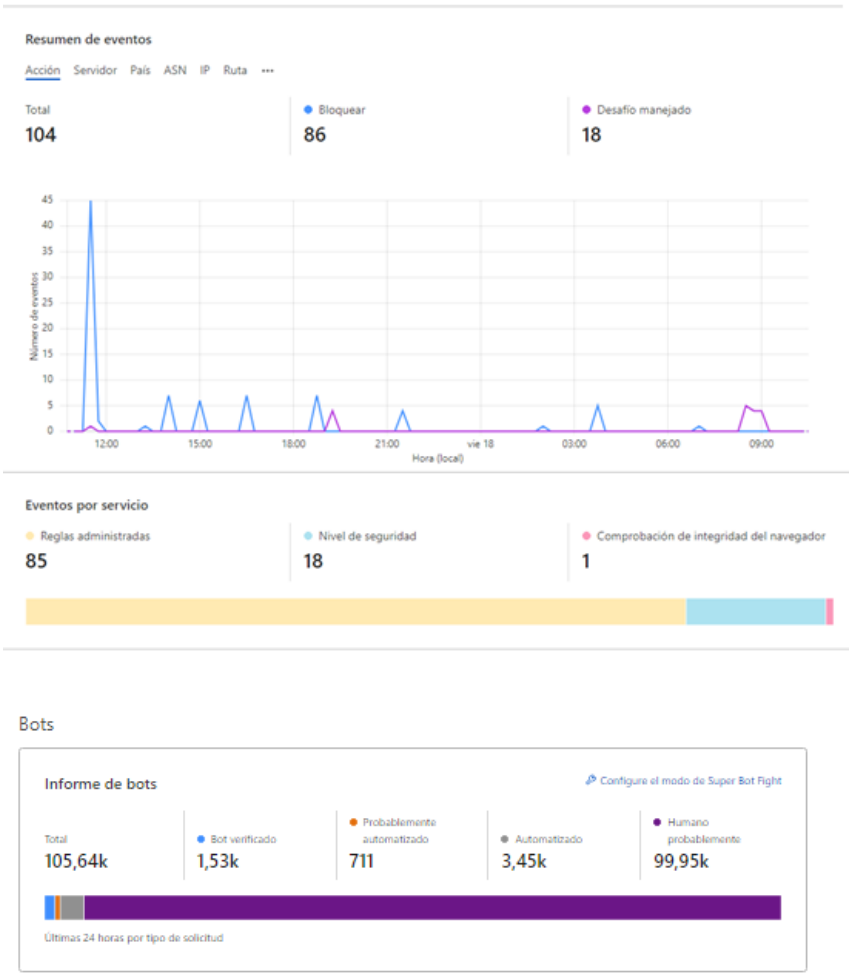
Informe de amenzas y su geolocalización



Nota. Adaptado de Servicio en la nube de Cloudflare, por Cloudflare, 2022, Cloudflare (https://dash.cloudflare.com/login). CC BY 2.0

Figura 13

Ataques contenidos y mitigados.



Nota. Adaptado de *Servicio en la nube de Cloudflare,* por Cloudflare, 2022, Cloudflare (https://dash.cloudflare.com/login). CC BY 2.0

CONCLUSIONES

La implementación del cortafuego de aplicación en plataformas web y API´s para la contención y mitigación de ciberataques dentro de la fase 3 correspondiente a perímetro externo, gestionado por el servicio en la nube de la infraestructura de cloudflare ha cumplido su objetivo. Se han contenido y mitigado los ciberataques. La factibilidad que representa su adopción es ineludible, mejora todos los aspectos de seguridad dentro del perímetro externo de la organización.

Estamos en tiempos donde la seguridad es un requerimiento obligatorio, no es opcional, si se desea tener protegida la infraestructura tecnológica, recordar que la información es

el activo más valioso de una institución y algo valioso debe ser resguardado. (World Economic Forum, 2020)

LISTA DE REFERENCIAS

Adorno, H. G. (5 de Abril de 2019). *Introducción a los Sistemas de Información.* Obtenido de Ciencias unam: https://cienciadatos.iimas.unam.mx/profesores/pilarang/docencia/bde/1-IntroduccionBaseDeDatos.pdf

Avast. (12 de Enero| de 2022). *Qué es la defensa en profundidad.* Obtenido de Defensa: https://www.avast.com/es-mx/business/resources/defense-in-depth#pc

Bandera, E. F., & Villero Contreras, S. L. (19 de Junio de 2021). *Importancia de la implementación de firewall en redes empresariales como mecanismo para la protección de información.* Obtenido de Ciencia e Ingeniería: http://revistas.uniguajira.edu.co/rev/index.php/cei/article/view/202

Ciberseguridad. (20 de Febrero de 2022). *Qué es la defensa en profundidad y cómo funciona.* Obtenido de Ciberseguridad: https://ciberseguridad.com/guias/prevencion-proteccion/defensa-profundidad-did/

CISCO. (12 de Agosto de 2019). *Qué es un firewall.* Obtenido de CISCO: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Cloudflare. (3 de Agosto de 2022). *Cloudflare.* Obtenido de Qué es cloudflare: https://www.cloudflare.com/es-es/learning/what-is-cloudflare/

Dielsa. (11 de Enero de 2019). *Cómo funciona un Firewall.* Obtenido de Seguridad: https://www.dielsa.com/blog/post/firewall-security-hillstone/

ESED Security. (1 de Junio de 2021). *Security Report.* Obtenido de LATAM 2022: https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

ESED Security. (1 de Junio de 2022). *Security Report.* Obtenido de LATAM 2022: https://eset-la.com/Public_files/ESET-security-report-LATAM2022.pdf?utm_campaign=latam-es-online-esr_-5&utm_medium=email&utm_source=Eloqua&elqTrackId=206cc1fa7f41452f9db

e370fe144e462&elq=27237345f3564c3d90c2f84031390208&elqaid=2832&elqat=1&elqCampaignId=

Fortinet. (3 de Febrero de 2022). *Gestión unificada de amenazas (UTM).* Obtenido de Definición de administrador unificado de amenazas: https://www.fortinet.com/lat/resources/cyberglossary/unified-threat-management

Hlaing, Z. C., & Khaing, M. (28 de Febrero de 2020). *A Detection and Prevention Technique on SQL Injection Attacks.* Obtenido de IEEE Conference on: https://doi.org/10.1109/ICCA49400.2020.9022833

Kaspersky. (21 de 01 de 2020). *Ciberseguridad.* Obtenido de Qué es la ciberseguridad: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kratikal. (1 de Agosto de 2020). *5 Biggest Data Breaches of 2020 (So Far).* Obtenido de Kratikal: https://kratikal.com/blog/5-biggest-data-breaches-of-2020-so-far/

Long, L. (7 de Febrero de 2012). *Profiling Hackers.* Obtenido de SANS Institute: http://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864

Méndez, S. S. (2 de Mayo de 2022). *FIREWALL DE APLICACIÓN WEB.* Obtenido de Seguridad de la información: https://revista.seguridad.unam.mx/numero-17/firewall-de-aplicaci%C3%B3n-web-parte-ii

Microsoft. (12 de Enero de 2022). *Ciberataque.* Obtenido de Seguridad de Microsoft: https://www.microsoft.com/es-es/security/business/security-101/what-is-a-cyberattack

Muhammad Nadeem, A. A. (31 de Octubre de 2022). *Preventing Cloud Network from Spamming Attacks Using Cloudflare and.* Obtenido de Tech Science Press: http://dx.doi.org/10.32604/cmc.2023.028796

Neupane, K., Haddad, R., & Lei, C. (2021). *Next Generation Firewall for Network Security: A Survey.* Obtenido de Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV): https://ieeexplore.ieee.org/document/8478973

OWASP. (7 de Octubre de 2022). *TOP 10.* Obtenido de OWASP: https://owasp.org/Top10/es/

Rodriguez, A. G., Yepez Holgin, J., Peralta Guaraca, T., & Ortiz Zambrano, M. (2018). Defensa en profundidad aplicado a un entorno empresarial. *Espacios*, 7. Obtenido de https://www.revistaespacios.com/a18v39n42/a18v39n42p19.pdf

SAP. (17 de Abril de 2013). *Implementation Tools.* Obtenido de Implementation Methodology: https://help.sap.com/doc/saphelpiis_hc_b1_image_repository_consultant_training_basic_b1_90_tb1200_01_01_pdf/9.0/en-US/B1_90_TB1200_01_01.pdf

Taeyong, K., Taewoong, K., Lee, J., & Jungsuk, S. (26 de Julio de 2021). *F/Wvis: Hierarchical Visual Approach for Effective Optimization of Firewall Policy.* Obtenido de IEEE Access: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9496640

World Economic Forum. (2020). *The Global Risks Report 2020 15th Edition.* Obtenido de weforum: https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf