REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

WEB APPLICATION FIREWALL (WAF) COMO SOLUCIÓN DE SEGURIDAD MEDIANTE LA METODOLOGÍA OWASP PARA LA PROTECCIÓN DE APLICACIONES EN EL SERVIDOR WEB DE LA UNIVERSIDAD TÉCNICA DEL NORTE.

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con mención en Seguridad Informática

AUTORA: Ing. Gabriela Elizabeth Cárdenas Rosero

DIRECTORA: PhD. Cathy Pamela Guevara Vega

IBARRA - ECUADOR

2023

APROBACIÓN DEL TUTOR

En calidad de tutora del trabajo de grado, presentado por la Ing. Gabriela Elizabeth Cárdenas Rosero, para optar por el título de Magíster en Computación con mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a presentación pública y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los veintiocho días del mes de noviembre del 2023.

1002334835 CATHY PAMELA GUEVARA VEGA

Firmado digitalmente por 1002334835 CATHY PAMELA GUEVARA VEGA
Fecha: 2023.11.28 20:41:46 -05'00'

PhD. Cathy Pamela Guevara Vega
C.C: 1002334835
TUTORA

APROBACIÓN DE ASESOR

En calidad de asesor del trabajo de grado, titulado: "Web Application Firewall (WAF) como solución de seguridad mediante la Metodología OWASP para la protección de aplicaciones en el servidor web de la Universidad Técnica del Norte", comunico que, según mi leal saber y entender, la maestrante Ing. Gabriela Elizabeth Cárdenas Rosero, ha aprobado su informe de investigación para optar por el título de Magíster en Computación con mención en Seguridad Informática y considero que el documento presentado cumple con los requerimientos exigidos en este proceso académico.

En la ciudad de Ibarra, a los veintiocho días del mes de noviembre del 2023.

PABLO ANDRES LANDETA LOPEZ

Firmado digitalmente por PABLO ANDRES LANDETA LOPEZ
Fecha: 2023.11.28 22:16:59 -05'00'

Msc. Pablo Andrés Landeta López
C.C: 1002161055
ASESOR

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	0401442330		
APELLIDOS Y NOMBRES:	CÁRDENAS ROSERO GABRIELA ELIZABETH		
DIRECCIÓN:	DANIEL REYES Y GUILLERMO GARZÓN		
EMAIL:	gecardenas@utn.edu.ec		
TELÉFONO FIJO:	s/n	**TELÉFONO MÓVIL:**	0969001106
DATOS DE LA OBRA			
TÍTULO:	WEB APPLICATION FIREWALL (WAF) COMO SOLUCIÓN DE SEGURIDAD MEDIANTE LA METODOLOGÍA OWASP PARA LA PROTECCIÓN DE APLICACIONES EN EL SERVIDOR WEB DE LA UNIVERSIDAD TÉCNICA DEL NORTE.		
AUTOR (ES):	ING. CÁRDENAS ROSERO GABRIELA ELIZABETH		
FECHA: DD/MM/AAAA	28/11/2023		
SOLO PARA TRABAJOS DE TITULACIÓN			
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**		
TITULO POR EL QUE OPTA:	Magíster en Computación con mención en Seguridad Informática.		
DIRECTOR:	PhD. Cathy Pamela Guevara Vega		
ASESOR:	Msc. Pablo Andrés Landeta López		

2. CONSTANCIAS

La autora manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es la titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 28 días del mes de noviembre de 2023.

LA AUTORA:

GABRIELA ELIZABETH CARDENAS ROSERO

Firmado digitalmente por GABRIELA ELIZABETH CARDENAS ROSERO
Fecha: 2023.11.28 14:17:10 -05'00'

……
Ing. Gabriela Elizabeth Cárdenas Rosero
C.C: 0401442330

DEDICATORIA

A mi esposo Jefferson y mi hija Nicole que son mi motivación, porque a pesar de que el viento no esté a nuestro favor siempre me demuestran su amor, gracias por apoyarme en mis locuras, los amo hasta el ¡infinito y más allá.!

Gaviota.

AGRADECIMIENTO

Quiero agradecer infinitamente a Dios por permitirme conocer su grandeza en los momentos más difíciles, agradecer a mis padres por su apoyo incondicional, a mi hija Nicole por ser mi inspiración, a la Universidad Técnica del Norte por forjar profesionales de excelencia, y como no agradecer al Programa de Becas Fortalécete del Gobierno del Ecuador del cual fui beneficiaria.

Gaviota.

ÍNDICE DE CONTENIDOS

APROBACIÓN DEL TUTOR 2
APROBACIÓN DE ASESOR 3
DEDICATORIA 6
AGRADECIMIENTO 7
ÍNDICE DE CONTENIDOS 8
RESUMEN 16
SUMMARY 17
INTRODUCCIÓN 18
CAPÍTULO I 19
EL PROBLEMA 19
1.1. Problema de investigación 19
1.2. Interrogante de la investigación 20
1.3. Objetivos de la investigación 20
1.3.1. Objetivo general 20
1.3.2. Objetivos específicos 20
1.4. Justificación 21
CAPÍTULO II 23
MARCO REFERENCIAL 23
2.1. Antecedentes 23
2.2. Marco teórico 24
2.2.1. Introducción a la ciberseguridad 24
2.2.2. Tipos de malware 25
2.2.3. Riesgos de ataque 26
2.2.4. Análisis de riesgos e impactos 27
2.2.5. Entornos web 28
2.2.6. Características de los servidores web 28
2.2.7. Tipos de servidores web 30
2.2.8. Sistema de Gestión de contenidos CMS 31
2.2.9. Características de un sistema de gestión de contenidos (CMS) 32
2.2.10. Sistema de gestión de contenidos (CMS) más populares 33
2.2.11. Posicionamiento web SEO 36
2.2.12. Web Application Firewall 36

2.2.13. Firewall como herramienta de seguridad 37
2.2.14. Políticas de los firewalls 37
2.2.15. Políticas de seguridad informática 38
2.2.16. Seguridad en la nube 38
2.2.17 Amenazas en la nube 39
2.2.18. Fortinet 40
2.2.19. FortiWeb 40
2.2.20. Open Web Application Security Project (OWASP) 41
2.2.21. Top 10 del OWASP 42
2.2.22. Tipos de ataques 44
2.2.23. Guía de pruebas de seguridad web de OWASP 45
2.2.24. Cómo hacer referencia a escenarios WSTG 45
2.2.25. Adaptación y priorización 45
2.3. Marco legal 46
CAPÍTULO III 48
MARCO METODOLÓGICO 48
3.1. Descripción del área de estudio 48
3.1.1. Organigrama estructural de Dirección de Desarrollo Tecnológico e Informático (DDTI) 48
3.1.2. Población 49
3.1.3. Muestra 49
3.2. Enfoque y tipo de investigación 50
3.2.1. Técnica de investigación 50
3.2.2. Instrumentos de investigación 50
3.3. Procedimiento de investigación 51
3.4. Consideraciones bioéticas 52
3.5. Recursos 53
3.6. Cronograma de actividades 53
CAPITULO IV 55
RESULTADOS Y DISCUSIÓN 55
4.1. Análisis de resultados de la encuesta 55
CAPÍTULO V 73
PROPUESTA 73
Título de la propuesta 73
Objetivo 73

Introducción 73
Primera fase de ejecución 73
Definir aplicaciones web que se van a proteger 74
Analítica y tráfico web de dominio utn.edu.ec 76
Segunda fase de ejecución 78
Configuración de Web Application Firewall en Fortinet 78
Cambios de direcciones IPs en el registro DNS 79
Tercera Fase de ejecución 81
Introducción Guía de Pruebas de OWASP WSTG 81
Metodología de pruebas OWASP 82
Pruebas de penetración 82
Laboratorio para escaneo de vulnerabilidades web 83
Instalación de MV Kali Linux 83
Instalación de OWASP ZAP 83
Cuarta Fase de ejecución 85
Pruebas de seguridad de aplicaciones web según la Metodología OWASP Web Security Testing Guide (WSTG) 85
Resultados de análisis de vulnerabilidades 87
A01:2021-Broken Access Control 87
A05:2021-Security Misconfiguration 88
A05:2021- Security Misconfiguration 88
A06:2021- Vulnerable and Outdated Components 89
A05:2021- Security Misconfiguration 89
A01:2021-Broken Access Control 90
A08:2021 – Software and Data Integrity Failures 90
A05:2021- Security Misconfiguration 91
A01:2021-Broken Access Control 91
A05:2021- Security Misconfiguration 92
A01:2021-Broken Access Control 93
Informativa 93
WSTG-v42-ATHN-06 94
WSTG-v42-ATHN-06 95
WSTG-v42-ATHN-06 96
Técnica de reconocimiento y transferencia de zona 96
Obtener los nombres de dominio 99

Meta archivos del servidor 101
Evaluación del WAF 101
Principales tipos de detección de ataques 101
Reportes del WAF 102
CONCLUSIONES Y RECOMENDACIONES 106
CONCLUSIONES 106
REFERENCIAS BIBLIOGRÁFICAS 109

ÍNDICE DE TABLAS

Tabla 1. Características de los servidores web 30
Tabla 3. Características de los CMS 33
Tabla 4. Políticas de seguridad 38
Tabla 5. Top 10 del OWASP 44
Tabla 6. Tipos de ataques en aplicaciones web 45
Tabla 7. Muestra del personal de la Dirección de Desarrollo Tecnológico e Informático (Nivel operativo) 50
Tabla 8. Cronograma de actividades realizados para proyecto de investigación 54
Tabla 9. Género DDTI 55
Tabla 10. Nivel Operativo DDTI 56
Tabla 11. La alta dirección entiende participa y toma decisiones relacionadas con la seguridad de la información Fuente: Encuesta autoría propia (2023) 57
Tabla 12. Se han asignado recursos, tanto financieros como humanos, para implementar y mantener medidas de seguridad informática efectivas 58
Tabla 13. Está familiarizado con Open Web Application Security Project (OWASP) top 10 59
Tabla 14. Qué nivel de conocimiento tiene sobre las vulnerabilidades más comunes de Open Web Application Security Project (OWASP) top 10 60
Tabla 15. Con que frecuencia ha utilizado un Sistema de Gestión de Contenido (CMS) de código abierto (por ejemplo, WordPress, Joomla, Drupal) 61
Tabla 16. Cree usted que los Content Management System (CMS) presentan vulnerabilidades o fallos de seguridad Fuente: Encuesta autoría propia (2023) 62
Tabla 17. Está de acuerdo que la metodología OWASP es importante para la seguridad de las aplicaciones web Fuente: Encuesta autoría propia (2023) 63
Tabla 18.Con qué frecuencia ha utilizado herramientas de pentesting para evaluar la seguridad de sistemas, redes y aplicaciones web 64
Tabla 19. Nivel de experiencia con aplicaciones en la nube 65
Tabla 20. Amenazas de seguridad en la nube 67
Tabla 21. Está de acuerdo en la implementación de una capa adicional de seguridad para proteger las aplicaciones web contra posibles amenazas y vulnerabilidades en el servidor web de la UTN 68
Tabla 22. Recomendaría el uso de una aplicación de código abierto para realizar pruebas de pentesting en el servidor web de la UTN 69
Tabla 23. Está de acuerdo que se utilice la metodología OWASP para identificar y corregir vulnerabilidades en el servidor web de la UTN 70
Tabla 24. Características de servidor web – UTN 74
Tabla 25. Sitios web protegidos por el WAF 79
Tabla 26. Registro de nuevas direcciones IPs en el DNS 80
Tabla 27. Análisis de vulnerabilidad Cross-Domain Misconfiguration en dominio utn.edu.ec 88
Tabla 28. Análisis de vulnerabilidades Content security policy (CSP) 88

Tabla 29. Análisis de vulnerabilidad Missing Anti-clickjacking Header..... 89
Tabla 30. Análisis de vulnerabilidad Vulnerable JS Library..... 89
Tabla 31. Análisis de vulnerabilidad Cookie Without Secure Flag en dominio utn.edu.ec 90
Tabla 32. Análisis de vulnerabilidad Cookie without SameSite Attribute..... 90
Tabla 33. Análisis de la vulnerabilidad Cross-Domain JavaScript Source File Inclusion 91
Tabla 34. Análisis de vulnerabilidad Strict-Transport-Security Header Not Set 91
Tabla 35. Análisis de vulnerabilidad Timestamp Disclosure..... 92
Tabla 36. Análisis de vulnerabilidad X-Content-Type-Options Header Missing 92
Tabla 37. Análissi de vulnerabilidad Information Disclosure - Suspicious Comments. 93
Tabla 38. Análisis de vulnerabilidad Information Disclosure - Suspicious Comments. 93
Tabla 39.Análisis de vulnerabilidades Re-examine Cache-control Directives 94
Tabla 40. Análisis de vulnerabilidades Retrieved from Cache 95
Tabla 41. Análisis de vulnerabilidad Session Management Response Identified 96
Tabla 42. Análisis de meta archivos dominio utn.edu.ec 101
Tabla 43. Tipos de ataques detectados por el WAF con más frecuencia en el mes de septiembre 2023..... 102

ÍNDICE DE FIGURAS

Figura 1. Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. 23
Figura 2. Análisis de riesgos e impactos 27
Figura 3. Impactos, funciones críticas y sus dependencias 28
Figura 4. Servidores más populares 31
Figura 5. Mayores amenazas de seguridad en las nubes públicas 40
Figura 6. Principales ataques según la metodología Open Web Application Security Project (OWASP) 41
Figura 7. Diagrama de la estructura DDTI 49
Figura 8. Procedimiento de investigación 52
Figura 9. Género DDTI 55
Figura 10. Nivel Operativo DDTI 56
Figura 11. La alta dirección entiende participa y toma decisiones relacionadas con la seguridad de la información Fuente: Encuesta autoría propia (2023) 57
Figura 12. Se han asignado recursos, tanto financieros como humanos, para implementar y mantener medidas de seguridad informática efectivas 58
Figura 13. Está familiarizado con Open Web Application Security Project (OWASP) top 10 59
Figura 14. Qué nivel de conocimiento tiene sobre las vulnerabilidades más comunes de Open Web Application Security Project (OWASP) top 10 60
Figura 15. Con que frecuencia ha utilizado un Sistema de Gestión de Contenido (CMS) de código abierto (por ejemplo, WordPress, Joomla, Drupal) 61
Figura 16. Cree usted que los Content Management System (CMS) presentan vulnerabilidades o fallos de seguridad 62
Figura 17. Está de acuerdo que la metodología OWASP es importante para la seguridad de las aplicaciones web Fuente: Encuesta autoría propia (2023) 63
Figura 18. Con que frecuencia ha utilizado herramientas de pentesting para evaluar la seguridad de sistemas, redes y aplicaciones web 64
Figura 19. Nivel de experiencia con aplicaciones en la nube 66
Figura 20. Amenazas de seguridad en la nube. 67
Figura 21. Está de acuerdo en la implementación de una capa adicional de seguridad para proteger las aplicaciones web contra posibles amenazas y vulnerabilidades en el servidor web de la UTN 68
Figura 22. Recomendaría el uso de una aplicación de código abierto para realizar pruebas de pentesting en el servidor web de la UTN 69
Figura 23. Está de acuerdo que se utilice la metodología OWASP para identificar y corregir vulnerabilidades en el servidor web de la UTN 70
Figura 24. Pantalla de panel de administrador en ISPConfig para la administración de sitios web de la UTN. 75
Figura 25. Analítica web utn.edu.ec (abril - sept 2023) 76
Figura 26. Analítica web dominio utn.edu.ec mes (mayo-septiembre 2023) 78
Figura 27. Configuración de política de seguridad en el WAF 79

Figura 28. Registro de Ip en el DNS dominio www.utn.edu.ec 80
Figura 29. Verificar la dirección Ip del sitio web utn.edu.ec 80
Figura 30. Verificar si el sitio web utn.edu.ec se encuentra protegido por el WAF 81
Figura 31. Pantalla de inicio de sesión de Kali..... 83
Figura 32. Instalación de OWASP ZAP..... 84
Figura 33. Pantalla de bienvenida de OWASP ZAP 84
Figura 34. Ataque al dominio utn.edu.ec en Aplicación OWASP ZAP..... 86
Figura 35. Alertas detectadas por OWASP ZAP..... 86
Figura 36. Búsqueda en Google dominio utn.edu.ec..... 97
Figura 37. Directiva caché de Google 97
Figura 38. Escaneo de puertos dominio utn.edu.ec 98
Figura 39. Registro MX de dominio utn.edu.ec 98
Figura 40. Figura 39. Nombres de dominio utn.edu.ec 99
Figura 41. Ping al DNS ns1.utn.edu.ec 99
Figura 42. Verificar registro TXT dominio utn.edu.ec..... 99
Figura 43. Listado de subdominios identificados..... 100
Figura 44. Reporte WAF- ataques más frecuentes periodo: 2023-09-24 hasta 2023-09-30 103
Figura 45. Ataques más frecuentes periodo octubre 15 al 20 de octubre 2023..... 104
Figura 46. Direcciones Ip con más intentos de ataque Fuente: Reporte WAF - UTN 104
Figura 47. Países de origen con más intentos de ataque..... 105
Figura 48. Host con más intentos de ataque. 105

WEB APPLICATION FIREWALL (WAF) COMO SOLUCIÓN DE SEGURIDAD MEDIANTE LA METODOLOGÍA OWASP PARA LA PROTECCIÓN DE APLICACIONES EN EL SERVIDOR WEB DE LA UNIVERSIDAD TÉCNICA DEL NORTE.

Autor: Ing. Gabriela Elizabeth Cárdenas Rosero
Tutor: PhD. Cathy Pamela Guevara Vega
Año: 2023

RESUMEN

La Universidad Técnica del Norte, como una decisión estratégica para garantizar la seguridad y proteger las aplicaciones web, implementó un Web Application Firewall (WAF), teniendo en cuenta que ofrece una capa adicional de seguridad al neutralizar amenazas e identificar los principales tipos de ataque detectados que podrían ser aprovechados, ayudando a reducir los riesgos y manteniendo la disponibilidad de los servicios en línea.

En el transcurso de esta investigación se caracterizó los principales tipos de ataques detectados por el WAF, de esta manera se determinó la eficacia en la detección y prevención de ataques web mediante la Guía pruebas de seguridad de OWASP, que se centra en proporcionar directrices y mejores prácticas de seguridad en aplicaciones web, su objetivo principal es garantizar que los sitios web de la UTN sean resistentes a las amenazas y vulnerabilidades comunes.

Adicional se proporcionó a los administradores web una analítica del WAF, de los ataques más frecuentes que han sido bloqueados por el Firewall; para que se tomen medidas de protección para reducir el riesgo de que una aplicación web sea comprometida, cumpliendo con los estándares de seguridad y protegiendo los datos sensibles del servidor web de la UTN.

Palabras clave: WAF, OWASP, seguridad, Firewall, servidor web, ataques.

WEB APPLICATION FIREWALL (WAF) AS A SECURITY SOLUTION THROUGH THE OWASP METHODOLOGY FOR THE PROTECTION OF APPLICATIONS ON THE WEB SERVER OF THE TECNICA DEL NORTE UNIVERSITY

Author: Ing. Gabriela Elizabeth Cárdenas Rosero
Tutor: PhD. Cathy Pamela Guevara Vega
Año: 2023

SUMMARY

The Universidad Técnica del Norte, as a strategic decision to guarantee security and protect web applications, implemented a Web Application Firewall (WAF), taking into account that it offers an additional layer of security by neutralizing threats and identifying the main types of attacks detected that could be leveraged, helping to reduce risks and maintaining the availability of online services.

During this research, the main types of attacks detected by the WAF were characterized, in this way the effectiveness in detecting and preventing web attacks was determined through the OWASP Security Testing Guide, which focuses on providing guidelines and best practices. security practices in web applications,
Its primary goal is to ensure that UTN websites are resilient to common threats and vulnerabilities.

Additionally, web administrators were provided with WAF analytics of the most frequent attacks that have been blocked by the Firewall; so that protective measures are taken to reduce the risk of a web application being compromised, complying with security standards and protecting sensitive data on the UTN web server.

Keywords: WAF, OWASP, security, Firewall, web server, attacks.

INTRODUCCIÓN

Las organizaciones han tenido que adoptar medidas de seguridad informática, conscientes del impacto que pueden sufrir en sus operaciones debido a un mal desempeño de sus sitios o aplicaciones web. Hoy en día todo es una estrategia de negocio que puede marcar la diferencia entre el éxito y la derrota, el administrador web debe conocer su arquitectura desde el diseño hasta el back end para que el contenido sea rápido, eficiente y efectivo, además de las tecnologías que existen para acelerar y asegurar la entrega desde el servidor web hasta el navegador del usuario final.

Internet se ha convertido en una imprescindible herramienta para la sociedad moderna, ya que el avance tecnológico y la interconexión son fundamentales para el funcionamiento del mundo actual. No se limita únicamente a navegar por la web y visitar sitios; ahora engloba aspectos como la socialización, las compras en línea, la evitación de colas en los bancos, la visualización de películas bajo demanda, la participación en eventos en tiempo real, la educación en línea y una amplia gama de servicios al alcance de un solo clic. (Picado y Pérez, 2021).

Dado lo expuesto resulta pertinente hablar del campo de la seguridad informática que se encarga de generar buenas prácticas, destinadas a garantizar sistemas de información seguros y confiables antes posibles riesgos. La seguridad informática busca reducir la posibilidad de que se materialicen los riesgos. De acuerdo con la información de Networking Academy (2023), en la época actual, el crecimiento y la expansión de internet son fenómenos notables. A lo largo de los años, hemos sido testigos de los progresos tecnológicos, y en la actualidad, hay literalmente miles de millones de dispositivos conectados en línea. Con la constante evolución, surgen nuevas amenazas en ciberseguridad a cada segundo, lo que hace que nuestro mundo sea cada vez más susceptible a los ataques cibernéticos.

CAPÍTULO I
EL PROBLEMA

1.1. Problema de investigación

La Universidad Técnica del Norte, es una universidad pública ubicada en la provincia de Imbabura, cuyo campus principal se encuentra en la ciudad de Ibarra, se caracteriza por su enfoque en la formación técnica y científica de sus estudiantes, ofreciendo programas académicos en diversas áreas del conocimiento, tanto a nivel de pregrado como posgrado, cuenta con una población estudiantil de 16.000 usuarios que se conectan simultáneamente a los servicios tecnológicos que ofrece la UTN, uno de ellos es el servicio web que alberga alrededor de 50 sitios web distribuidos para congresos, blogs de carrera, posgrado, biblioteca y portal principal, que proporcionan un punto de encuentro virtual entre la universidad y la comunidad en general con temas de interés sobre proyectos de investigación, eventos culturales, actividades deportivas y programas de vinculación que involucran a la comunidad local y nacional.

En la UTN la plataforma de gestión de contenidos ampliamente utilizada en todo tipo de sitios web es WordPress por su amplia popularidad también la convierte en un objetivo frecuente para los ciberdelincuentes ya que el hecho de que utiliza complementos y temas gratuitos que tienen fallos de seguridad. Sin embargo, los ataques de fuerza bruta son intentos repetidos y automatizados de adivinar las credenciales de inicio de sesión de administradores, lo que puede dar a los atacantes acceso no autorizado al sitio.

Los sitios web están expuestos a una amplia gama de amenazas, si una aplicación web no protege adecuadamente la información confidencial, como nombres de usuario, contraseñas u otra información personal, los atacantes pueden acceder y utilizar esos datos para fines maliciosos, como el robo de identidad. Algunos tipos de ataques se producen cuando insertan scripts maliciosos en páginas web legítimas, lo que permite la ejecución de código en el navegador de los usuarios que acceden a dichas páginas. Esto lleva al robo de información confidencial, como contraseñas o cookies de sesión (Sevillano, 2021).

El incremento exponencial de los datos que circulan en la red y las amenazas crecientes hacia aplicaciones web han evolucionado y se han vuelto más sofisticadas, con

el tiempo los atacantes han desarrollado técnicas avanzadas para eludir las medidas de seguridad y comprometer la seguridad de las aplicaciones haciendo necesario que la universidad cuente con un mecanismo de protección que sea efectivo y eficiente (Pavón, 2019).

1.2. Interrogante de la investigación

¿Cuáles son las principales vulnerabilidades y amenazas que un WAF puede ayudar a mitigar?

¿Cuáles son los ataques más frecuentes detectados según la metodología OWASP en el servidor web de la Universidad Técnica del Norte?

¿Cuáles son las mejores prácticas para evaluar la efectividad de un WAF en la protección de una aplicación web?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Evaluar la efectividad Web Application Firewall (WAF) como solución de seguridad mediante la metodología OWASP para detectar y bloquear los ataques en el servidor web de la UTN.

1.3.2. Objetivos específicos

- Implementar una capa adicional de seguridad para proteger las aplicaciones web contra posibles amenazas y vulnerabilidades de seguridad en el servidor web de la UTN.
- Caracterizar los principales tipos de ataque detectados por el WAF que pueden ser explotados y tomar medidas de protección adecuadas para reducir el riesgo de que una aplicación web sea comprometida.
- Determinar la eficacia del Firewall en la detección y prevención de ataques web mediante pruebas de penetración OWASP que implica ataques simulados contra las aplicaciones web protegidas por el WAF.
- Proporcionar a los administradores web una analítica del WAF, de los ataques más frecuentes que han sido bloqueados por el Firewall.

1.4. Justificación

En la última década, la cuestión de la conectividad ha evolucionado hacia una dimensión más compleja y exigente. Ya no se trata únicamente de proporcionar acceso a Internet a nivel global. Ahora, el enfoque se centra en lograr una conectividad universal que garantice una experiencia en línea segura, satisfactoria, enriquecedora, productiva y asequible. Lamentablemente, los países menos desarrollados están lejos de alcanzar este objetivo. La brecha digital entre estos países y el resto del mundo parece mantenerse sin reducirse significativamente. A medida que el mundo adquiere cada vez más experiencia en aprovechar Internet para generar valor, los países menos desarrollados corren el riesgo de quedarse aún más rezagados. (ONU, 2023).

A diario se producen numerosos ciberataques; cuando alguno de ellos es detectado surgen varias preguntas, es probable que nunca se pueda identificar al atacante y lo que aún es más preocupante para muchas organizaciones es si podrá recuperarse de los daños y recuperar la información perdida. El objetivo de la ciberseguridad es minimizar los riesgos, reduciendo las vulnerabilidades y bloquear las amenazas en un proceso continuo que va desde la detección de las vulnerabilidades hasta el análisis de los ataques recibidos, basándonos en el monitoreo en tiempo real de lo que sucede en los sitios web (Herrero, 2022)

Implementar un Web Application Firewall (WAF) es una decisión estratégica y necesaria para garantizar la seguridad. Un WAF ayuda a proteger las aplicaciones web contra una amplia variedad de ataques comunes, como inyección de código SQL, ataques de fuerza bruta, ataques de cross-site scripting (XSS) y muchos otros. Al filtrar y bloquear estas amenazas conocidas, el WAF puede prevenir eficazmente la explotación de vulnerabilidades y reducir el riesgo de comprometer la seguridad de la aplicación. Además de proteger contra ataques conocidos, un WAF también puede detectar y mitigar ataques desconocidos o de día cero, utilizando técnicas de detección de anomalías y análisis de comportamiento, un WAF puede identificar patrones de tráfico malicioso y tomar medidas para bloquear o limitar esos intentos de ataque. Esto proporciona una capa adicional de seguridad para enfrentar amenazas emergentes y evolutivas (Pavón, 2019).

Finalmente, acorde a las líneas de investigación contempladas para la propuesta de investigación “Web Application Firewall (WAF) como solución de seguridad mediante la metodología OWASP para la protección de aplicaciones en el servidor web

de la Universidad Técnica del Norte", se atribuye a la línea denominada "Desarrollo, aplicación de software y cyber security (seguridad cibernética)".

CAPÍTULO II
MARCO REFERENCIAL

2.1. Antecedentes

En los últimos años, ha habido un aumento significativo en los ataques dirigidos a aplicaciones web como expresa Akamai (2023), los ciberdelincuentes aprovechan las vulnerabilidades conocidas y desconocidas para infiltrarse en sistemas, robar datos confidenciales, comprometer la integridad de las aplicaciones o interrumpir los servicios. Estos ataques pueden acarrear consecuencias devastadoras en términos de pérdida de datos, daño a la reputación y costos financieros.

De acuerdo con Gonzáles (2018), el artículo de investigación titulado "Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web" analiza las capacidades para la detección de vulnerabilidades y propone las principales metodologías de pruebas de penetración ISSAF, OSSTMM, OWASP, PTES y NIST SP 800-115, obteniendo como resultado que la Guía de Pruebas de Open Web Application Security Project (OWASP) resulta la más completa, seguida de la metodología de ISSAF.

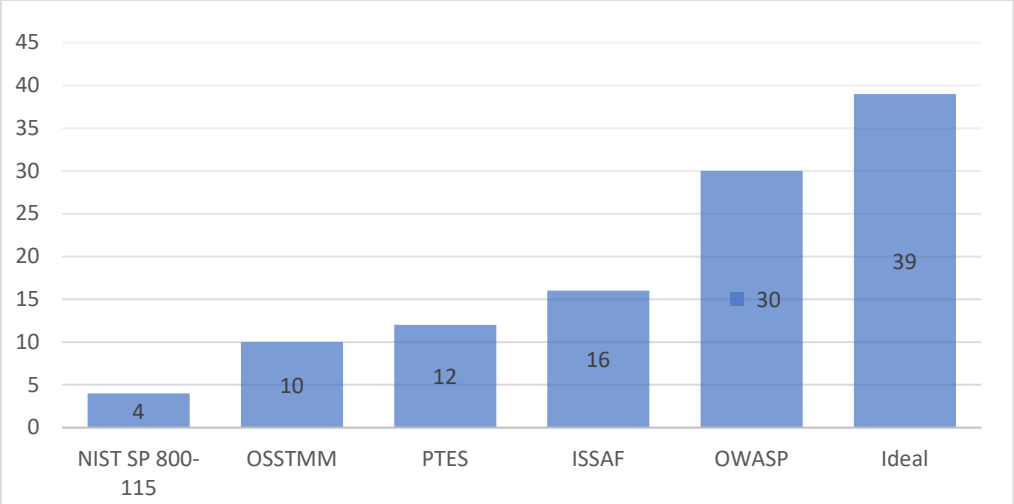


Figura 1. Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web.
Fuente: Tomado de González. (2018). http://scielo.sld.cu/pdf/rcci/v12n4/rcci05418.pdf

La relevancia de una solución WAF como segmento de seguridad en los sitios web de la Universidad Técnica del Norte con el fin de garantizar la confidencialidad, integridad disponibilidad de la información, basado en la Metodología OWASP que está divida en varios grupos de pruebas de seguridad que comprueban aspectos específicos de las aplicaciones web, teniendo en cuenta que la Guía de Pruebas de OWASP resulta la más completa y más adecuada para ser tomada como base en las prueba de penetración en aplicaciones web.

Bonilla (2018) realizó una investigación con el tema "Identificación y Diseño de las reglas de detección de amenazas de INEGI para un Web Application Firewall", en el cual manifiesta que la mayoría de los WAF tiene un costo, donde Qualys y Fortinet son de los más costosos por su tecnología usada y son muy buenas opciones porque tienen aprendizaje de amenazas y estaban basados en el top ten de OWASP. A demás el autor recomienda para futuras investigaciones relacionadas con el tema de investigación se puede ampliar las amenazas detectadas, incluyendo todo el Top 10 de OWASP.

Vega, et al., (2022) realizaron un artículo científico sobre "Análisis de factores de seguridad informática mediante la metodología OWASP v4.2: Caso de estudio ISTJOL" se enfatiza la importancia del OWASP Testing Guide como una guía principal para la detección de vulnerabilidades en una amplia variedad de aplicaciones y servidores. Esta guía goza de una elevada reputación y eficacia, lo que la convierte en una elección frecuente de diversas entidades que buscan asegurar la seguridad y el funcionamiento de sus aplicaciones web. OWASP ha adquirido renombre a nivel mundial en el ámbito de la seguridad informática y ha acumulado numerosos casos de éxito. Por lo tanto, para llevar a cabo la investigación en curso, se han considerado algunas de las soluciones proporcionadas por esta guía, las cuales están disponibles en su página web oficial.

2.2. Marco teórico

2.2.1. Introducción a la ciberseguridad

De acuerdo con Cisco Networking Academy (2022), la ciberseguridad es el esfuerzo continuo para proteger a las personas, las organizaciones y los gobiernos de los ataques digitales mediante la protección de los sistemas y datos en red contra el uso o daño no autorizados. A nivel personal, debe proteger su identidad, sus datos y sus dispositivos informáticos. A nivel corporativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la organización. A medida que se recopila y

comparte más información digital, su protección se vuelve aún más vital a nivel gubernamental, donde la seguridad nacional, la estabilidad económica y la seguridad y el bienestar de los ciudadanos están en juego.

Muchos investigadores y autores especializados en el tema de la seguridad informática se centran en que las características que debe poseer la información son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a los estándares y confiabilidad que se basan de acuerdo con el marco de gestión y de negocio global para el gobierno y la gestión de las Tecnologías de la Información (TI) de las empresas COBIT (Baca, 2016).

Según Baca (2016), define la seguridad informática como la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. Definitivamente para nadie es un secreto que los datos crecen cada día a ritmos vertiginosos y que estos datos se han convertido en el principal activo de cualquier empresa, la información en la actualidad es el nuevo oro digital.

2.2.2. Tipos de malware

Los delincuentes cibernéticos emplean una variedad de software perjudicial, conocido como malware, con el propósito de llevar a cabo sus acciones. El malware se define como cualquier tipo de código diseñado para sustraer datos, evadir sistemas de seguridad o causar daño o vulnerar un sistema. Conocer los distintos tipos de malware y sus métodos de propagación resulta esencial para controlar y erradicar estas amenazas. (Cisco Networking Academy, 2022).

Spyware: Creado con el propósito de seguir y observar sus actividades, el spyware supervisa su comportamiento en línea y tiene la capacidad de registrar cada pulsación de tecla que realice en su teclado, capturando así prácticamente todos sus datos, incluyendo información personal confidencial, como sus datos bancarios en línea. Este tipo de software malicioso altera las configuraciones de seguridad de sus dispositivos. A

menudo, el spyware se distribuye junto con aplicaciones legítimas o se camufla como troyanos (Sevillano, 2021).

Adware: El adware a menudo se instala con algunas versiones de software y estádiseñado para entregar automáticamente anuncios a un usuario, la mayoría de las veces en un navegador web. Es común que el adware venga con spyware (Cisco Networking Academy, 2022).

Ransomware: El ransomware a menudo se propaga a través de correos electrónicos de phishing que lo alientan a descargar un archivo adjunto malicioso o a través de una vulnerabilidad (Cybersecurity Insiders, 2023).

Rootkits: Este malware pueden modificar las herramientas de monitoreo y análisis forense del sistema, lo que los hace muy difíciles de detectar. En la mayoría de los casos, un equipo infectado por un rootkit debe borrarse y reinstalarse cualquier software necesario (Cisco Networking Academy, 2022).

Virus: es una forma de software que, una vez activado, se duplica y se adhiere a otros archivos ejecutables, como documentos, al incorporar su propio código. La mayoría de los virus dependen de la interacción del usuario final para desencadenar su activación y pueden ser programados para operar en momentos específicos, según una fecha o una hora predeterminada. Los virus pueden ser relativamente inofensivos, como los que muestran una imagen divertida. O pueden ser destructivos, como los que modifican o eliminan datos (Cisco Networking Academy, 2022).

Troyanos: A diferencia de los virus, los troyanos no se replican a sí mismos, sino que actúan como señuelo para colar software malicioso a los usuarios desprevenidos.

2.2.3. Riesgos de ataque

Según López (2010), se entiende como riesgo la probabilidad de que una amenaza se materialice al explotar una vulnerabilidad. No se considera un riesgo cuando no existe una vulnerabilidad presente. Cuando una organización se enfrenta a un riesgo específico, tiene la opción de elegir entre tres alternativas:

- Asumirlo sin hacer nada. Esto resulta cuando el perjuicio esperado no tiene valor alguno.
- Aplicar medidas para disminuirlo o anularlo.
- Transferirlo

2.2.4. Análisis de riesgos e impactos

Lo primero que se debe hacer es identificar los posibles daños o peligros con el fin de tomar medidas de seguridad. Se debe tomar en cuenta el valor de los activos, la frecuencia de las amenazas, su desconocimiento, la consecuencia del daño, la eficacia de las medidas de seguridad y su costo (Palacios, 2020).

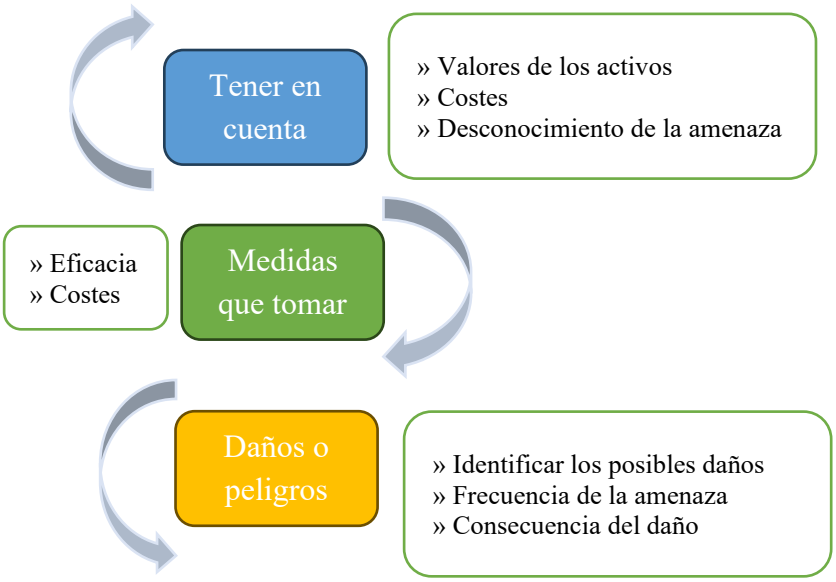


Figura 2. Análisis de riesgos e impactos
Fuente: Tomado de Palacios (2020).

Según Palacios (2020), el impacto es la consecuencia negativa que una organización padece cuando una función se ve interrumpida y ello conlleva un tiempo de recuperación permitido tal que no acarree su inactividad total, el daño producido por el impacto puede ser crítico priorizando las estrategias de recuperación para minimizar el tiempo de recuperación.

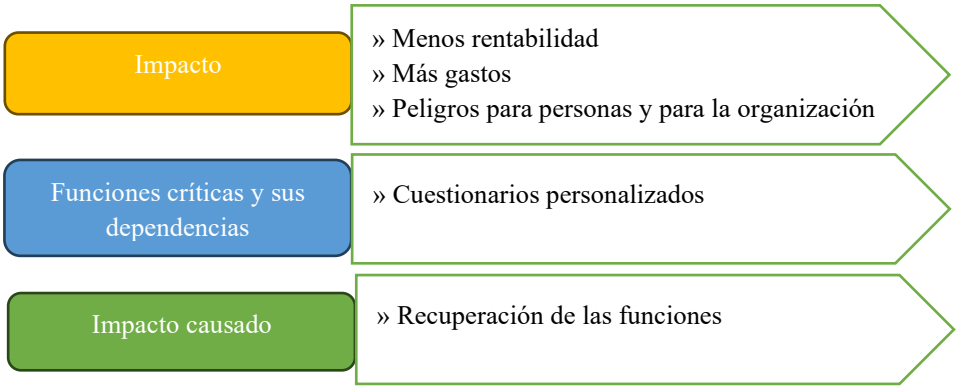


Figura 3. Impactos, funciones críticas y sus dependencias
Fuente: Tomado de Palacios (2020).

2.2.5. Entornos web

La importancia para un administrador web identificar los conceptos generales de las tecnologías detrás de un ambiente implementado para un sitio web, conocer su arquitectura de servidor y servicios de hospedaje de tal manera que permita conocer la tecnología que se encuentra detrás de una aplicación para hacer posible su acceso y buen funcionamiento. La arquitectura puede ser compleja y más si el hospedaje es contratado y es que cada vez es más común que las empresas decidan dejar en manos de terceros la administración de servicios en la nube y al fin y al cabo para que invertir en equipos de red si otros poseen la infraestructura y se puede alquilar (Quiña-Mera et al., 2021).

Además del hardware, también hay soluciones en software como sistemas operativos, además de un rol que ejecute los servicios web como Apache, Nginx, base de datos como MySQL, Oracle, SQL Server. Todo este ecosistema se pude convertir en una bomba de tiempo ya que una de estas piezas puede incluir una serie de vulnerabilidades conocidas porque hoy en día nada es infalible así que puede ser cuestión de tiempo para que la seguridad del sitio web sea vulnerada provocando una reacción en cadena tanto para los usuarios finales como para el negocio (Picado y Pérez, 2021).

2.2.6. Características de los servidores web

Según Villada Romero, J. L. (2016), la elección de un servidor web no es una tarea trivial ya que de ello depende toda la infraestructura lógica de la empresa. Además, conforme van creciendo las necesidades de las empresas, los servidores web en muchas ocasiones ya no son una sola máquina conectada al internet sirviendo HTML, sino un

sistema (grupo o cluster) de servidores interrelacionados que se coordinan para proveer los servicios a los usuarios con alta disponibilidad, seguridad y velocidad. Es importante destacar que hay varios servidores web disponibles, siendo Apache, Nginx e IIS (Internet Information Services) algunos de los más conocidos y utilizados. Cada uno tiene sus características específicas y su rendimiento puede variar según el tipo de aplicación y los requisitos del sistema (Guevara-Vega et al., 2019).

De acuerdo con Kinsta (2022), en su sitio oficial menciona que la mayoría de los proyectos web suelen requerir aplicaciones como Apache o Nginx como servidores web, bases de datos como MySQL o MariaDB, así como lenguajes de programación como PHP o Python. Este conjunto de tecnologías se ha diseñado principalmente con el sistema operativo Linux en mente. A pesar de que estos programas también son compatibles con Windows, esta plataforma no es la más adecuada para ellos de forma nativa. Además, es importante tener en cuenta que los servidores Windows tienden a ser más costosos debido a las licencias que requieren, por lo que se recomienda su uso solo si es realmente necesario.

Características	**Descripción**
Protocolos de comunicación	Los servidores web generalmente soportan los protocolos HTTP (HyperText Transfer Protocol) y HTTPS (HTTP Secure) para la comunicación segura.
Procesamiento de solicitudes	Los servidores web reciben solicitudes de los clientes y procesan esas solicitudes para recuperar los recursos solicitados, como páginas HTML, imágenes, archivos CSS, scripts, etc.
Logs y estadísticas	Los servidores web suelen mantener registros (logs) de las solicitudes y respuestas, lo que permite realizar análisis de tráfico y diagnósticos en caso de problemas.
Almacenamiento y gestión de contenido:	Los servidores web almacenan y administran el contenido web, ya sea servido directamente desde el sistema de archivos del servidor o desde una base de datos.
Direcciones IP y nombres de dominio	Cada servidor web tiene una dirección IP única y puede estar asociado con uno o varios nombres de dominio.

Seguridad	Los servidores web deben implementar medidas de seguridad para protegerse contra ataques, como firewalls, cifrado SSL/TLS, autenticación y autorización, y otros mecanismos de seguridad.
Compresión y caché	Los servidores web pueden comprimir contenido para una entrega más rápida y almacenar en caché recursos para acelerar el tiempo de carga de las páginas web repetidamente solicitadas.

Tabla 1. Características de los servidores web
Fuente: Tomado de Villada Romero, J. L. (2016)

2.2.7. Tipos de servidores web

Apache

Con base en Palma (2020), Apache es una opción popular para alojar sitios web y aplicaciones debido a su versatilidad, capacidad de personalización, confiabilidad y soporte continuo de la comunidad de desarrolladores.

Nginx

Según Palma (2020) Nginx se destaca por su rendimiento, eficiencia y versatilidad, y es ampliamente utilizado como servidor web, proxy inverso y balanceador de carga en una variedad de entornos, desde sitios web pequeños hasta aplicaciones empresariales de alto tráfico.

Microsoft Internet Information Services (IIS)

IIS goza de una gran popularidad gracias a su fortaleza, capacidad de escalabilidad y una interfaz de usuario amigable. Sin embargo, la eficiencia de los servidores web de IIS puede ser influenciada por diversos factores, entre los que se incluyen el hardware, la calidad de la conexión de red y la configuración del software. (Yunapanta, 2022).

Servidor Cloudflare

De acuerdo con Vendrell (2020), Cloudflare actúa como un intermediario entre los visitantes del sitio y el servidor original Cloudflare es una de las CDN (red de entrega de contenido) que puede hacer que el sitio web se cargue a mayor velocidad. La función principal de la CDN es salvaguardar el sitio web, la primera defensa contra los piratas informáticos, así como protección contra otras amenazas. Cloudflare tiene varios sitios de servidor en todo el mundo.

LiteSpeed

Según artículo de PR Newswire (2007), LiteSpeed se presenta como una alternativa a Apache, ya que comparten configuraciones similares y son altamente compatibles entre sí. Lo que distingue a LiteSpeed son sus mejoras en la capacidad para gestionar miles de conexiones concurrentes, un rendimiento excepcional, altos estándares de seguridad, actualizaciones automáticas en línea y una interfaz de usuario sencilla para la administración. En los últimos años, LiteSpeed ha experimentado un crecimiento significativo, acercándose al nivel de la herramienta de Microsoft para servicios web, actualmente, se utiliza en aproximadamente el 7% de todas las páginas web en Internet.

Con base en lo expuesto anteriormente se presenta una tabla con los servidores web más utilizados según sitio oficial de W3Techs, siendo Nginx el servidor web más popular con el 34,3% seguido de Apache con el 31,4%, cifras obtenidas hasta junio 2023.

© W3Techs.com	uso	cambio desde el 1 de junio de 2023
1. Nginx	34,3%	-0.1%
2. apache	31,4%	-0.5%
3. Servidor Cloudflare	20,6%	+0.1%
4. LiteSpeed	12,2%	+0,3%
5. Microsoft-IIS	5,4%	-0.1%

porcentajes de sitios

Figura 4. Servidores más populares
Fuente: Fuente: W3Techs-ecuestas de tecnología web, (https://w3techs.com/)

2.2.8. Sistema de Gestión de contenidos CMS

Cada organización es única, al igual que los actores de amenazas para esa organización, sus objetivos y el impacto de cualquier infracción. Si una organización de interés público usa un Content Management System (CMS) para la información pública y un sistema de salud usa exactamente el mismo sistema de gestión de contenidos CMS para registro de salud confidenciales, los actores de menazas y los impactos comerciales pueden ser muy diferentes para el mismo software. Es fundamental comprender el riesgo para la organización en función de los agentes de menaza aplicables y los impactos comerciales (OWASP, 2017).

2.2.9. Características de un sistema de gestión de contenidos (CMS)

De acuerdo con Rodríguez, M. (2021), se trata de una aplicación destinada a la generación y control de contenidos, particularmente en el ámbito de páginas web. Estos sistemas de administración de contenidos requieren establecer conexión con una o más bases de datos para el almacenamiento de la información del sitio web. Dentro de los CMS, es factible la creación de diversos roles, como administrador, editor, suscriptor, entre otros. Estos sistemas de administración de contenidos se caracterizan por su alta versatilidad, ya que permiten desarrollar proyectos web desde cero o emplear estructuras predefinidas. Las características de estos servicios varían de acuerdo con la finalidad que se les atribuya, y en función de esto, los CMS se clasifican de la siguiente manera:

TIPOS DE CMS	DESCRIPCIÓN
Gestores de contenidos para Empresas Corporativas	Los sistemas de gestión de contenidos (CMS) más destacados, como Joomla, Drupal y WordPress, son reconocidos por su enfoque en sitios web dinámicos y portales de contenidos. Estos CMS están equipados con herramientas estructuradas basadas en bases de datos y facilitan la gestión de perfiles de usuarios.
Gestores de contenidos para blog	Facilitan la creación de blogs de manera sencilla. Los principales sistemas de gestión de contenidos (CMS) para blogs incluyen Blogger, que es un servicio de Google que permite crear blogs en línea sin necesidad de editar o escribir código, ni de instalar programas de servidor.

Gestores de contenidos para cursos y entornos educativos	Estos sistemas permiten la generación de contenido multimedia, aulas virtuales, cursos, evaluaciones y módulos para el seguimiento de actividades, entre otras funciones. En esta categoría de CMS, se presenta una amplia variedad de roles, lo que posibilita la creación de usuarios con diferentes perfiles, tales como profesores, estudiantes, visitantes y administradores, entre otros. Moodle es el CMS más prevalente en esta categoría, y se distingue por ser de código abierto y ampliamente utilizado en instituciones públicas y gubernamentales.
Gestores de contenidos para Wikis	Estos son idóneos para trabajos colaborativos o participativos. La mayoría son fáciles de reconocer por el nombre en el dominio wiki.
Gestores de contenidos para tiendas on-line	Se han concebido con la finalidad de habilitar la realización de compras en línea y presentan características propias de un sitio de comercio electrónico, incluyendo bases de datos para gestionar productos y catálogos, entre otros elementos. PrestaShop es uno de los sistemas más empleados en esta categoría.

Tabla 2. Características de los CMS
Fuente: Tomado de Rodríguez, M. (2021)

2.2.10. Sistema de gestión de contenidos (CMS) más populares

WordPress es un sistema de gestión de sitios web de código abierto que opera mediante PHP y MySQL, y normalmente se integra con servidores de bases de datos MySQL o MariaDB, aunque también es compatible con el motor de base de datos SQLite. Su panel de administración de fácil manejo facilita la creación de sitios web modernos y

altamente funcionales. El desarrollo de WordPress se basa en PHP y MySQL, lo que permite que su código sea personalizable y que se puedan incorporar mejoras o complementos al sitio web de manera eficaz. WordPress es una herramienta de blogging de sencilla instalación y fácil adaptación conforme a los estándares web. Una de sus características destacadas es la extensa comunidad de usuarios y desarrolladores que brindan un sólido respaldo. Esta comunidad ofrece una amplia variedad de foros, grupos de usuarios y recursos en línea donde es posible obtener asistencia, acceder a tutoriales y compartir conocimientos con otros usuarios de WordPress (Bagus, 2023).

Joomla es un sistema de gestión de contenido de código abierto y gratuito que se utiliza para construir y administrar sitios web y aplicaciones en línea. Al utilizar Joomla como gestor de contenido, puedes realizar las siguientes tareas: Crear y editar contenido, organizar y categorizar el contenido, administrar usuarios y permisos, personalizar la apariencia. Una de las ventajas de Joomla es su capacidad para extender su funcionalidad mediante la instalación de extensiones. Joomla cuenta con un sistema de gestión de actualizaciones que te permite mantener tu sitio web seguro y actualizado. Puedes recibir notificaciones sobre nuevas versiones de Joomla y sus extensiones, y aplicar fácilmente las actualizaciones desde el panel de administración. (García, 2015)

Según García (2015) a pesar de sus numerosas ventajas, Joomla también tiene algunas desventajas que es importante tener en cuenta, a medida que Joomla lanza nuevas versiones, puede haber problemas de compatibilidad con algunas extensiones y plantillas de terceros. Si dependes de extensiones específicas para tu sitio web, es posible que debas esperar a que los desarrolladores de esas extensiones actualicen sus productos antes de actualizar Joomla, lo que puede retrasar el proceso de actualización y mantenimiento. Aunque Joomla cuenta con una comunidad de usuarios y desarrolladores activa y solidaria, manifiesta el autor que el soporte técnico oficial puede ser limitado. Si enfrentas problemas técnicos o necesitas asistencia especializada, puede ser necesario recurrir a expertos externos o buscar soluciones en los foros y comunidades en línea. Es importante considerar estas desventajas en relación con las necesidades y objetivos antes de decidir utilizar Joomla como CMS para un proyecto web.

Drupal es otro CMS popular utilizado para crear y gestionar sitios web. Según Yanney et al., (2023) al igual que otros sistemas de gestión de contenidos, Drupal ofrece una variedad de características y funcionalidades entre ellas:

1. Personalización avanzada: Drupal ofrece una gran capacidad de personalización y control sobre la apariencia y funcionalidad de un sitio web. Proporciona un sistema de módulos y temas que permiten ampliar y modificar el CMS según las necesidades específicas del proyecto.

2. Escalabilidad y rendimiento: Drupal está diseñado para manejar sitios web con alto tráfico y volúmenes de contenido significativos. Puede escalar para satisfacer las necesidades de crecimiento del sitio y ofrece características para mejorar el rendimiento, como caché y optimización de bases de datos.

3. Gestión de contenido estructurado: Drupal se destaca en la gestión de contenido estructurado y complejo. Permite definir diferentes tipos de contenido, campos personalizados y relaciones entre ellos, lo que facilita la creación y gestión de sitios web con contenido altamente organizado.

Aunque Drupal ofrece muchas ventajas, también tiene algunas desventajas que hay que considerar

1. Curva de aprendizaje: Drupal tiene una curva de aprendizaje más pronunciada en comparación con otros CMS más simples. Requiere un mayor nivel de familiaridad con su estructura y funcionalidades, lo que puede llevar más tiempo y esfuerzo para los principiantes.

2. Actualizaciones: Al igual que cualquier CMS, las actualizaciones regulares son importantes para mantener la seguridad y el rendimiento del sitio Drupal. Sin embargo, el proceso de actualización en Drupal puede ser más complejo debido a su arquitectura modular. Algunas actualizaciones pueden requerir más tiempo y esfuerzo para garantizar la compatibilidad de los módulos y temas personalizados.

3. Comunidad más pequeña: Aunque Drupal tiene una comunidad activa de usuarios y desarrolladores, es relativamente más pequeña en comparación con otros CMS populares como WordPress. Esto puede resultar en menos recursos y menos soporte disponible en comparación.

2.2.11. Posicionamiento web SEO

De acuerdo con Celaya Luna, A. (2014), El posicionamiento web, similar al enfoque del marketing tradicional, se refiere a la ubicación que una marca ocupa en la percepción del consumidor, es decir, la imagen que los consumidores tienen de ella en comparación con sus competidores. Este concepto se ha adaptado al contexto del posicionamiento web, que se refiere a la importancia de un sitio web específico en el entorno digital. Esta relevancia se evalúa en función de la posición que ocupa el sitio web al buscar términos relacionados con la marca en los motores de búsqueda en Internet.

Es importante entender que el posicionamiento web está relacionado con palabras claves empleadas en las búsquedas de Google, Bing, Yahoo, entre otros. Por ejemplo, la web de la UTN se basa en fuentes como *universidad ibarra*, *UTN portafolios*, *utn admisiones, oferta grado utn, oferta posgrado utn.* El SEO (Optimización para motores de búsqueda) es un proceso continuo, por lo tanto, es importante mantenerse actualizado con las mejores prácticas y ajustar las estrategias según sea necesario para mantener un buen posicionamiento web.

2.2.12. Web Application Firewall

Un WAF resguarda las aplicaciones web de una variedad de ataques en la capa de aplicación, tales como el cross-site scripting (XSS), la inyección de SQL y la manipulación de cookies, entre otros. Estos ataques a las aplicaciones son la causa principal de violaciones de seguridad, ya que representan la vía de acceso a datos críticos. Al implementar un WAF apropiado, es factible bloquear diversos tipos de ataques que tienen como objetivo comprometer los sistemas y acceder a dichos datos. (F5, 2023, Cortafuegos de aplicaciones web).

De acuerdo con Narváez y Chaparro (2022), los WAF también tienen la capacidad de prevenir ataques que no pueden ser detenidos por los firewalls de red o los sistemas de

prevención de intrusiones. Un WAF se sitúa delante de la aplicación web, es decir, todo el tráfico debe pasar a través de esta herramienta antes de acceder a la aplicación web en sí. Además, supervisa la actividad en la aplicación y genera alertas, o bien tiene la capacidad de bloquear el tráfico que se identifica como malicioso o que no cumple con reglas específicas que han sido configuradas. El objetivo principal es detectar ataques a nivel de aplicación, como las inyecciones SQL y los ataques de cross-site scripting, así como los intentos de manipulación del comportamiento de la aplicación web.

2.2.13. Firewall como herramienta de seguridad

La seguridad de la red se enfoca en la implementación de medidas de seguridad destinadas a resguardar la confidencialidad, integridad y disponibilidad de una red local en el ámbito de una organización. Estos componentes de seguridad siguen progresando y demandan esfuerzos constantes para mantener alejados a los posibles atacantes de la red. La utilización de un firewall es esencial para salvaguardar la red contra amenazas cibernéticas, aunque es importante destacar que tener un firewall no garantiza automáticamente la seguridad total de un negocio. (Caicedo, 2022).

2.2.14. Políticas de los firewalls

Los firewalls son una parte fundamental de la seguridad de redes y sistemas informáticos. Establecer políticas adecuadas en un firewall es esencial para proteger la red y los activos digitales. A continuación, se presentan algunas de las políticas comunes que se pueden configurar en un firewall, según sitio oficial (Fortinet, 2023).

Política	Descripción
Política de filtrado de direcciones IP	Se pueden establecer reglas para bloquear o permitir tráfico en función de direcciones IP específicas, tanto a nivel de origen como de destino. Esto es útil para restringir o permitir el acceso a ciertas redes o ubicaciones geográficas.
Política de denegación predeterminada	Esta política establece que todo el tráfico debe ser bloqueado a menos que se especifique explícitamente lo

	contrario. Es una medida de seguridad fundamental para prevenir accesos no autorizados.
Política de filtrado de puertos y protocolos	Se configuran reglas para permitir o bloquear el tráfico en función de los puertos y protocolos utilizados. Por ejemplo, se pueden bloquear puertos no utilizados o restringir el acceso a protocolos considerados inseguros.
Política de registro y auditoría	Se puede configurar el firewall para registrar eventos y actividades relevantes, lo que permite el monitoreo y la auditoría de la seguridad de la red. Esto es útil para detectar patrones de ataque, analizar incidentes y mejorar la postura de seguridad. Es importante tener en cuenta que las políticas de firewall deben ser personalizadas y adaptadas a las necesidades específicas de cada organización o entorno de red.

Tabla 3. Políticas de seguridad
Nota: Tomado del sitio oficial de Fortinet (2023).

2.2.15. Políticas de seguridad informática

La protección de datos ocupa un lugar central en las TI modernas. Las políticas de seguridad son un conjunto de normas que el equipo de trabajo debe seguir para colaborar en la protección del entorno cibernético contra acciones delictivas. Capacitar a los colaboradores, crear y memorizar contraseñas complicadas, es una política extremadamente importante, esta actitud se debe explicar a toda la organización para promover las contraseñas fuertes, desde el e-mail personal hasta los accesos a los diferentes sistemas (Napse, 2023).

2.2.16. Seguridad en la nube

Según el nuevo informe Cloud Security Report realizado por Check Point y Cybersecurity Insiders (2023) arroja que el 76% de las compañías está preocupada ante el aumento de los ataques a las redes basadas en el cloud. La evolución de la seguridad en la nube ha sido turbulenta, manifestándose a menudo en ráfagas de cambios revolucionarios, y sigue siendo una gran preocupación para los profesionales de la

ciberseguridad. Según la encuesta, están extremadamente o muy preocupados por la seguridad en la nube. Esto destaca la necesidad urgente de un cambio en la forma en que protegemos la infraestructura de la nube. El panorama de la nube en rápida evolución presenta a las organizaciones desafíos complejos para administrar y asegurar de manera efectiva su infraestructura en la nube, lo que requiere la adopción de soluciones integrales para mitigar los riesgos y salvaguardar los activos críticos.

Los analistas de seguridad se enfrentan a un panorama de amenazas en rápida evolución, los actores de amenazas continúan lanzando campañas de ataque cada vez más sofisticadas que aprovechan nuevos marcos de ataque. Para el analista de la seguridad se vuelve aún más desafiante a medida que sus organizaciones trasladan más aplicaciones a la nube. A medida que la superficie de ataque de las aplicaciones continúa con su rápida evolución y expansión los analistas de seguridad necesitan herramientas mejoradas para mantenerse al día con el creciente volumen de alertas generadas por sus herramientas de seguridad (Cybersecurity Insiders, 2023).

2.2.17 Amenazas en la nube

De acuerdo con informe realizado por realizado por Check Point y Cybersecurity Insiders (2023) manifiesta que cuando se trata de las principales amenazas de seguridad, vemos que la mala configuración de la plataforma en la nube o la configuración incorrecta ocupa el primer lugar con un 59 %, seguida de la exfiltración de datos confidenciales (51 %), interfaces/API inseguras (51 %) y acceso no autorizado (49%). Esto demuestra que una parte importante de las organizaciones aún son vulnerables a las amenazas de seguridad en la nube, en particular, las configuraciones incorrectas y el control de acceso. Los hallazgos también enfatizan la importancia de las configuraciones adecuadas, la protección sólida de la cuenta y la gestión oportuna de vulnerabilidades. Independientemente de si una organización ha sufrido un incidente de seguridad hasta el momento, los siguientes hallazgos se alinean estrechamente con la experiencia general en la industria.

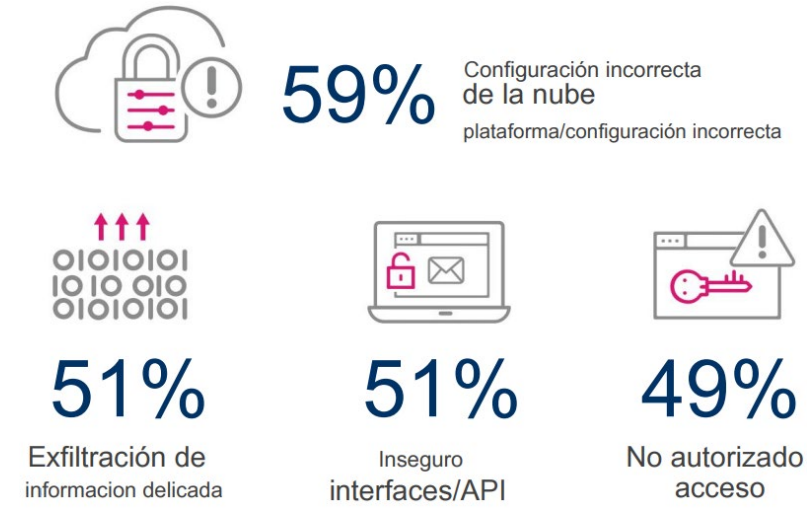


Figura 5. Mayores amenazas de seguridad en las nubes públicas
Fuente: Tomado de informe Cloud Security Report realizado por Check Point y Cybersecurity Insiders (2023).

2.2.18. Fortinet

Es una compañía especializada en soluciones de seguridad cibernética que se enfoca en combinar diversas funciones en una única plataforma. Su principal objetivo es ofrecer una seguridad completa y un rendimiento superior para la infraestructura tecnológica de las redes empresariales. A través de esta plataforma, se brindan servicios como el filtrado web, antivirus, cortafuegos y control de aplicaciones existentes. Fortinet opera con la finalidad de mantener la red segura de manera integrada, automática y escalable, previniendo amenazas y reduciendo el riesgo de intrusiones (Fortinet, 2023).

2.2.19. FortiWeb

Según sitio oficial de Fortinet (2023), se encarga de salvaguardar aplicaciones web y APIs contra las 10 principales amenazas señaladas por OWASP, así como ataques de denegación de servicio distribuido (DDoS) y ataques realizados por bots maliciosos. Este producto dispone de funciones avanzadas basadas en aprendizaje automático (Machine Learning) que mejoran la seguridad y al mismo tiempo reducen la carga de trabajo administrativa. Entre las capacidades destacadas se incluyen la detección de anomalías, la identificación y protección de APIs, la mitigación de bots y un análisis avanzado de amenazas para detectar las amenazas más críticas en todas las aplicaciones que se encuentran bajo su protección.

2.2.20. Open Web Application Security Project (OWASP)

OWASP se define como una comunidad en constante evolución que se dedica a la identificación y mitigación de riesgos de seguridad presentes en aplicaciones web. Según la información proporcionada por el sitio oficial de OWASP (2021), su conjunto de directrices es considerado como un estándar de sensibilización dirigido tanto a desarrolladores como a profesionales de la seguridad de aplicaciones web. Estas directrices representan un amplio consenso acerca de los riesgos de seguridad más críticos asociados a las aplicaciones web. Es importante resaltar que OWASP no mantiene ninguna afiliación con empresas de tecnología, aunque respalda el uso informado de tecnologías de seguridad comerciales. La comunidad genera diversos tipos de materiales de manera colaborativa, transparente y abierta (OWASP, 2021).

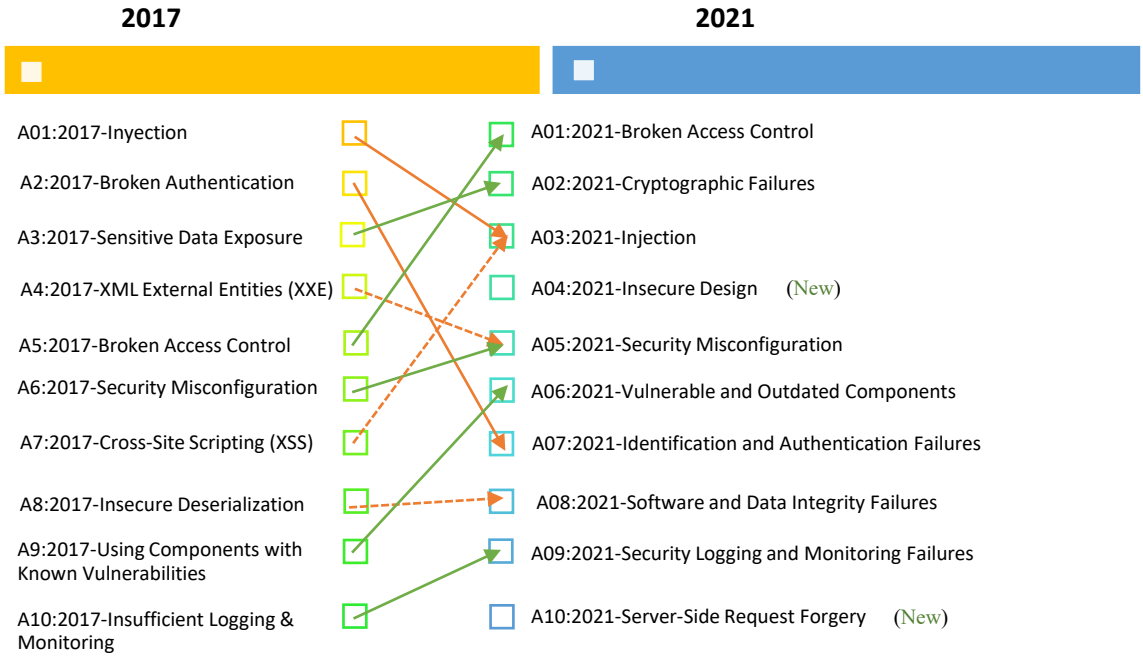


Figura 6. Principales ataques según la metodología Open Web Application Security Project (OWASP)
Fuente: Tomado del sitio oficial del OWASP-top 10-2021 https://owasp.org/Top10/

2.2.21. Top 10 del OWASP

Top 10 OWASP	Descripción
A01:2021-Broken Access Control	Asciende desde el quinto lugar a la categoría con el riesgo de seguridad de aplicaciones web más crítico, siendo este el control que presenta el mayor número de incidentes.
A02:2021- Cryptographic Failures	Asciende a la posición 2, anteriormente conocido como A3:2017: exposición de datos confidenciales.
A03:2021-Injection	Ocupa el tercer lugar en el ranking. Se evaluó el 94 % de las aplicaciones en busca de posibles inyecciones, y los 33 CWE asignados a esta clasificación presentan la segunda mayor cantidad de instancias en las aplicaciones. En esta edición, Cross-site Scripting se ha incorporado a esta categoría.
A04:2021-Insecure Design	Es una categoría recién introducida en 2021, centrada en los peligros vinculados a deficiencias en el diseño. Esto demanda una mayor aplicación de la modelización de amenazas, estándares y conceptos de diseño seguro, así como modelos de referencia arquitectónica.
A05:2021-Security Misconfiguration	Avanza desde el sexto lugar en la edición anterior; el 90 % de las aplicaciones fueron sometidas a pruebas en busca de cualquier tipo de configuración errónea. A pesar de la tendencia hacia un software cada vez más configurable, resulta llamativo que esta categoría esté en ascenso. La categoría previa para vulnerabilidades de entidades externas XML (XXE) se ha fusionado con esta en esta edición.
A06:2021-Vulnerable and Outdated Components	El uso de componentes con vulnerabilidades previamente identificadas se sitúa en la segunda posición en la encuesta de la comunidad Top 10. Además, esta categoría reúne suficiente información para ser incluida en el Top 10 a través del análisis de datos. En comparación con el año 2017, esta categoría ha ascendido desde el noveno puesto y representa un desafío bien conocido en cuanto a pruebas y evaluación de riesgos. Lo que la

	hace única es que no se le han asignado vulnerabilidades y exposiciones comunes (CVE) a los elementos CWE que incluye. Por lo tanto, en sus calificaciones se considera un valor de explotación predefinido y ponderaciones de impacto de 5.0.
A07:2021-Identification and Authentication Failures	Esta categoría solía abordar problemas de autenticación comprometida, pero ha ido descendiendo desde la segunda posición y ahora incorpora CWE más centrados en deficiencias de identificación. Aunque continúa siendo un elemento fundamental en el Top 10, parece que la mayor disponibilidad de marcos estándar está teniendo un impacto positivo en esta área.
A08:2021-Software and Data Integrity Failures	Es una categoría recién introducida en 2021, la cual se concentra en realizar suposiciones sin verificar la integridad en relación con actualizaciones de software, datos críticos y flujos de trabajo de Integración Continua/Entrega Continua (CI/CD). Uno de los impactos ponderados más elevados proviene de los datos asignados a los 10 CWE en esta categoría a través del sistema de Puntuación de Vulnerabilidad Común/Vulnerabilidad Común y Sistema de Puntuación (CVE/CVSS). La deserialización insegura del año 2017 ahora se incluye en esta categoría de alcance más amplio.
A09:2021-Security Logging and Monitoring Failures	Eran más conocidos por la falta de registros y supervisión, y se han trasladado desde el tercer puesto en la encuesta de la industria, mejorando su posición anterior en el décimo lugar. Esta categoría se ha expandido para abarcar diversos tipos de defectos, los cuales son difíciles de verificar y carecen de una representación adecuada en los datos de CVE/CVSS. A pesar de esta limitación, las deficiencias en esta categoría pueden tener un impacto directo en la visibilidad, las alertas de incidentes y la investigación forense.
A10:2021-Server-Side Request Forgery	Los datos indican que esta categoría tiene una tasa de incidencia relativamente baja, a pesar de contar con una cobertura de pruebas por encima del promedio. Además, obtiene calificaciones superiores a la media en cuanto al potencial de explotación e impacto. En esta categoría, la comunidad de

	seguridad enfatiza su importancia, aunque actualmente no se refleje de manera evidente en los datos.

Tabla 4. Top 10 del OWASP
Fuente: Tomado del sitio oficial del OWASP-top 10-2021 https://owasp.org/Top10/

2.2.22. Tipos de ataques

Existen diversos tipos de ataques, según el Herrero (2022), nos presenta las siguientes como ataques principales:

Tipos de ataque	Descripción
Ataques de malware	El malware se refiere a software malicioso diseñado para dañar, comprometer o tomar el control de un sistema. Esto puede incluir virus, gusanos, troyanos, ransomware y spyware, entre otros.
Ataques de denegación de servicio (DDoS)	Estos ataques buscan sobrecargar un sistema o red con una gran cantidad de tráfico, lo que provoca una interrupción o inaccesibilidad del servicio para los usuarios legítimos.
Ataques de phishing	En este tipo de ataque, los atacantes se hacen pasar por entidades legítimas, como instituciones financieras o empresas reconocidas, con el fin de obtener información confidencial de los usuarios, como contraseñas o datos bancarios.
Ataques de fuerza bruta	En este tipo de ataque, los atacantes intentan descifrar contraseñas o claves de cifrado probando sistemáticamente todas las combinaciones posibles hasta encontrar la correcta.
Ataques de interceptación de datos (sniffing):	Los atacantes utilizan herramientas para capturar y analizar el tráfico de red con el fin de obtener información

	confidencial, como contraseñas o datos de tarjetas de crédito.
Ataques de explotación de vulnerabilidades	Los atacantes buscan aprovechar las debilidades o vulnerabilidades presentes en sistemas, aplicaciones o redes para comprometer la seguridad y obtener acceso no autorizado.

Tabla 5. Tipos de ataques en aplicaciones web
Nota: Tomado de Herrero (2022).

2.2.23. Guía de pruebas de seguridad web de OWASP

El Web Security Testing Guide WSTG es una guía completa para probar la seguridad de aplicaciones y servicios web. Creado gracias a los esfuerzos colaborativos de profesionales de la ciberseguridad y voluntarios dedicados, el WSTG proporciona un marco de mejores prácticas utilizadas por evaluadores de penetración y organizaciones de todo el mundo (OWASP, 2021).

2.2.24. Cómo hacer referencia a escenarios WSTG

Según la Guía de pruebas de seguridad web OWASP (2021), cada escenario tiene un identificador en el formato WSTG-<category>-<number>, donde: 'categoría' es una cadena mayúscula de 4 caracteres que identifica el tipo de prueba o debilidad, y 'número' es un valor numérico rellenado con ceros del 01 al 99. Por ejemplo: WSTG-INFO-02es la segunda prueba de recopilación de información (Jahanavi y Mubeen, 2023).

2.2.25. Adaptación y priorización

Las organizaciones deberían adoptar esta guía de pruebas de acuerdo con la necesidad para que coincida con la tecnología, procesos y estructura organizativa. En general, hay varios roles diferentes dentro de las organizaciones que pueden utilizar esta guía, según lo describe WSTG-v4.2, en su sitio oficial de OWASP.

- Los desarrolladores deben utilizar esta guía para asegurarse de producir código seguro. Estas pruebas deben ser parte del código normal y de los procedimientos de prueba unitaria (Guevara-Vega et al., 2022).

- Los evaluadores de software y el control de calidad deben utilizar esta guía para ampliar el conjunto de casos de prueba que aplican a las aplicaciones. Detectar estas vulnerabilidades a tiempo ahorra mucho tiempo y esfuerzo en el futuro.
- Los especialistas en seguridad deben utilizar esta guía en combinación con otras técnicas como una forma de verificar que no se hayan pasado por alto agujeros de seguridad en una aplicación.
- Los gerentes de proyectos deben considerar la razón por la que existe esta guía y que los problemas de seguridad se manifiestan a través de errores en el código y el diseño.

2.3. Marco legal

Ley Orgánica de Educación Superior: Según LOES (2018), las universidades y escuelas politécnicas públicas se definen como comunidades académicas que poseen su propia personalidad jurídica. Además, cuentan con autonomía en aspectos académicos, administrativos, financieros y organizativos, todo ello en concordancia con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución. Estas instituciones se caracterizan por ser esencialmente pluralistas, lo que significa que están abiertas a todas las corrientes y enfoques del pensamiento universal presentados de manera científica.

Ley de Protección de Datos Personales: En Ecuador, la Ley de Protección de Datos Personales está regulada por la Ley Orgánica de Protección de Datos Personales (LOPD) y su Reglamento General. Estas normativas establecen los principios, derechos y obligaciones relacionados con la protección de los datos personales de los ciudadanos ecuatorianos. Esta ley establece las obligaciones de las organizaciones para proteger los datos personales de sus usuarios, incluyendo medidas de seguridad informática adecuadas para prevenir vulnerabilidades y ataques cibernéticos. Con la Ley de Protección de Datos Personales, se busca cuidar a las personas titulares de los datos, para que ellas puedan decidir a quién entregar su información personal porque confían en los proveedores de servicios digitales (Registrospublicos, 2021).

El Plan Estratégico y Prospectivo: La Constitución Política del Ecuador vigente, ratifica a la planificación como medio para lograr los objetivos del Plan Nacional de Desarrollo; propicia la equidad social y territorial; promueve la igualdad en la diversidad; garantiza derechos y concerta principios rectores, en concordancia con los Objetivos

Nacionales y Políticas definidas en el Plan Nacional de Desarrollo (PND), 2017-2021; las entidades del Estado deben desarrollar sus planes institucionales y dirigir sus esfuerzos hacia la obtención eficiente de resultados y la implantación de una nueva cultura organizacional. El Plan Estratégico y Prospectivo UTN-2019-2023-2035 cuenta con cinco capítulos que plantean nuevos desafíos para el futuro, en un entorno global y local en permanente cambio, que requiere ser abordado de manera multi, inter y transdisciplinariamente (PEPDI, 2019).

CAPÍTULO III
MARCO METODOLÓGICO

En la presente investigación se considera los requisitos previos para la adecuada implementación y funcionamiento del WAF como solución de seguridad en las aplicaciones del servidor web de la UTN, así como garantizar un flujo correcto del tráfico.

3.1. Descripción del área de estudio

La Universidad Técnica del Norte, se encuentra ubicada en la cuidad de Ibarra, provincia de Imbabura, cuenta con una población estudiantil alrededor de 16.000 estudiantes. El área de estudio se centra en el área de Desarrollo Tecnológico e informático específicamente en el área de Gestión Web, donde la universidad mantiene un servidor web que alberga alrededor de 50 sitios, siendo el portal web principal es uno de sitios web más visitados de manera simultánea.

El presente estudio se centra en evaluar la efectividad del WAF como solución de seguridad, caracterizando los diferentes tipos de ataques detectados, este proyecto está encaminado a realizar las pruebas de seguridad utilizando la herramienta OWASP ZAP, que permite determinar las vulnerabilidades y analizar las posibles soluciones para mitigar el riesgo.

3.1.1. Organigrama estructural de Dirección de Desarrollo Tecnológico e Informático (DDTI)

Nivel Directivo: El nivel directivo está conformado por el director responsable de dirigir al equipo de trabajo, encargado de la toma de decisiones estratégicas y la supervisión general del DDTI.

Nivel Ejecutivo: El nivel ejecutivo establecido en la estructura organizacional es ejercido por el subdirector, mismo que implementa políticas y lineamientos establecidos por la Dirección, se encarga de coordinar y supervisar el trabajo del equipo.

Nivel Operativo: El nivel operativo establecido en la estructura organizacional, se encuentra los funcionarios de desarrollo de software, conforme a los lineamientos establecidos desde la dirección.

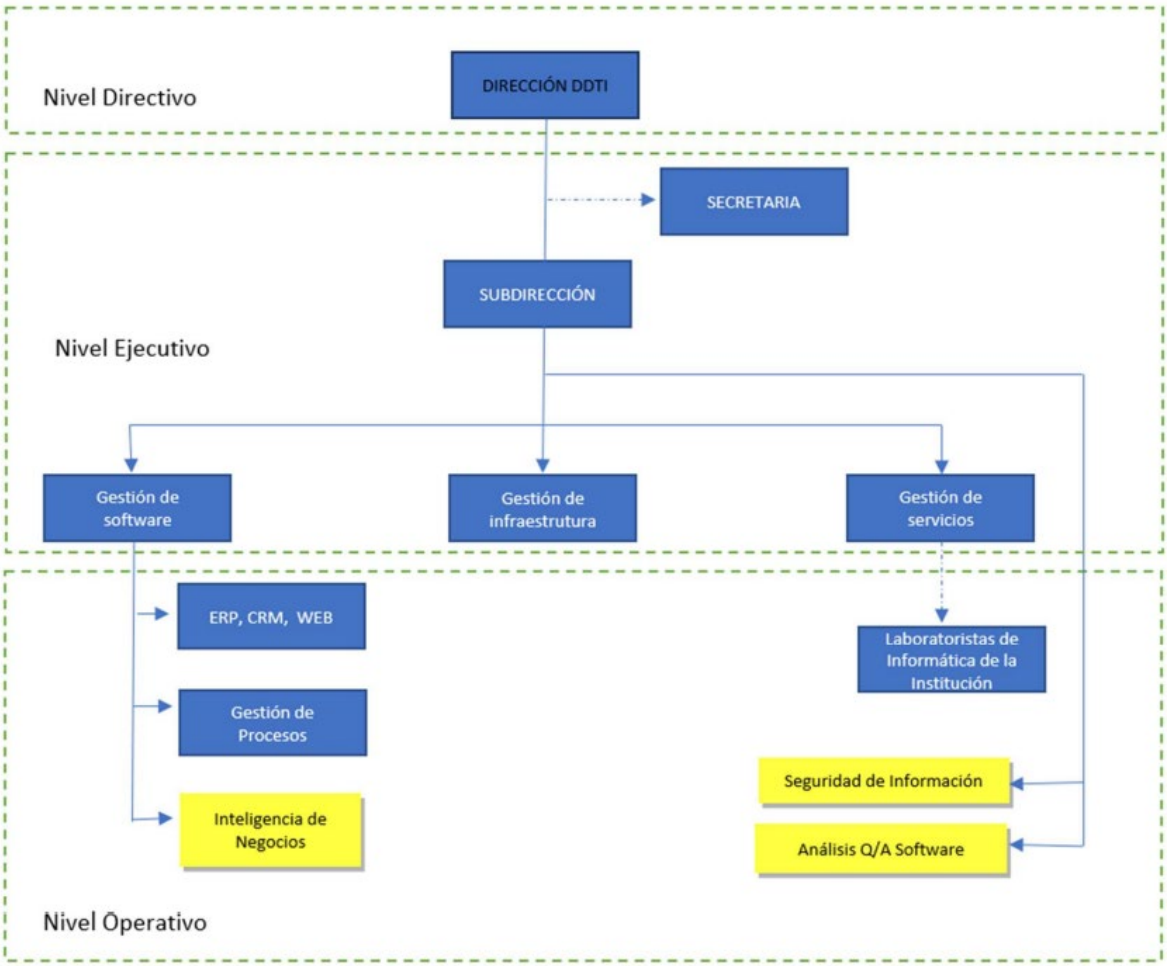


Figura 7. Diagrama de la estructura DDTI
Fuente: Planificación estratégica DDTI (2023).

3.1.2. Población

Está conformada por el personal que trabaja en la Dirección de Desarrollo Tecnológico e Informático (DDTI), como se muestra la Figura 6.

3.1.3. Muestra

Está representada por 25 funcionarios del área de tecnología, entre ellos el área de Desarrollo de Software, área de Redes y Telecomunicaciones, área de Gestión web y Laboratoristas de cada Facultad, que trabajan en **Nivel Operativo** de la Dirección de Desarrollo Tecnológico e Informático (DDTI), como se muestra la Figura 6.

Nivel operativo	**Mujer**	**Hombre**	**Total**
Desarrollo de Software	4	6	10
Área de Gestión web	1	0	1
Redes y telecomunicaciones	1	2	3
Laboratoristas	8	3	11
TOTAL	14	11	25

Tabla 6. Muestra del personal de la Dirección de Desarrollo Tecnológico e Informático (Nivel operativo)
Fuente: Autoría Propia (2023).

3.2. Enfoque y tipo de investigación

El estudio se realizó bajo un enfoque **cuantitativo** ya que está fundamentado en la recolección y análisis de datos estadísticos con el fin de establecer pautas de comportamiento y cuantificar los diferentes tipos de ataque.

Se considera una investigación **descriptiva** puesto que se recopila y analiza información con el fin de proporcionar una representación precisa y detallada de los hechos para caracterizar los diferentes tipos de ataques, para ello se recopilan datos en el lugar de estudio, lo que puede implicar tomar mediciones, muestras, realizar pruebas de testing, realizar encuestas para recolección de datos.

3.2.1. Técnica de investigación

La técnica utilizada fue la encuesta, la cual permitió recoger la mayor información sobre la tecnología que utiliza las aplicaciones web y la apertura para la implementación de medidas de seguridad mediante la metodología OWASP en el servidor web de la Universidad Técnica del Norte, esta técnica se caracteriza por tener un estándar de procedimientos para recoger y analizar datos de la muestra del personal Nivel Operativo del DDTI.

3.2.2. Instrumentos de investigación

La herramienta empleada fue el cuestionario, se procedió a validar por 2 expertos, el Msc. Ramiro Pulgar especialista en Ciberseguridad, y el PhD. Marco Pusdá quien tiene experticia en seguridad de sistemas, este cuestionario consta de 13 preguntas cerradas con múltiples opciones de respuesta que están vinculadas al tema de investigación.

3.3. Procedimiento de investigación

Ficha técnica de las aplicaciones Web: Consideramos las aplicaciones que se van a proteger en el WAF, para ello se analiza número de visitas de cada sitio web.

Verificar IP pública donde se encuentra alojado el servicio: es la dirección donde está publicado el servicio o aplicativos disponibles al público en internet.

A actividades con DNS: Socializar con el personal redes y telecomunicaciones los cambios en los registros DNS públicos de las aplicaciones a proteger cada una de las actividades definidas para la implementación.

Establecer reglas de seguridad: Determinar con los encargados de administrar el acceso a los servicios que se van a proteger las reglas y permisos para la configuración relacionada con el WAF.

Realizar pruebas de penetración: Establecer pruebas de penetración según la guía de pruebas OWASP.

Evaluar la efectividad del WAF: Una vez realizado pruebas de seguridad, se procede a verificar en tiempo real los ataques que fueron bloqueados por las reglas del Firewall.

Establecer reportes: Luego de un análisis de los ataques más frecuentes se genera reportes o una analítica de los ataques que serán de manera detallada para los administradores tanto de redes como el área web.

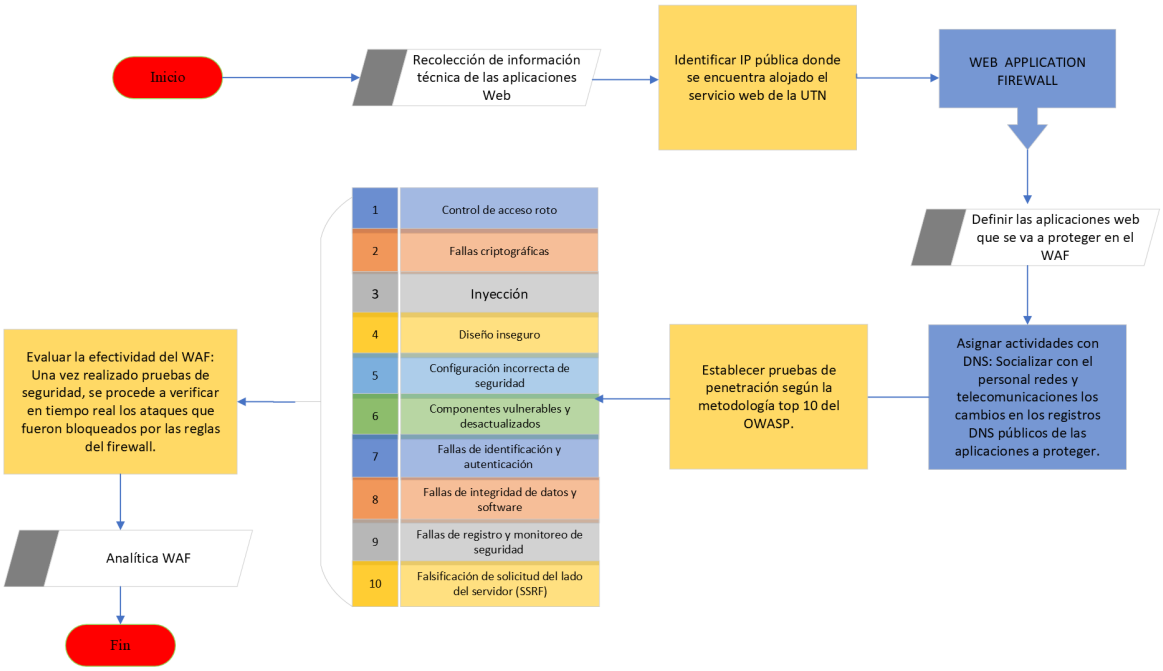


Figura 8. Procedimiento de investigación
Fuente: Autoría propia (2023)

3.4. Consideraciones bioéticas

Privacidad y protección de datos: para evaluar la efectividad del WAF como solución de seguridad en las aplicaciones del servidor web de la UTN, se recopila la información, se realiza un análisis de datos sensibles, como los registros de tráfico web y los patrones de comportamiento de los usuarios, es fundamental garantizar la privacidad de los datos y cumplir con las regulaciones y normativas de protección de datos correspondientes.

Consentimiento informado: la presente investigación involucra la participación de personal administrativo como el director de TI, Analista de Redes, Analista de sistemas, Webmáster y se procede a informar a los participantes que se proporcionará información clara y comprensible sobre la investigación, sus beneficios potenciales y sobre todo permitir que los participantes tomen una decisión informada sobre su participación.

Transparencia y divulgación: Es importante ser transparente sobre los métodos utilizados en la investigación de la evaluación de la efectividad del WAF y divulgar los resultados de manera clara y comprensible. Esto promueve la rendición de cuentas y permite la revisión y la replicación de los hallazgos por parte de la comunidad científica.

3.5. Recursos

La implementación de un Web Application Firewall (WAF) puede requerir diferentes recursos de tiempo y financieros, dependiendo de la organización y la infraestructura existente. Se debe realizar un análisis exhaustivo de los requisitos de seguridad y las necesidades de la organización antes de la implementación. Esto implica definir objetivos, evaluar riesgos y planificar la estrategia de implementación. El tiempo requerido para esta etapa puede variar dependiendo de la complejidad del entorno.

La implementación de un WAF implica la adquisición de licencias y suscripciones del proveedor del WAF. El costo varía según el proveedor seleccionado, la cantidad de licencias necesarias y la duración de las suscripciones.

3.6. Cronograma de actividades

La gestión de proyectos implica el proceso de iniciar, preparar, ejecutar y concluir las actividades necesarias para alcanzar los objetivos del proyecto. Se utilizan herramientas que permiten mantener una visión y control a largo plazo de todas las etapas del ciclo de vida del proyecto, gestionar cambios, abordar riesgos, fomentar la comunicación entre las partes involucradas, administrar tareas y hitos, controlar los gastos relacionados con las tareas individuales y llevar a cabo la gestión financiera, así como realizar un seguimiento del tiempo. Las actividades planificadas para esta investigación se detallan en el siguiente diagrama.

Actividades	May	Jun	Jul	Ago	Sep	Oct
Recolección de información técnica del servidor web y las aplicaciones.						
Aplicar la encuesta al personal de Nivel Operativo del DDTI.						
Analizar cuales sitios web se van a proteger. Realizar Backups						
Aplicar pruebas de seguridad mediante la guía de pruebas de aplicaciones web del OWASP WSTG						
Conocer los ataques más frecuentes al servidor web de la UTN.						
Reporte del WAF						

Tabla 7. Cronograma de actividades realizados para proyecto de investigación
Fuente: Autoría propia (2023)

CAPITULO IV
RESULTADOS Y DISCUSIÓN

Se aplicó la encuesta como instrumento de investigación, para este proceso se recopiló datos y opiniones del personal de Nivel Operativo de la Dirección de Desarrollo Tecnológico e Informático de la UTN para el proyecto de investigación: "WEB APPLICATION FIREWALL (WAF) COMO SOLUCIÓN DE SEGURIDAD MEDIANTE LA METODOLOGÍA OWASP PARA LA PROTECCIÓN DE APLICACIONES EN EL SERVIDOR WEB DE LA UNIVERSIDAD TÉCNICA DEL NORTE."

4.1. Análisis de resultados de la encuesta

Género	Frecuencia	%
Masculino	11	44
Femenino	14	56
Otro	0	0
Total	25	100

Tabla 8. Género DDTI
Fuente: Encuesta autoría propia (2023)

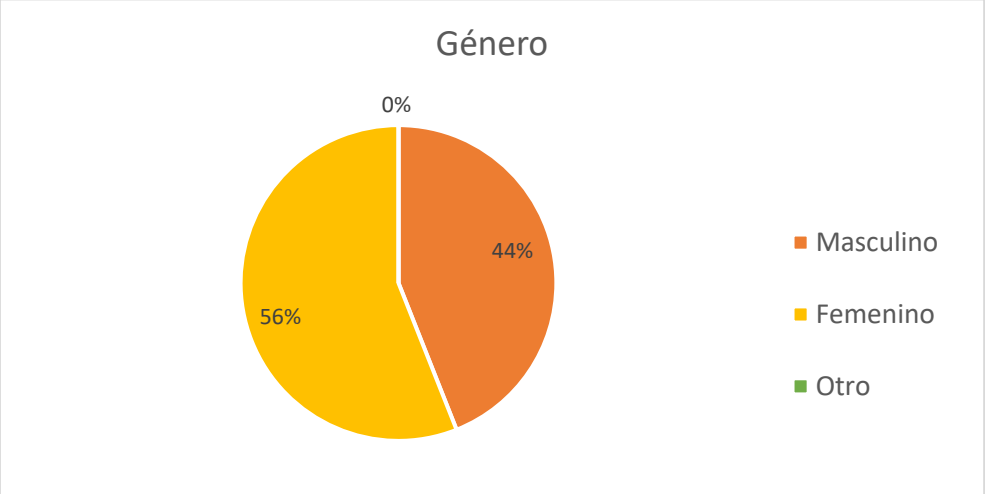


Figura 9. Género DDTI
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 8, se puede observar que el 56% de los funcionarios que pertenecen a Nivel Operativo son de género femenino, mientras que el 44% son masculino, con un total de 25 funcionarios.

Nivel Operativo	Frecuencia	%
Desarrollo de Software	10	40
Área de Gestión web	1	4
Redes y Telecomunicaciones	3	12
Laboratoristas	11	44
Total	25	100

Tabla 9. Nivel Operativo DDTI
Fuente: Encuesta autoría propia (2023)

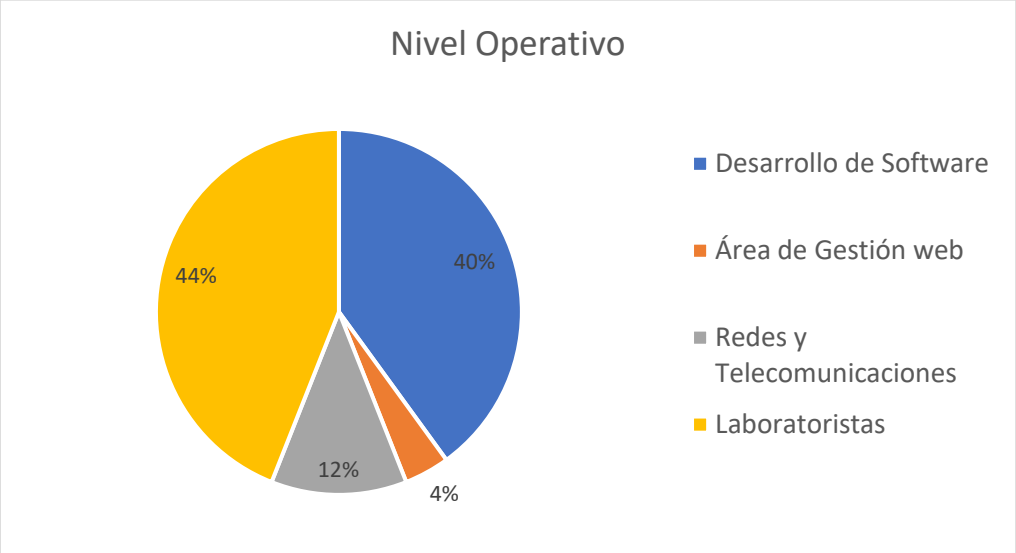


Figura 10. Nivel Operativo DDTI
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 9, se evidencia que el 44% de funcionarios que pertenecen a Nivel Operativo del DDTI son Laboratoristas, esto significa que la universidad mantiene un gran número de personal en los laboratorios de computación que se encuentran distribuidos en cada Facultad tanto de grado como posgrado, el 40 % son funcionarios

dedicados a Desarrollo de Software, el 12% representa a funcionarios del área de Redes y Telecomunicaciones y un 4 % representa al área de gestión web.

RESULTADOS DEL CUESTIONARIO

1. **¿La alta dirección entiende participa y toma decisiones relacionadas con la seguridad de la información?**

Escala	Frecuencia	%
Muy frecuente	6	24
Frecuente	12	48
Poco frecuente	7	28
Nunca	0	0
Total	25	100

Tabla 10. La alta dirección entiende participa y toma decisiones relacionadas con la seguridad de la información
Fuente: Encuesta autoría propia (2023)

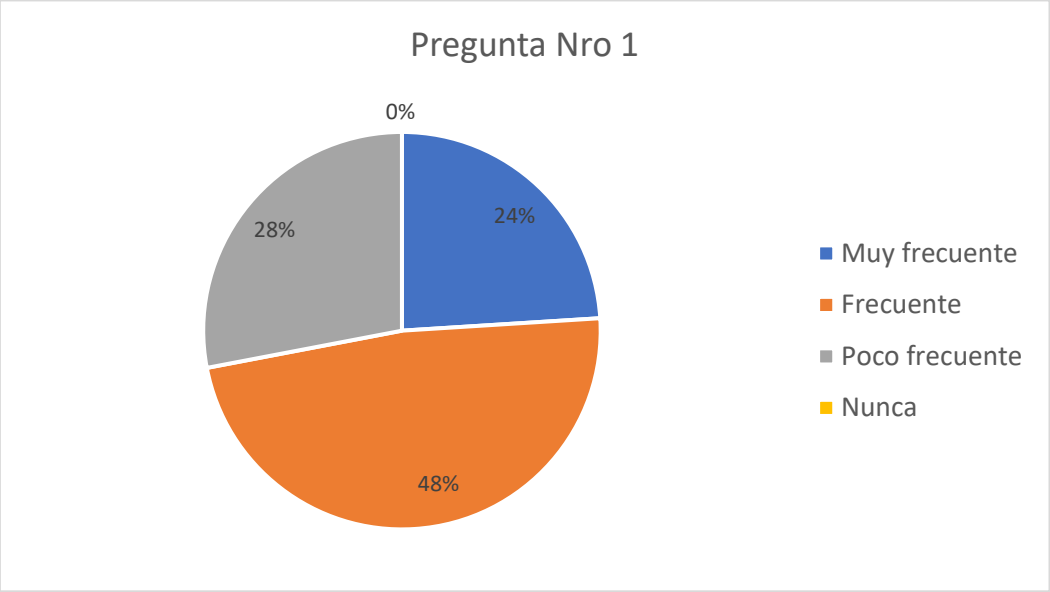


Figura 11. La alta dirección entiende participa y toma decisiones relacionadas con la seguridad de la información
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 10, se puede verificar que el 48% de los profesionales consideraron que es frecuente que la alta dirección participa y toma decisiones relacionadas con la seguridad de la información y un 24 % manifestaron que es muy frecuente, esto nos indica que, si coexiste una participación activa en la gestión de la seguridad de la información en la UTN, por parte de los directores del DDTI están comprometidos e involucrados en la protección de la información sensible y crítica de la organización.

2. **¿Se han asignado recursos, tanto financieros como humanos, para implementar y mantener medidas de seguridad informática efectivas?**

Escala	Frecuencia	%
Siempre	1	4
Casi siempre	9	36
A veces	8	32
Casi nunca	7	28
Nunca	0	0
Total	25	100

Tabla 11. Se han asignado recursos, tanto financieros como humanos, para implementar y mantener medidas de seguridad informática efectivas
Fuente: Encuesta autoría propia (2023)

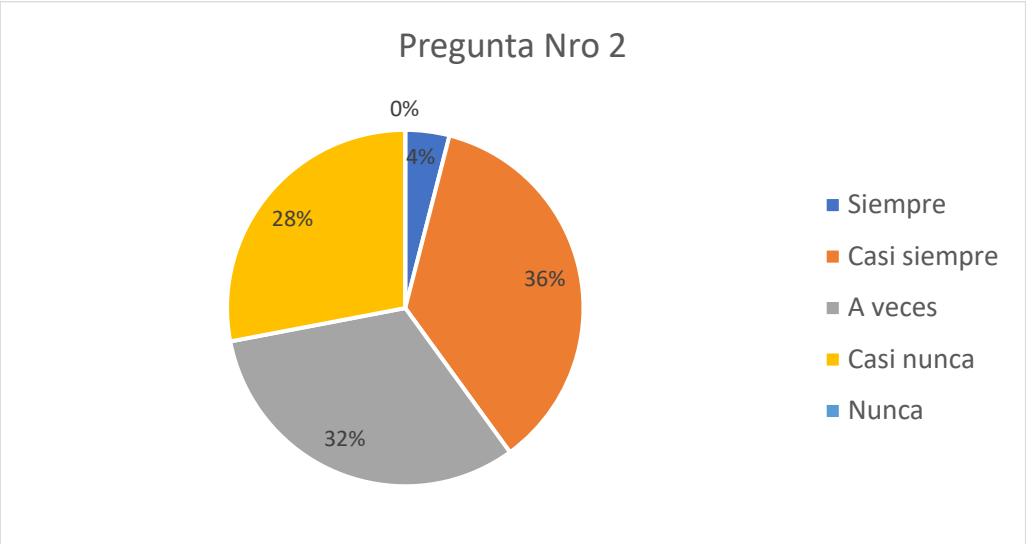


Figura 12. Se han asignado recursos, tanto financieros como humanos, para implementar y mantener medidas de seguridad informática efectivas
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 11, se evidencia que un 36% de los profesionales consideran que casi siempre se han asignado recursos tanto financieros como humanos para implementar y mantener medidas de seguridad informática efectivas, un 32% respondieron que a veces y un 28 % casi nunca, aquí hay algunas consideraciones relacionadas con la asignación de recursos tanto como para el financiamiento adecuado y personal calificado. Este es un indicador donde nos muestra que existe un índice medio bajo, verificando que la UTN necesita fortalecer en la gestión de recursos financieros y humanos para el área de seguridad informática en el DDTI.

3. ¿Está familiarizado con Open Web Application Security Project (OWASP) top 10?

Escala	Frecuencia	%
Si	9	36
No	16	64
Total	25	100

Tabla 12. Está familiarizado con Open Web Application Security Project (OWASP) top 10
Fuente: Encuesta autoría propia (2023)

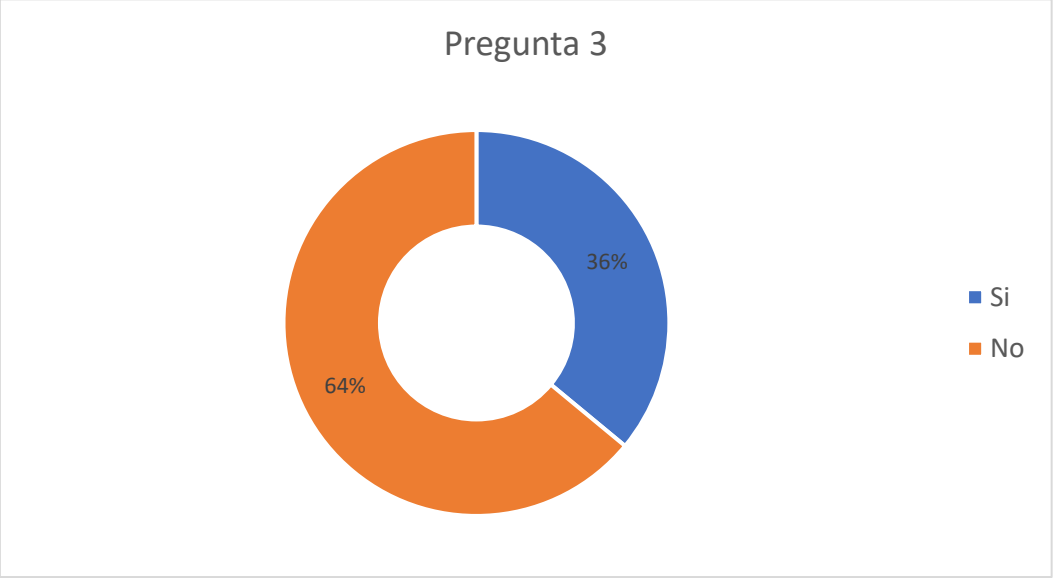


Figura 13. Está familiarizado con Open Web Application Security Project (OWASP) top 10
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 12, podemos evidenciar que el 64 % de los profesionales a nivel operativo del DDTI no están familiarizados con Open Web Application Security Project (OWASP) top 10, indica que un gran porcentaje de los funcionarios a nivel operativo no conocen la metodología OWASP top 10, esto puede surgir varios problemas en relación con la seguridad de las aplicaciones desarrolladas ya que su conocimiento es fundamental para desarrollar software seguro.

4. ¿Qué nivel de conocimiento tiene sobre las vulnerabilidades más comunes de Open Web Application Security Project (OWASP) top 10?

Escala	Frecuencia	%
Excelente	0	0
Muy bueno	2	8
Bueno	7	28
Regular	11	44
Deficiente	5	20
Total	25	100

Tabla 13. Qué nivel de conocimiento tiene sobre las vulnerabilidades más comunes de Open Web Application Security Project (OWASP) top 10
Fuente: Encuesta autoría propia (2023)

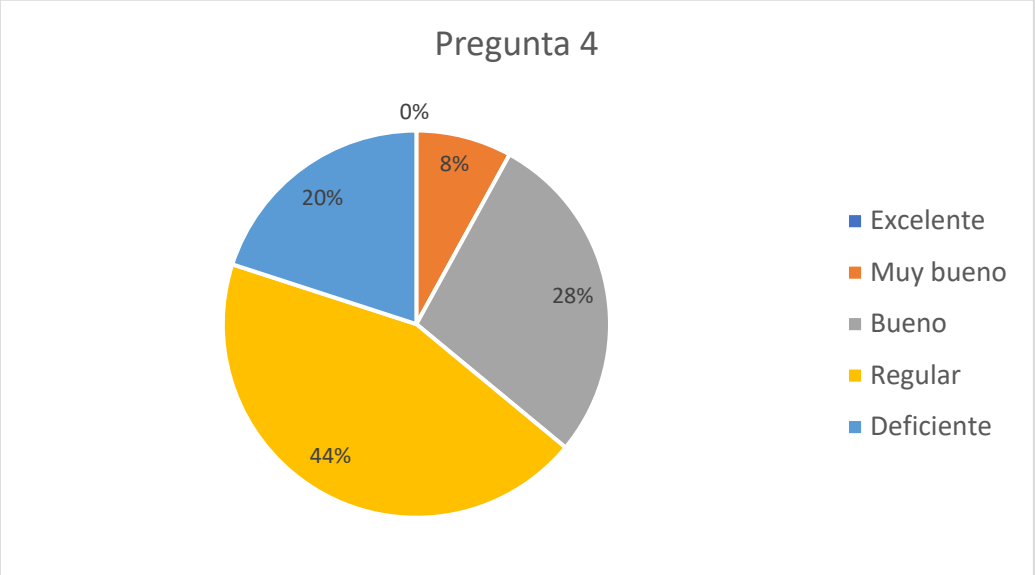


Figura 14. Qué nivel de conocimiento tiene sobre las vulnerabilidades más comunes de Open Web Application Security Project (OWASP) top 10
Fuente: Encueta autoría propia (2023)

Análisis

En la Figura 13, se puede observar que el 44 % de funcionarios de Nivel Operativo del DDTI, tienen un nivel de conocimiento regular sobre las vulnerabilidades más comunes de Open Web Application Security Project (OWASP) top 10, y un 20 % de profesionales un nivel de conocimiento deficiente en esta metodología para desarrollo de software seguro, por lo que es importante que la UTN invierta en capacitación y concienciación en su equipo de desarrollo.

5. ¿Con que frecuencia ha utilizado un Sistema de Gestión de Contenido (CMS) de código abierto (por ejemplo, WordPress, Joomla, Drupal) ?

Escala	Frecuencia	%
Muy frecuente	13	52
Frecuente	7	28
Poco frecuente	4	16
Nunca	1	4
Total	25	100

Tabla 14. Con que frecuencia ha utilizado un Sistema de Gestión de Contenido (CMS) de código abierto (por ejemplo, WordPress, Joomla, Drupal)
Fuente: Encuesta autoría propia (2023)

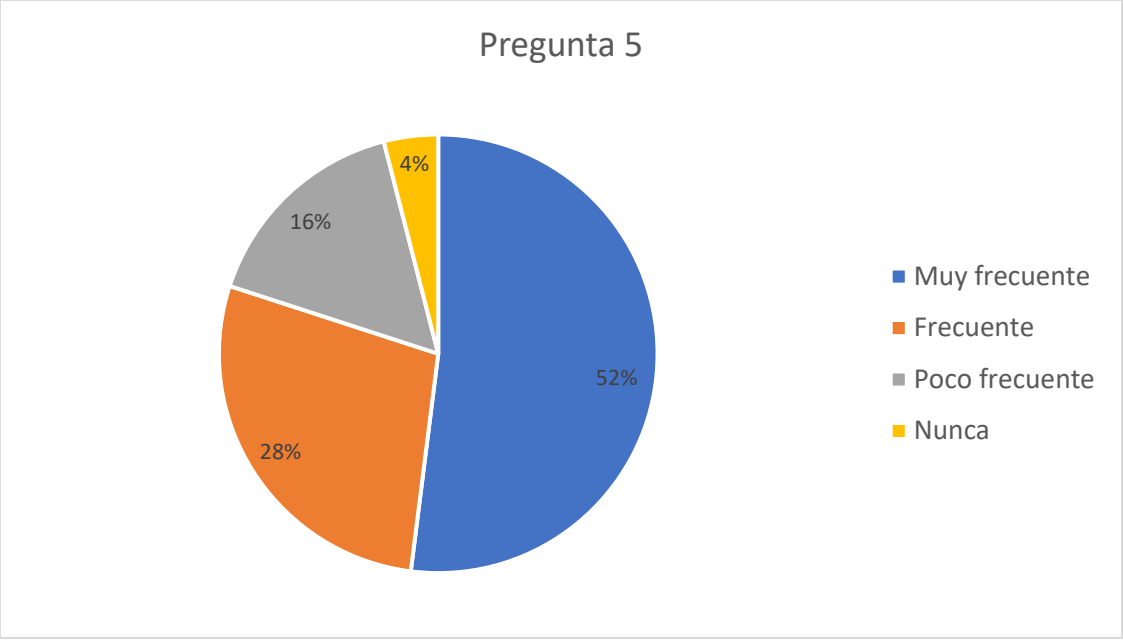


Figura 15. Con que frecuencia ha utilizado un Sistema de Gestión de Contenido (CMS) de código abierto (por ejemplo, WordPress, Joomla, Drupal)
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 14, evidencia que el 52% de profesionales de Nivel Operativo ha utilizado un Sistema de Gestión de Contenido (CMS) de código abierto de manera muy frecuente y 28 % de los profesionales respondieron frecuente, este es un indicador que refleja en su gran mayoría han utilizado un CMS y tienen un nivel de conocimiento de tecnología.

6. **¿Cree usted que los Content Management System (CMS) presentan vulnerabilidades o fallos de seguridad?**

Escala	Frecuencia	%
Si	21	84
No	4	16
Total	25	100

Tabla 15. Cree usted que los Content Management System (CMS) presentan vulnerabilidades o fallos de seguridad
Fuente: Encuesta autoría propia (2023)

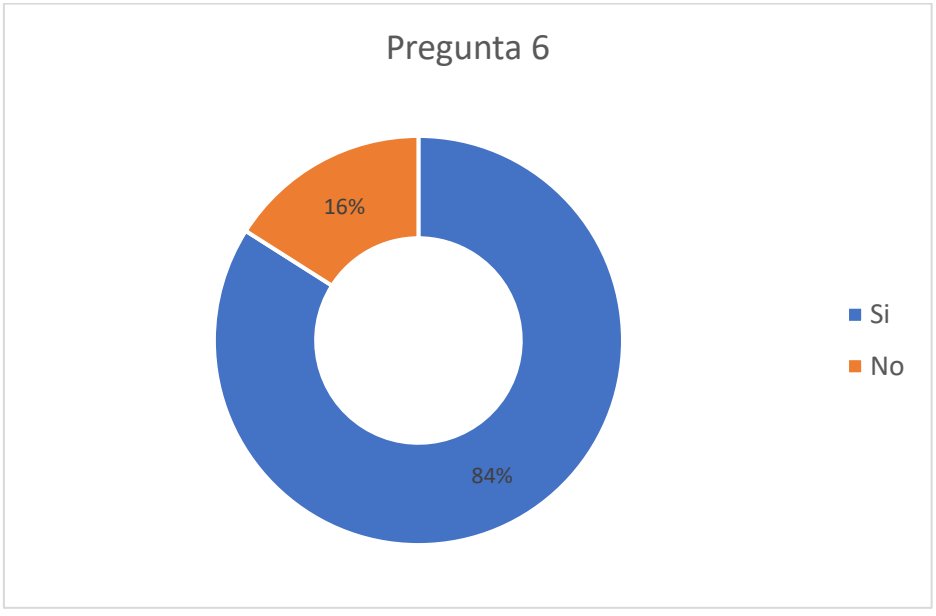


Figura 16. Cree usted que los Content Management System (CMS) presentan vulnerabilidades o fallos de seguridad
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 15, se verifica que un 84 % de profesionales del Nivel Operativo respondieron que si creen que los Content Management System (CMS) presentan vulnerabilidades o fallos de seguridad y un 16 % de los funcionarios consideran que los CMS no presentan vulnerabilidades o fallos de seguridad, este indicador nos facilita comprender que los funcionarios en su gran mayoría conocen los posibles ataques debido a su amplia adopción de gestionar contenido en línea.

7. **¿Está de acuerdo que la metodología OWASP es importante para la seguridad de las aplicaciones web?**

Escala	Frecuencia	%
Totalmente de acuerdo	12	48
De acuerdo	11	44
Ni de acuerdo ni en desacuerdo	2	8
En desacuerdo	0	0
Total	25	100

Tabla 16. Está de acuerdo que la metodología OWASP es importante para la seguridad de las aplicaciones web
Fuente: Encuesta autoría propia (2023)

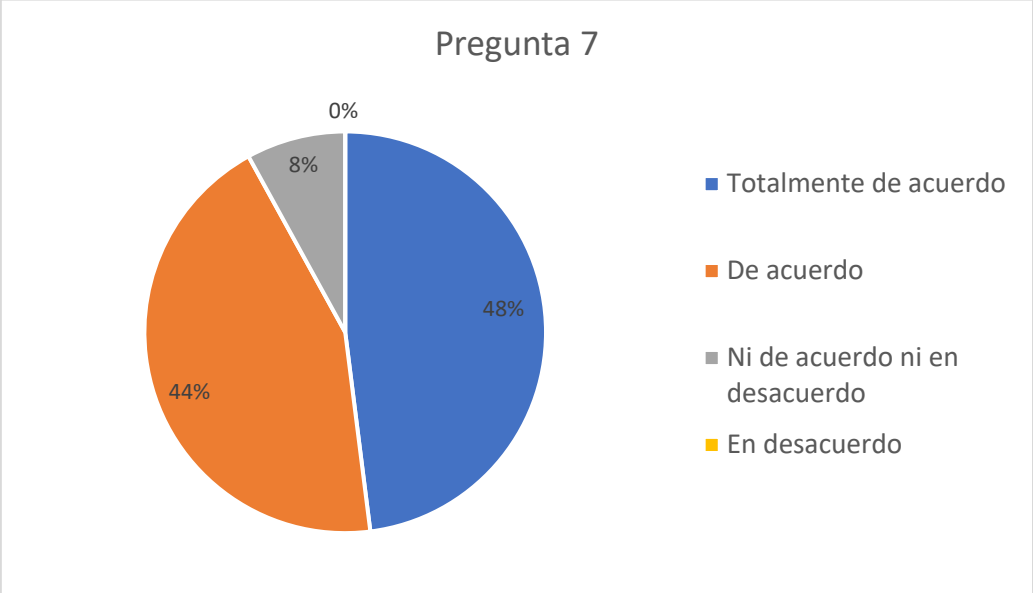


Figura 17. Está de acuerdo que la metodología OWASP es importante para la seguridad de las aplicaciones web
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 16, se obtiene que el 48 % de los profesionales están totalmente de acuerdo en que la metodología OWASP es importante para la seguridad de las aplicaciones web, y un 44 % de los funcionarios de Nivel Operativo están de acuerdo en la importancia para la seguridad de las aplicaciones web.

8. ¿Con qué frecuencia ha utilizado herramientas de pentesting para evaluar la seguridad de sistemas, redes y aplicaciones web?

Escala	Frecuencia	%
Muy frecuente	2	8
Frecuente	3	12
Poco frecuente	11	44
Nunca	9	36
Total	25	100

Tabla 17.Con qué frecuencia ha utilizado herramientas de pentesting para evaluar la seguridad de sistemas, redes y aplicaciones web
Fuente: Encuesta autoría (2023)

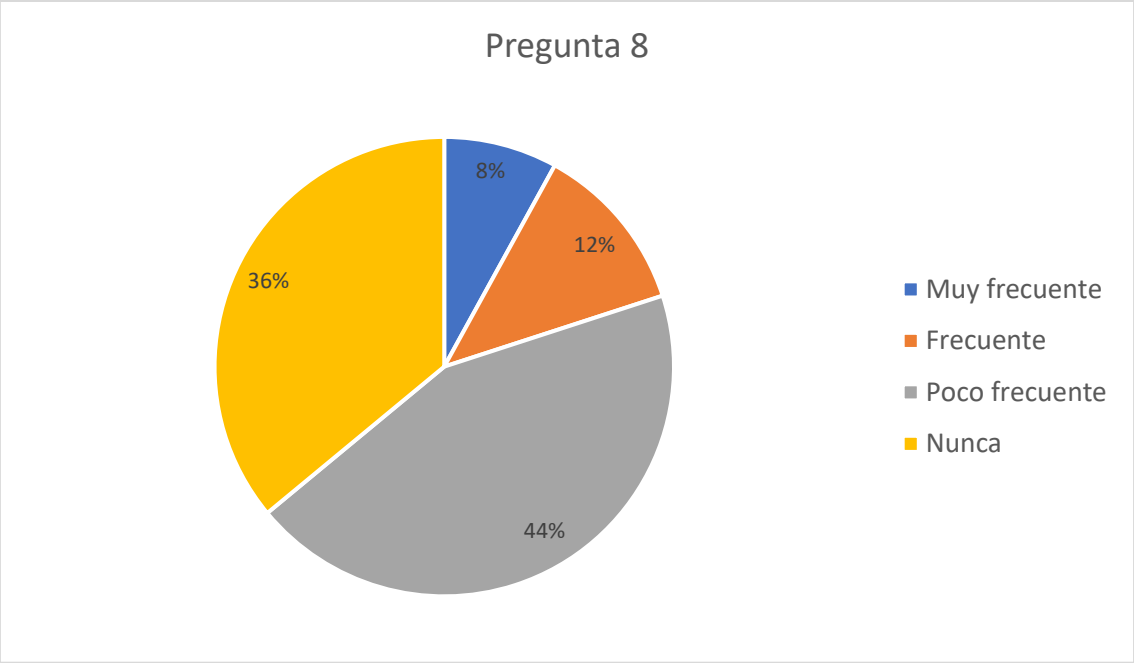


Figura 18. Con que frecuencia ha utilizado herramientas de pentesting para evaluar la seguridad de sistemas, redes y aplicaciones web
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 17, podemos evidenciar que el 44 % de funcionarios del Nivel Operativo han utilizado de manera poco frecuente herramientas de pentesting para evaluar la seguridad de sistemas, redes y aplicaciones web, y un 36% respondieron que nunca han utilizado este tipo de herramientas, este indicador representa un nivel bajo de evaluación de seguridad ya que deben ser realizadas por profesionales de seguridad certificados y autorizados, para evaluar la seguridad de sistemas, redes y aplicaciones web. Estas pruebas deben llevarse a cabo de manera controlada y con el permiso adecuado para evitar cualquier interrupción del servicio.

9. ¿Qué nivel de experiencia tiene con aplicaciones en la nube?

Escala	Frecuencia	%
Excelente	6	24
Muy bueno	5	20
Bueno	10	40
Regular	4	16
Deficiente	0	0
Total	25	100

Tabla 18. Nivel de experiencia con aplicaciones en la nube
Fuente: Encuesta autoría propia (2023)

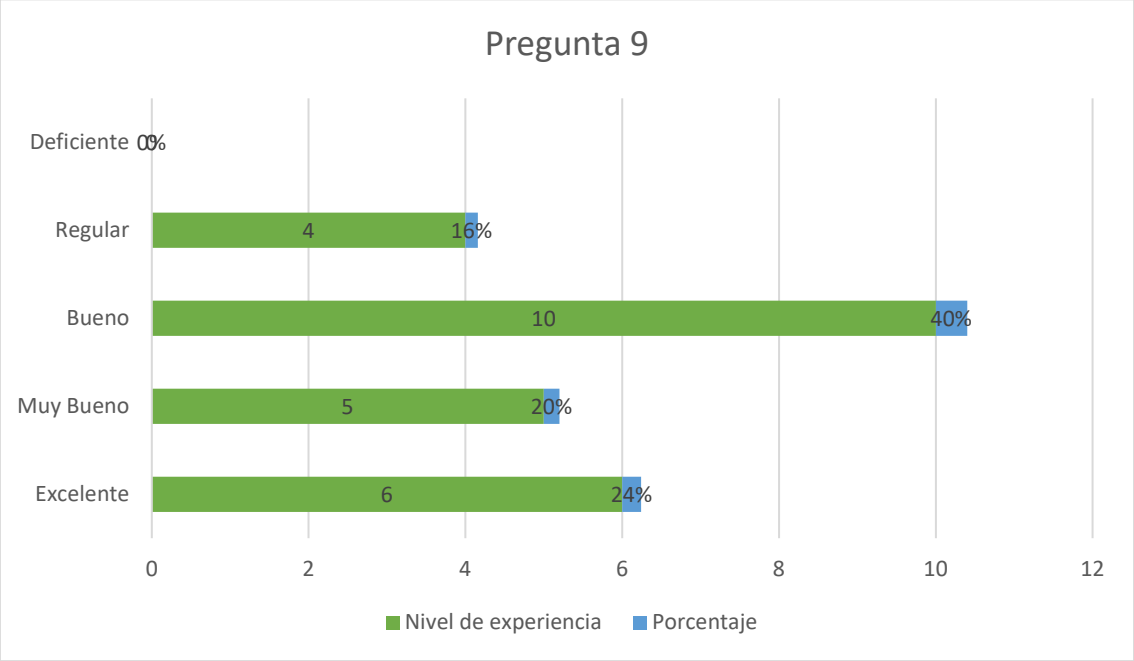


Figura 19. Nivel de experiencia con aplicaciones en la nube
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 18, se evidencia que un 40 % de profesionales del Nivel Operativo tiene un nivel de experiencia bueno con aplicaciones en la nube y 24% respondieron que tienen un nivel Excelente, este indicador nos refiere que los funcionarios del DDTI tienen la experiencia y conocimiento para la administración de aplicaciones en la nube, es importante enfocar la experiencia desde la administración de la infraestructura en la nube hasta el desarrollo de aplicaciones en la nube.

10. ¿Cuáles amenazas de seguridad en la nube usted conoce?

Escala	Frecuencia	%
Configuración incorrecta en la nube	17	68
Malware en la nube	12	48
Acceso no autorizado	15	60
Ataques de denegación de Servicio (DoS)	11	44
API inseguras	8	32
Otra	0	0

Tabla 19. Amenazas de seguridad en la nube
Fuente: Encuesta autoría propia (2023)

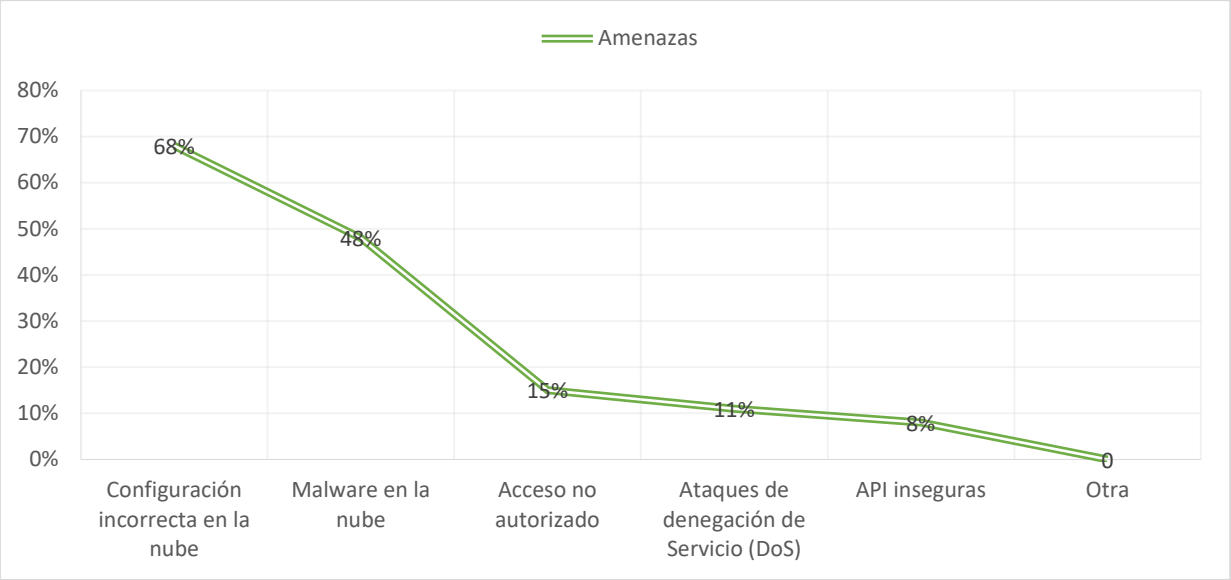


Figura 20. Amenazas de seguridad en la nube.
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 19, podemos observar que el 68 % de profesionales de Nivel Operativo manifestaron que la amenaza de seguridad en la nube más conocida es la Configuración incorrecta en la nube, y un 48 % respondieron que el Malware en la nube, y el 15 % respondieron el acceso no autorizado. Este es un indicador valioso ya que el funcionario conoce las amenazas de seguridad más comunes en la nube y los riesgos que

puede ocasionar ante una configuración errónea, donde los atacantes pueden aprovechar para infiltrarse en sistemas y redes, comprometiendo la integridad, la confidencialidad o la disponibilidad de los datos en la organización.

11. ¿Está de acuerdo en la implementación de una capa adicional de seguridad para proteger las aplicaciones web contra posibles amenazas y vulnerabilidades en el servidor web de la UTN?

Escala	Frecuencia	%
Totalmente de acuerdo	19	76
De acuerdo	5	20
Ni de acuerdo ni en desacuerdo	1	4
En desacuerdo	0	0
Total	25	100

Tabla 20. Está de acuerdo en la implementación de una capa adicional de seguridad para proteger las aplicaciones web contra posibles amenazas y vulnerabilidades en el servidor web de la UTN
Fuente: Encuesta autoría propia (2023)

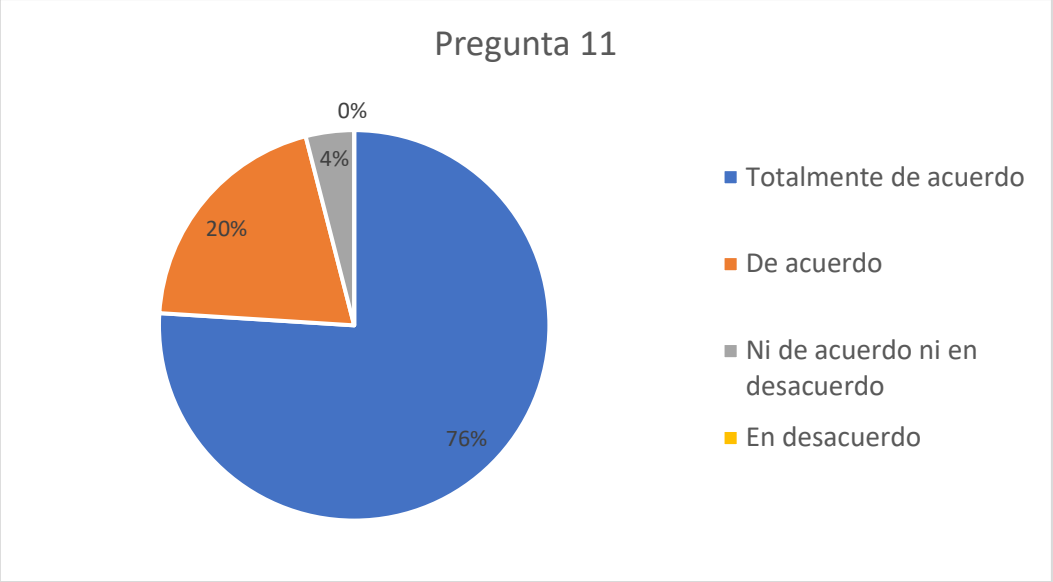


Figura 21. Está de acuerdo en la implementación de una capa adicional de seguridad para proteger las aplicaciones web contra posibles amenazas y vulnerabilidades en el servidor web de la UTN
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 20, podemos evidenciar que el 76% de profesionales del Nivel Operativo respondieron que están totalmente de acuerdo en la implementación de una capa adicional de seguridad para proteger las aplicaciones web contra posibles amenazas y vulnerabilidades en el servidor web de la UTN, el 20 % respondieron que están de acuerdo, este indicar nos facilita entender que en su gran mayoría de funcionarios están de acuerdo en proteger las aplicaciones web contra posibles amenazas y vulnerabilidades en el servidor web ya que es una buena práctica en la seguridad informática.

12. ¿Recomendaría el uso de una aplicación de código abierto para realizar pruebas de pentesting en el servidor web de la UTN?

Escala	Frecuencia	%
Muy frecuente	8	36
Frecuente	11	50
Poco frecuente	2	9
Nunca	1	5
Total	25	100

Tabla 21. Recomendaría el uso de una aplicación de código abierto para realizar pruebas de pentesting en el servidor web de la UTN
Fuente: Encuesta autoría propia (2023)

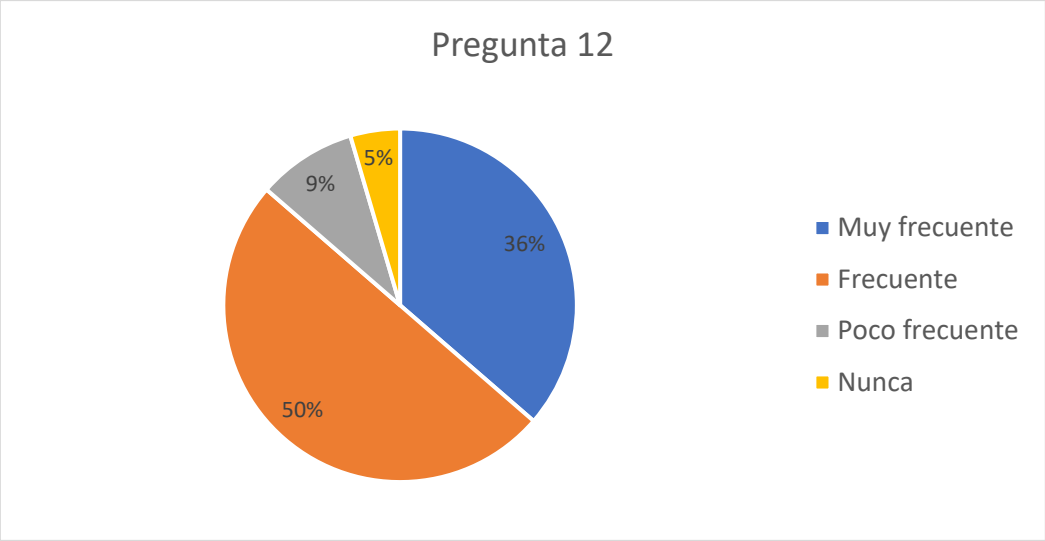


Figura 22. Recomendaría el uso de una aplicación de código abierto para realizar pruebas de pentesting en el servidor web de la UTN
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 21, podemos visualizar que el 50% de funcionarios de Nivel Operativo respondió que si recomiendan el uso frecuente de una aplicación de código abierto para realizar pruebas de pentesting en el servidor web de la UTN, un 36 % de profesionales respondieron que si recomendarían de manera muy frecuente, este indicador nos permite validar la importancia de realizar pruebas de penetración, estas pruebas ayudan a identificar vulnerabilidades y debilidades en el servidor web antes de que los atacantes las aprovechen.

13. ¿Está de acuerdo que se utilice la metodología OWASP para identificar y corregir vulnerabilidades en el servidor web de la UTN?

Escala	Frecuencia	%
Totalmente de acuerdo	12	48
De acuerdo	13	52
Ni de acuerdo ni en desacuerdo	0	0
En desacuerdo	0	0
Total	25	100

Tabla 22. Está de acuerdo que se utilice la metodología OWASP para identificar y corregir vulnerabilidades en el servidor web de la UTN
Fuente: Encuesta autoría propia 2023

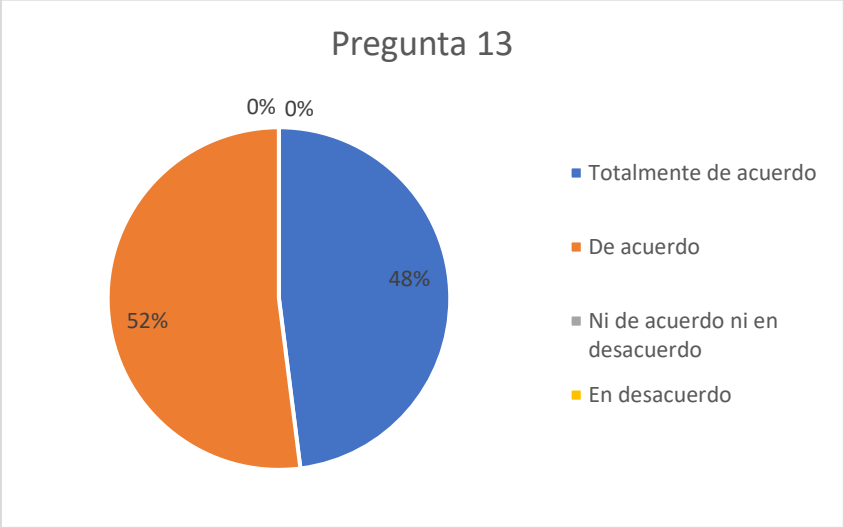


Figura 23. Está de acuerdo que se utilice la metodología OWASP para identificar y corregir vulnerabilidades en el servidor web de la UTN
Fuente: Encuesta autoría propia (2023)

Análisis

En la Figura 22, se puede evidenciar que el 52% de profesionales de Nivel Operativo están de acuerdo en que se utilice la metodología OWASP para identificar y corregir vulnerabilidades en el servidor web de la UTN, y el 48% respondieron que están totalmente de acuerdo, este indicar nos permite tener referencia de la necesidad de identificar y corregir vulnerabilidades en servidores web y mantener la seguridad a largo plazo.

DISCUSIÓN DE RESUTADOS

De acuerdo con los resultados encontrados en la encuesta, se presenta el siguiente análisis comparativo:

- Los profesionales de Nivel Operativo del DDTI conocen las amenazas en la nube y los posibles riesgos que pueden acarrear una mala configuración, pero se requiere cubrir necesidades a nivel de recursos humanos en el área de seguridad informática cumpliendo con el requerimiento del organigrama estructural, este análisis concuerda con el estudio de CULOT (2019), donde los profesionales en seguridad informática son muy escasos, las organizaciones deben abordar los desafíos de la ciberseguridad y tomar conciencia sobre como los lideres deben participar activamente.

- Los funcionarios tienen experiencia con administración en la nube y conoce las amenazas de seguridad más comunes y los riesgos que puede ocasionar ante una configuración errónea, donde los atacantes pueden aprovechar para infiltrarse en sistemas y redes, comprometiendo la integridad, la confidencialidad o la disponibilidad de los datos en la organización, por lo que están de acuerdo que se implemente una capa adicional de seguridad en el servidor web de la UTN y se realice pruebas de pentesting de manera frecuente para mitigar e identificar vulnerabilidades y debilidades en el servidor web antes de que los atacantes las aprovechen (Gangineni y Tasmiya, 2023).

- De igual manera señalaron en su mayoría que han utilizado un Gestor de Contenido (CMS) y tienen un nivel de conocimiento de tecnología y están de acuerdo en utilizar la metodología OWASP para identificar, corregir y proteger las aplicaciones web contra posibles amenazas y vulnerabilidades en el servidor de la UTN ya que es una buena práctica en la seguridad informática. Estos resultados concuerdan con lo que manifiesta Gonzáles (2018), que la metodología Open Web Application Security Project (OWASP) es la más utilizada para proteger aplicaciones web siendo la guía más completa para realizar pruebas de seguridad.

CAPÍTULO V
PROPUESTA

Título de la propuesta

Metodología OWASP Web Security Testing Guide (WSTG) V4.2

Objetivo

Analizar las vulnerabilidades en aplicaciones web y evaluar la efectividad del WAF como solución de seguridad en el servidor web de la Universidad Técnica del Norte.

Introducción

Muchas organizaciones de desarrollo de software no incluyen pruebas de seguridad como parte de su proceso de desarrollo de software estándar. La responsabilidad inicial de la seguridad de las aplicaciones debe recaer sobre los desarrolladores porque son ellos los que escriben el código. La guía de pruebas de seguridad web de OWASP es conjunto de técnicas que puede utilizar para encontrar diferentes tipos de agujeros de seguridad. Pero no todas las técnicas son igualmente importantes. El presente trabajo de grado se centra en el servidor web de la Universidad Técnica del Norte, para identificar vulnerabilidades mediante herramientas open source, realizar pruebas de penetración según la guía de pruebas de seguridad web de OWASP y verificar la seguridad de las aplicaciones web en ejecución, corregir vulnerabilidades y garantizar el flujo de desarrollo seguro de programación de acuerdo con la metodología OWASP.

Primera fase de ejecución

Identificar características del servidor web de la UTN

Esta fase se centra en la recolección de información técnica de las aplicaciones en el servidor web de la Universidad Técnica del Norte, para identificar la tecnología en el servidor web utilizamos una herramienta llamada **Wappalyzer** que es muy popular en Linux para identificar las tecnologías utilizadas en cada página web. Wappalyzer está disponible como línea de comandos en Linux y también como una extensión para el navegador Chrome y Firefox, lo que permite obtener información sobre las tecnologías utilizadas en los portales web directamente desde el navegador.

Características del Servidor web de la UTN

Ip servidor	**190.15.141.17**
Alojamiento en la nube	Cedia
Dominio	utn.edu.ec
Servidor Web	Apache
Base de datos	MySQL
Sistema de Gestión de Contenido (CSM)	WordPress
SSL/TLS	SHA-256 con cifrado RSA

Tabla 23. Características de servidor web – UTN
Fuente: Autoría propia (2023)

Definir aplicaciones web que se van a proteger

Un Web Application Firewall (WAF), es una solución de seguridad que se utiliza para proteger las aplicaciones web contra diversas amenazas y ataques cibernéticos. Para definir las aplicaciones que se van a proteger primero se procede a identificar las aplicaciones web que sean públicas, como sitios corporativos, tiendas online, blogs, ya que son objetivos comunes para ataques de inyección SQL, cross-site scripting (XSS), ataques de fuerza bruta y más. Es importante realizar un análisis de riesgo para determinar que aplicaciones web son más críticas y están en mayor riesgo de estar atacadas.

La Universidad Técnica del Norte mantiene alrededor de 50 sitios web, administrados mediante ISPConfig que es un panel de control de alojamiento web de código abierto que permite a los administradores de múltiples sitios web gratuitos y de código abierto para Linux, permite la gestión de subdominios, administrar la Base de datos y facilita la creación y gestión de sitios web mediante la configuración de la gestión de archivos a través de FTP o SFTP. Además, que facilita la instalación y renovación de certificados SSL/TLS para cifrar las conexiones HTTPS.

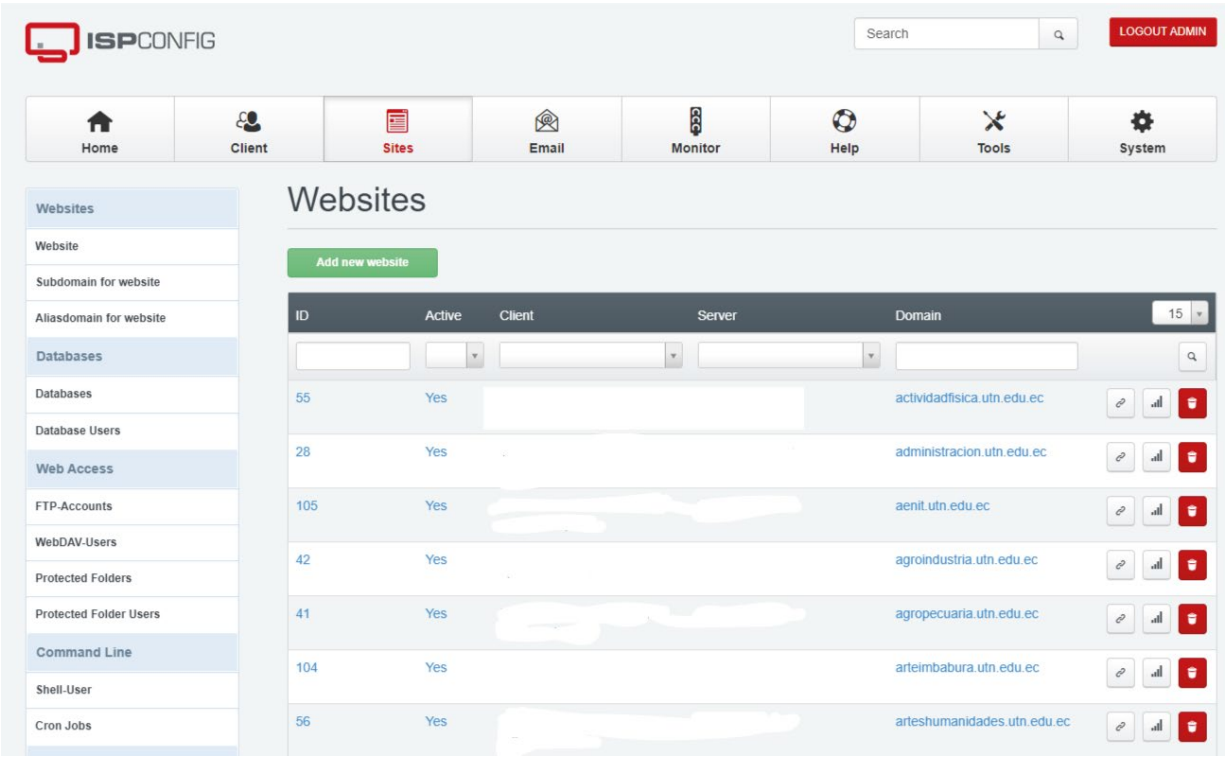


Figura 24. Pantalla de panel de administrador en ISPConfig para la administración de sitios web de la UTN. Fuente: Servidor web - Autoría propia (2023)

La decisión de qué sitios web proteger con un Web Application Firewall (WAF) se basó en varios factores, incluida la audiencia y el tráfico del sitio web. Actualmente la Universidad Técnica del Norte, mantiene varios sitios web públicos de alto perfil, y es ampliamente conocido y visitado por una audiencia masiva a nivel de educación superior y se convierte en un objetivo de ataque cibernético debido a su visibilidad.

Con estas consideraciones se procedió a realizar una evaluación de dominio de la Universidad Técnica del Norte, https://utn.edu.ec mediante la configuración de la propiedad analítica web en Google Analytics 4 [GA4], ya que es fundamental para realizar el seguimiento del tráfico del sitio web, siendo una herramienta poderosa para recopilar datos valiosos sobre el comportamiento del usuario y obtener información detallada sobre como los usuarios llegan al sitio web, permitiendo mejorar la eficacia de las estrategias de marketing y la experiencia del usuario.

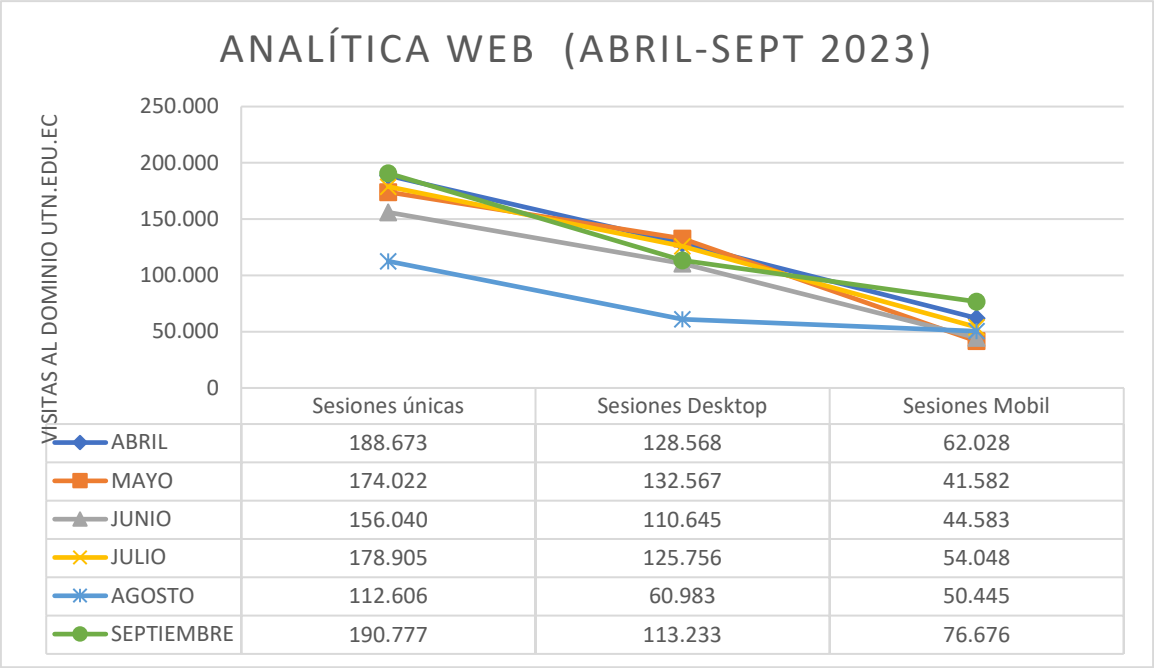
Analítica y tráfico web de dominio utn.edu.ec

La analítica web son importantes para comprender y evaluar el tráfico y la experiencia del usuario en el portal web. Cada una de estas métricas proporciona información específica que puede ser útil para diferentes propósitos.

Sesiones únicas: representan el número de usuarios únicos que han visitado el sitio web en un período de tiempo específico. Cada usuario único se cuenta solo una vez durante ese período, independientemente de cuántas veces haya visitado el portal.

Sesiones por desktop: representa el número de visitas realizadas desde dispositivos de escritorio (como computadoras portátiles y computadoras de escritorio) en el sitio web.

Sesiones móviles: Se refiere al número de visitas que provienen de dispositivos móviles, esta métrica es importante para comprender como la audiencia accede y navega en el sitio web, lo que influye a la toma de decisiones relacionadas con la experiencia del usuario y la optimización del sitio web de la UTN.



	Sesiones únicas	Sesiones Desktop	Sesiones Mobil
ABRIL	188.673	128.568	62.028
MAYO	174.022	132.567	41.582
JUNIO	156.040	110.645	44.583
JULIO	178.905	125.756	54.048
AGOSTO	112.606	60.983	50.445
SEPTIEMBRE	190.777	113.233	76.676

Figura 25. Analítica web utn.edu.ec (abril - sept 2023)
Fuente: Google Analytics GA4 - 2023

Los canales predeterminados del usuario son las categorías específicas en las que GA4 clasifica el tráfico que llega al sitio web. Los canales predeterminados del usuario son:

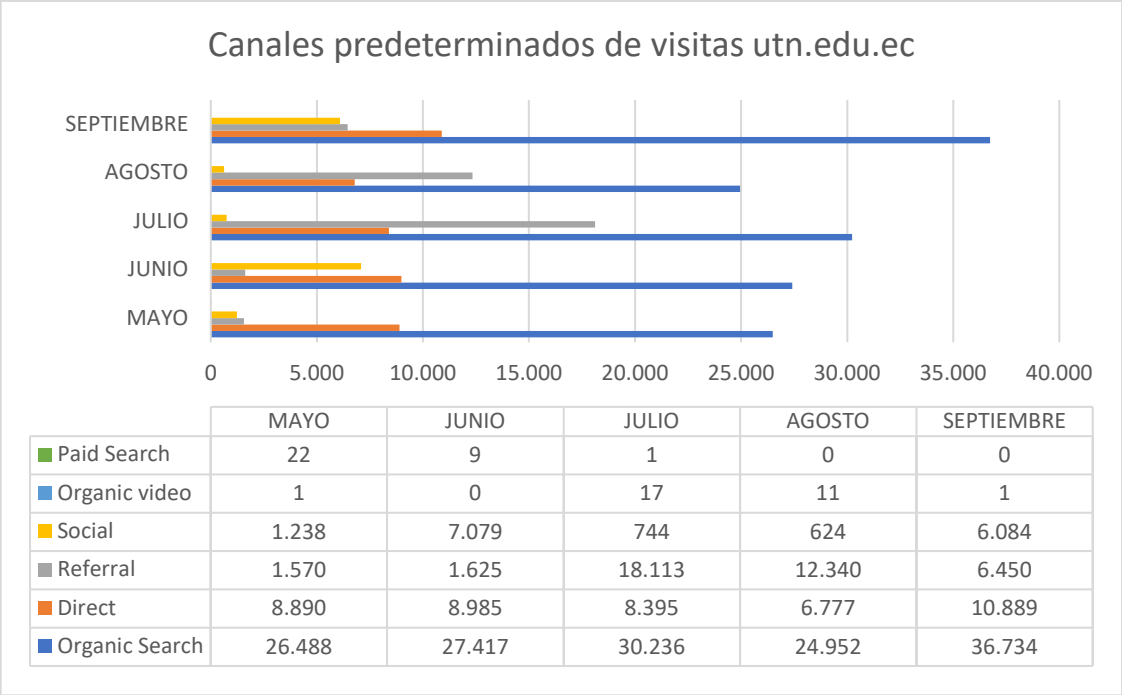
Orgánico: Este canal incluye el tráfico que proviene de motores de búsqueda como Google, Bing u otros, es decir cuando los visitantes hacen clic en enlaces no pagados.

Directo: Este canal se refiere al tráfico que llega directamente al sitio web mediante la introducción de la URL en el navegador o mediante marcadores guardados.

Referido: Significa que los visitantes llegan al sitio web desde otros sitios web externos a esto se le conoce como tráfico de referencia.

Social: Este canal incluye el tráfico que proviene de las redes sociales, como Facebook, Twitter, LinkedIn, Instagram, etc. GA4, registra el tráfico que llega al sitio web desde enlaces compartidos en plataformas de redes sociales.

Video orgánico: Se refiere a una fuente de tráfico específica que proviene de búsquedas de videos, como YouTube, y que llega al sitio web a través de enlaces no pagados desde plataformas de video.



	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE
Paid Search	22	9	1	0	0
Organic video	1	0	17	11	1
Social	1.238	7.079	744	624	6.084
Referral	1.570	1.625	18.113	12.340	6.450
Direct	8.890	8.985	8.395	6.777	10.889
Organic Search	26.488	27.417	30.236	24.952	36.734

Figura 26. Analítica web dominio utn.edu.ec mes (mayo-septiembre 2023)
Fuente: Google Analytics GA4- UTN (2023)

A continuación, se presenta la analítica web del dominio utn.edu.ec, tomando como referencia los meses desde mayo hasta septiembre 2023, donde se puede evidenciar el incremento de visitas orgánicas, siendo el mes de septiembre con mayor número de visitas con un total de 36.734 usuarios únicos que han realizado la búsqueda de manera orgánica; en el mes de julio se observa que 18.113 usuarios han realizado la búsqueda mediante visitas referenciales siendo el rango más alto dentro de los meses establecidos; en cuanto a visitas sociales se puede verificar que el mayor número fue en el mes de junio con un total de 7.079 usuarios que han visitado el sitio web mediante redes sociales.

Segunda fase de ejecución

Configuración de Web Application Firewall en Fortinet

Para esta fase se consideró 7 aplicaciones web, siendo las más visitadas y se procede a registrar en el WAF.

https://www.utn.edu.ec	Portal web principal
https://biblioteca.utn.edu.ec/	Biblioteca
https://posgrado.utn.edu.ec/	Posgrado
https://colegio.utn.edu.ec/	Colegio Universitario
https://estudiante.utn.edu.ec/	Oficina del Estudiante
https://legislacion.utn.edu.ec/	Legislación Universitaria
https://transparencia.utn.edu.ec/	Transparencia Universitaria

Tabla 24. Sitios web protegidos por el WAF
Fuente: Autoría propia (2023)

Configuramos la política de seguridad WAF, seleccionamos las firmas de ataque y las **habilitamos**, en acción seleccionamos **bloquear** y en severidad seleccionamos **alta.**

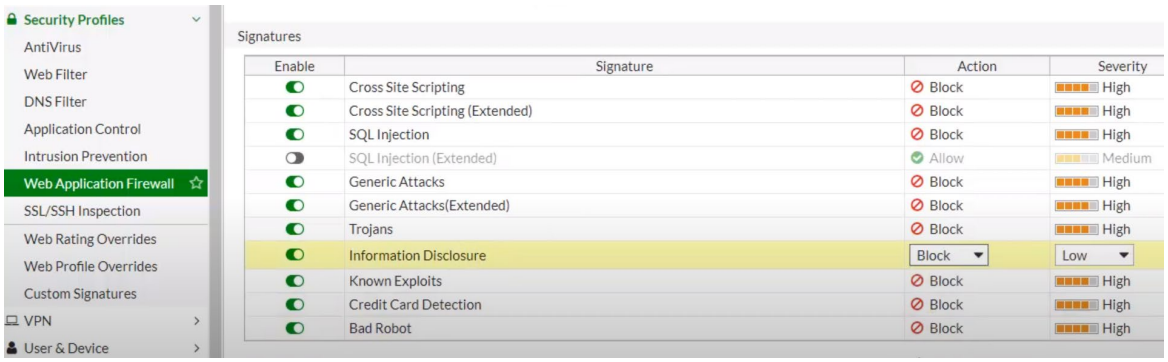


Figura 27. Configuración de política de seguridad en el WAF
Fuente: WAF UTN (2023)

Cambios de direcciones IPs en el registro DNS

La Universidad Técnica del Norte, mantiene la administración de DNS en Hurricane Electric que ofrece servicio de alojamiento DNS gratuito. Esto significa que se puede utilizar la plataforma para administrar los registros DNS sin costo alguno.

Para realizar esta fase consideramos la participación del funcionario de Nivel Operativo del DDTI, que se encarga de la administración de dominios en Hurricane Electric y se procede a registrar las nuevas direcciones IPs en el DNS externo e interno, este es un proceso estratégico para redireccionar el tráfico a través del WAF, esto permite que el WAF inspeccione y filtre el tráfico antes de que llegue al servidor.

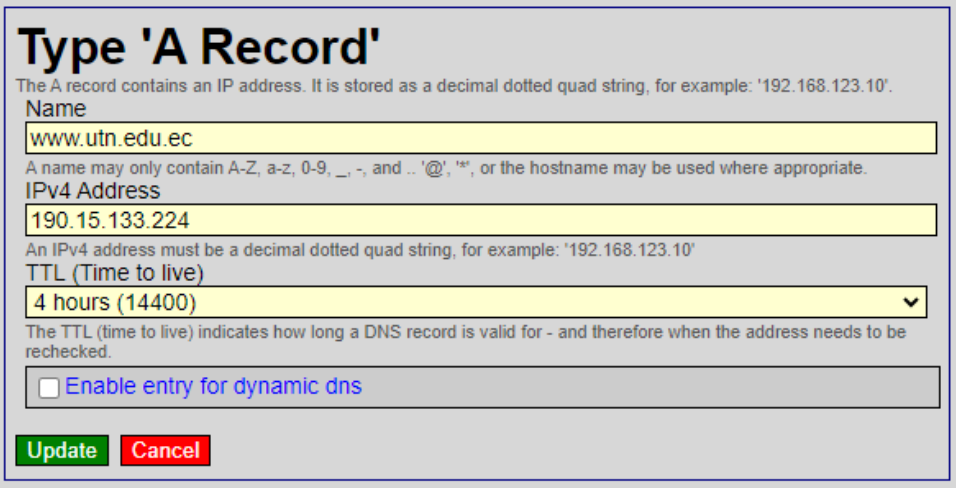


Figura 28. Registro de Ip en el DNS dominio www.utn.edu.ec
Fuente: Autoría propia (2023)

En este caso abrimos una ventana de comandos y simplemente utilizamos **nslookup** para verificar la dirección IP que estamos utilizando.

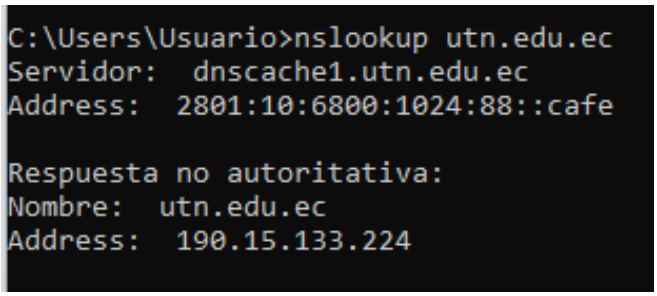


Figura 29. Verificar la dirección Ip del sitio web utn.edu.ec
Fuente: Autoría propia (2023)

https://www.utn.edu.ec	Portal web principal	190.15.133.224
https://biblioteca.utn.edu.ec/	Biblioteca	190.15.133.132
https://posgrado.utn.edu.ec/	Posgrado	190.15.133.225
https://colegio.utn.edu.ec/	Colegio Universitario	190.15.133.177
https://estudiante.utn.edu.ec/	Oficina del Estudiante	190.15.133.226
https://legislacion.utn.edu.ec/	Legislación Universitaria	190.15.133.227
https://transparencia.utn.edu.ec/	Transparencia Universitaria	190.15.133.228

Tabla 25. Registro de nuevas direcciones IPs en el DNS
Fuente: Autoría propia (2023)

Verificar si el sitio web está protegido por el WAF

Para chequear la seguridad, necesitamos abrir un terminal en Kali Linux, y utilizamos la herramienta **wafw00f** que es de código abierto para identificar si un sitio web está protegido por un Firewall de Aplicaciones Web (WAF). Se puede verificar que el sitio web **utn.edu.ec** está detrás de FortiWeb (Fortinet)

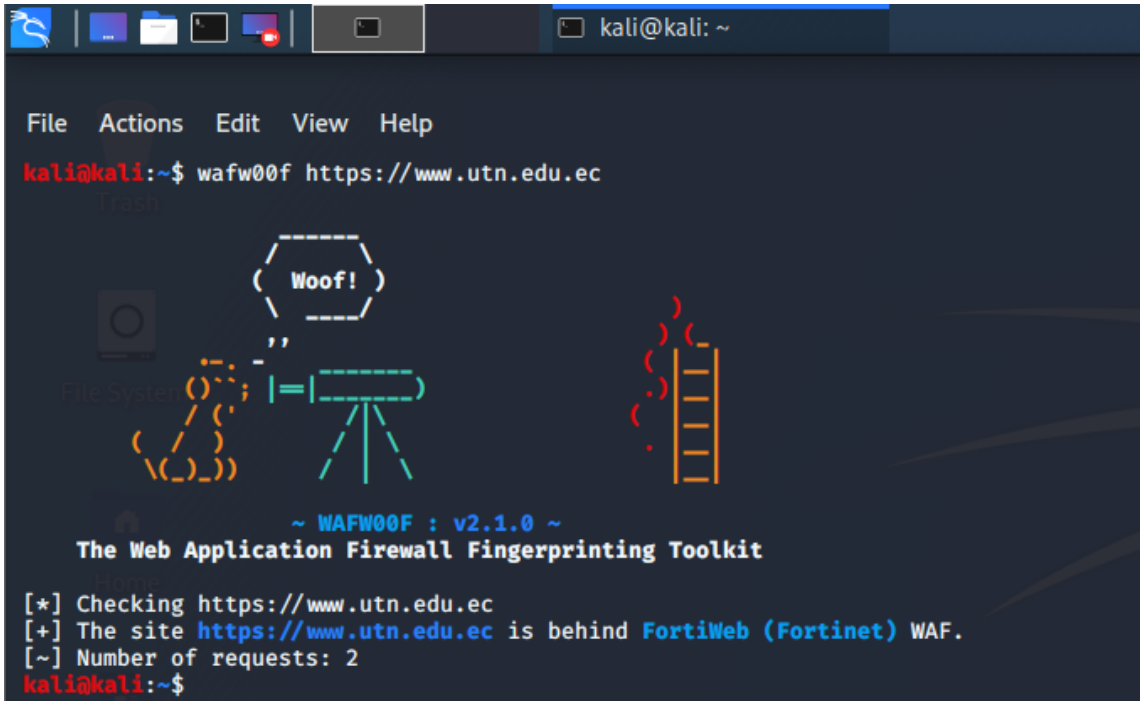


Figura 30. Verificar si el sitio web utn.edu.ec se encuentra protegido por el WAF

Fuente: WAF - Autoría propia (2023)

Tercera Fase de ejecución

Introducción Guía de Pruebas de OWASP WSTG

La creación de la versión 4.2 de la guía de pruebas OWASP tiene como propósito ser una guía estándar para realizar pruebas de penetración contra aplicaciones web. Este proyecto ha estado en desarrollo por muchos años y el objetivo es ayudar a las personas a entender el cómo el porqué, cuando, dónde y cómo de las pruebas hacia aplicaciones web. Esta estructura puede utilizar como marco de trabajo como una plantilla para realizar una propia estructura para realizar las pruebas (OWASP, 2021).

Según el OWASP define **vulnerabilidad** como una falla o debilidad en el diseño, implementación, operación o administración de un sistema que podría explotarse para comprometer los objetivos de seguridad del sistema. Y **amenaza es** cualquier cosa (un atacante externo malicioso, un usuario interno, una inestabilidad del sistema, etc.) que

pueda dañar los activos de una empresa como los datos en una base de datos o en el sistema de archivos al explotar una vulnerabilidad.

Metodología de pruebas OWASP

Las pruebas de seguridad nunca serán una ciencia exacta, donde se puede definir una lista completa de todos los posibles inconvenientes a ser evaluados. De hecho, las pruebas de seguridad son una técnica apropiada para probar la seguridad de las aplicaciones web bajo ciertas circunstancias. El objetivo del proyecto es recopilar todas las técnicas de pruebas posibles, explicar las técnicas y mantener la guía actualizada. El método de pruebas de seguridad en aplicaciones web se basa en la perspectiva de caja negra, en donde el profesional no conoce nada o tiene poca información sobre la aplicación a ser evaluada. El modelo está constituido por: el profesional, herramientas y finalmente la aplicación. Hay muchos escenarios a los cuales se puede enfrentar, depende de la experiencia del profesional. Hay una inadecuada percepción de utilizar las herramientas sin antes conocer la metodología (Marulanda & Díaz, 2018).

Pruebas de penetración

Según la guía de Pruebas OWASP (2021), la prueba de penetración es el arte de probar una aplicación en funcionamiento de manera remota, para encontrar vulnerabilidades de seguridad, sin conocer el funcionamiento interno de la aplicación en sí, típicamente un equipo de pruebas de penetración tendrá acceso hacia una aplicación, como si fuesen los usuarios. El profesional actúa como un atacante e intenta encontrar y explotar vulnerabilidades. Una prueba de seguridad contra aplicaciones web se enfoca únicamente en evaluar la seguridad de una aplicación. El proceso involucra análisis activo por debilidades, fallas técnicas, o vulnerabilidades.

Laboratorio para escaneo de vulnerabilidades web

Instalación de MV Kali Linux

Esta herramienta está diseñada para profesionales de la seguridad, es ampliamente utilizado para llevar a cabo pruebas de seguridad e identificar vulnerabilidades en aplicaciones. Los administradores de sistemas y los expertos en seguridad pueden utilizar estas herramientas para fortalecer la seguridad de sus sistemas.

Procedemos a configurar un software de virtualización puede ser VirtualBox o VMware

Descargar la máquina virtual de Kali Linux de su sitio web oficial **https://cdimage.kali.org/kali-2023.3/kali-linux-2023.3-vmware-amd64.7z**

Abrir máquina virtual de Kali en VMware

Usuario y contraseña por defecto: **kali**

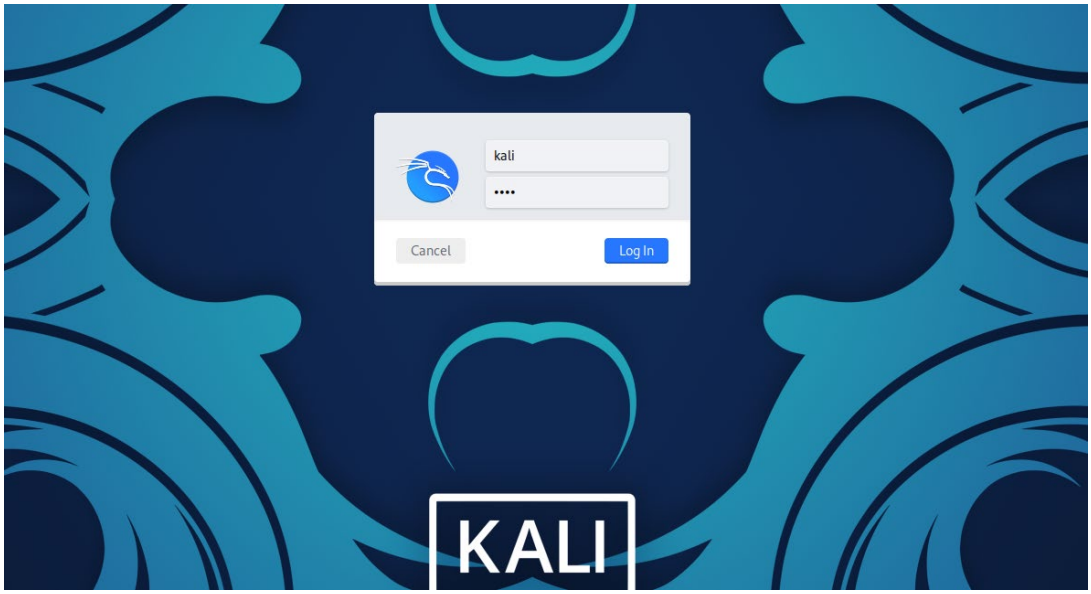


Figura 31. Pantalla de inicio de sesión de Kali Linux Fuente: Autoría propia (2023)

Instalación de OWASP ZAP

OWASP ZAP (Zed Attack Proxy) es una herramienta de código abierto ampliamente utilizada para probar y evaluar la seguridad de aplicaciones web. Es un escáner de vulnerabilidades que identifica los fallos de seguridad, asigna un nivel de riesgo y recomienda mecanismos de explotación y solución.

Actualizar la base de datos de apt

sudo apt-get update

Instalar zaproxy via apt

sudo apt-get install zaproxy

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install zaproxy
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  zaproxy
0 upgraded, 1 newly installed, 0 to remove and 757 not upgraded.
Need to get 186 MB of archives.
After this operation, 246 MB of additional disk space will be used.
Get:1 http://mirror.cedia.org.ec/kali kali-rolling/main amd64 zaproxy all 2.1
3.0-0kali1 [186 MB]
Fetched 186 MB in 21s (9,043 kB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 398680 files and directories currently installed.)
Preparing to unpack .../zaproxy_2.13.0-0kali1_all.deb ...
Unpacking zaproxy (2.13.0-0kali1) ...
Setting up zaproxy (2.13.0-0kali1) ...
Processing triggers for kali-menu (2023.4.3) ...
```

Figura 32. Instalación de OWASP ZAP
Fuente: Autoría propia (2023)

Posterior a la instalación se verifica en el menú de aplicaciones, el icono ZAP y la pantalla inicial.

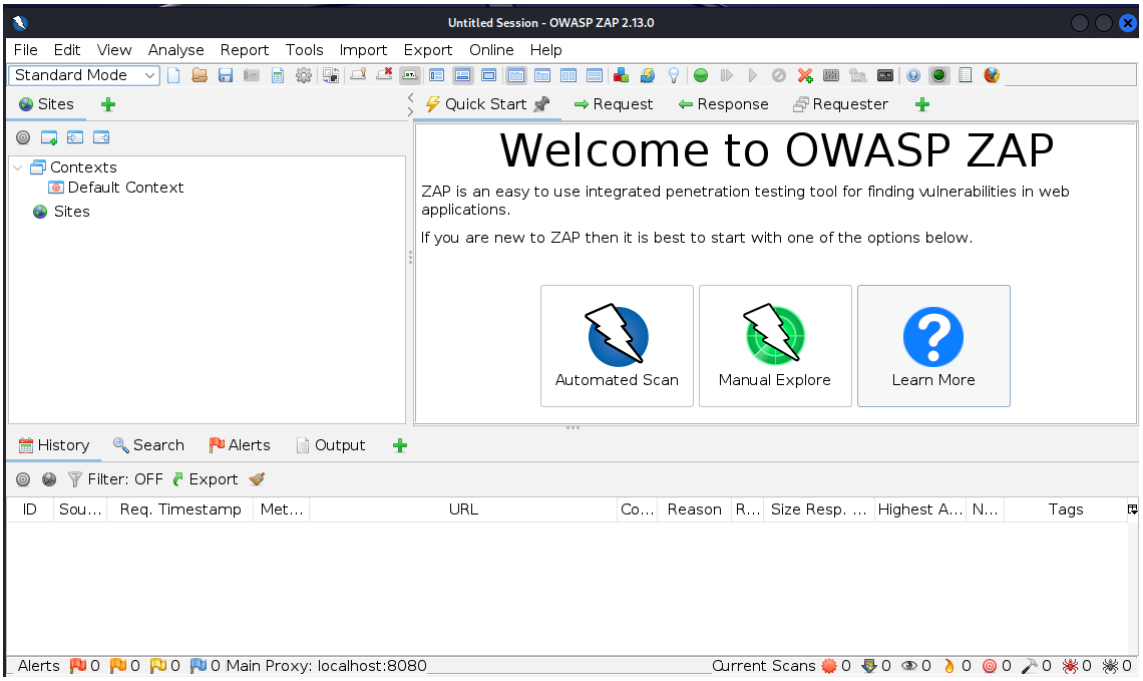


Figura 33. Pantalla de bienvenida de OWASP ZAP
Fuente: Autoría propia (2023)

Cuarta Fase de ejecución

Pruebas de seguridad de aplicaciones web según la Metodología OWASP Web Security Testing Guide (WSTG)

El WSTG es una guía que proporciona un conjunto de prácticas recomendadas y metodologías para llevar a cabo pruebas de seguridad en aplicaciones web. ZAP es una herramienta ampliamente reconocida en la comunidad de seguridad web y es una elección sólida para realizar muchas de las actividades de pruebas de seguridad que se describen en el WSTG.

Existen varios tipos de escaneo, OWASP ZAP cuenta con 4 tipos de escáner:

Safe mode: escaneo con un nivel menos intrusivo, este tipo de escaneo no lanza ninguna prueba maliciosa que pudiera comprometer la disponibilidad del servicio.

Protected mode: este escaneo extiende su alcance, OWASP ZAP encuentra nuevos sitios web, subdominios, reduce la probabilidad de ejecutar acciones que puedan tener consecuencias no deseadas, como ataques de inyección o eliminación de datos.

Standard mode: este escaneo es el más utilizado y permite lanzar todas las pruebas de ataque, proporciona una variedad de herramientas y capacidades que permiten a los profesionales de seguridad identificar y mitigar vulnerabilidades en aplicaciones web. (Recomendado)

ATTACK mode: En este modo, los profesionales de seguridad pueden realizar ataques específicos y evaluar cómo reacciona una aplicación a diversas amenazas.

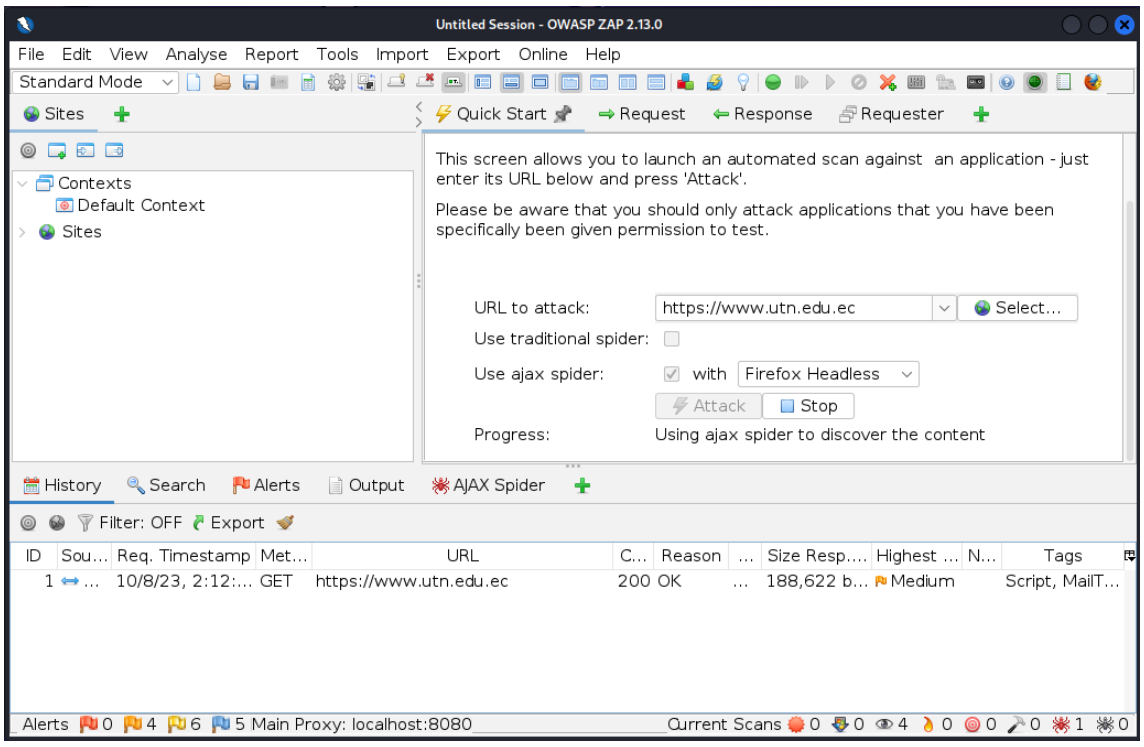


Figura 34. Ataque al dominio utn.edu.ec en Aplicación OWASP ZAP
Fuente: Autoría propia (2023)

En alertas podemos observar los fallos de seguridad, que como escáner de vulnerabilidades ha encontrado OWASP ZAP.

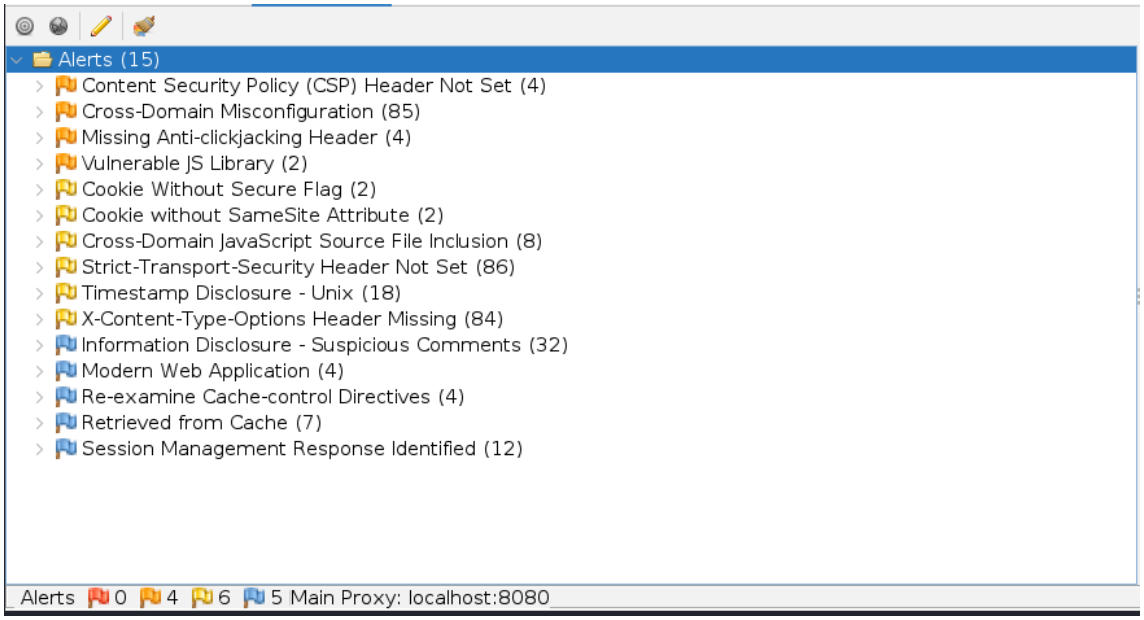


Figura 35. Alertas detectadas por OWASP ZAP
Fuente: Autoría propia (2023)

Resultados de análisis de vulnerabilidades

Indicador	Vulnerabilidad	Descripción
A01:2021-Broken Access Control	Cross-Domain Misconfiguration	Es posible que se puedan cargar datos del navegador web debido a una mala configuración de Cross Origin Resource Sharing (CORS) en el servidor web. La mala configuración de CORS en el servidor web permite solicitudes de lectura entre dominios desde dominios arbitrarios de terceros, utilizando API no autenticadas en este dominio. Sin embargo, las implementaciones del navegador web no permiten que terceros arbitrarios lean la respuesta de las API autenticadas. Esto reduce un poco el riesgo. Un atacante podría utilizar esta configuración errónea para acceder a datos que están disponibles sin autenticación, pero que utilizan alguna otra forma de seguridad, como una lista blanca de direcciones IP.
	Evidencia	Access-Control-Allow-Origin: *
	Solución	Verificar que los datos confidenciales no estén disponibles de manera no autenticada (mediante una lista blanca de direcciones IP, por ejemplo). Configure el encabezado HTTP "Access-Control-Allow-Origin" para un conjunto de dominios más restrictivo, o elimine todos los encabezados CORS por completo, para permitir que el navegador web aplique la Política del mismo origen (SOP) de una manera más restrictiva.

	Riesgo	Medio
	CWE ID	264

Tabla 26. Análisis de vulnerabilidad Cross-Domain Misconfiguration en dominio utn.edu.ec
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
A05:2021-Security Misconfiguration	Content security policy (CSP)	La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la destrucción de sitios o la distribución de malware.
	Solución	Asegurarse de que el servidor web, servidor de aplicaciones, equilibrador de carga, etc. esté configurado para establecer el encabezado Content-Security-Policy.
	Riesgo	Medio
	CWE ID	693

Tabla 27. Análisis de vulnerabilidades Content security policy (CSP)
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
A05:2021- Security Misconfiguration	Missing Anti-clickjacking Header	La respuesta no incluye la Política de seguridad de contenido con la directiva frame-ancestors o X-Frame-Options para proteger contra ataques de ClickJacking.
WSTG-v42-CLNT-09	Solución	Los navegadores web modernos admiten los encabezados HTTP Content-Security-Policy y X-Frame-Options. Verificar que

		uno de ellos esté configurado en todas las páginas web devueltas por el sitio web.
	Riesgo	Medio
	CWE ID	1021

Tabla 28. Análisis de vulnerabilidad Missing Anti-clickjacking Header
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
A06:2021- Vulnerable and Outdated Components	Vulnerable JS Library	La biblioteca identificada bootstrap, versión 3.3.7, es vulnerable.
	Evidencia	* Bootstrap v3.3.7
	Solución	Actualizar a la última versión de bootstrap.
	Riesgo	Medio
	CWE ID	829
	CVE	2019-8331

Tabla 29. Análisis de vulnerabilidad Vulnerable JS Library
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
A05:2021- Security Misconfiguration	Cookie Without Secure Flag	Se ha configurado una cookie sin el indicador seguro, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas.
WSTG-v42-SESS-02	Evidencia	Set-Cookie: cookiesession1
	Solución	Siempre que una cookie contenga información confidencial o sea un token de sesión, siempre debe transmitirse mediante un canal cifrado. Verificar que la bandera segura esté configurada para las cookies que contienen información confidencial.
	Riesgo	Bajo
	CWE ID	614

	WASC ID	13

Tabla 30. Análisis de vulnerabilidad Cookie Without Secure Flag en dominio utn.edu.ec
Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	**Vulnerabilidad**	**Descripción**
A01:2021-Broken Access Control	Cookie without SameSite Attribute	El atributo SameSite es una contramedida eficaz contra la falsificación de solicitudes entre sitios, la inclusión de secuencias de comandos entre sitios (cross-site) y los ataques de sincronización.
	Evidencia	Set-Cookie: cookiesession1
	Solución	Asegurarse de que el atributo SameSite esté configurado en "lax" o, “strict” para todas las cookies.
	Riesgo	Bajo
	CWE ID	1275
	WASC ID	13

Tabla 31. Análisis de vulnerabilidad Cookie without SameSite Attribute
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	**Vulnerabilidad**	**Descripción**
A08:2021 – Software and Data Integrity Failures	Cross-Domain JavaScript Source File Inclusion	La página incluye uno o más archivos de script con fuentes.
	Evidencia	<script type='text/javascript' src='https://www.googletagmanager.com/gtag/js?id=UA-103334727-1' id='google_gtagjs-js' async></script>
	Solución	Asegurarse de que los archivos fuente de JavaScript se carguen únicamente desde fuentes confiables y que los usuarios finales de la aplicación no puedan controlar las fuentes.
	Riesgo	Bajo

	CWE ID	829
	WASC ID	15

Tabla 32. Análisis de la vulnerabilidad Cross-Domain JavaScript Source File Inclusion
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
A05:2021- Security Misconfiguration	Strict-Transport-Security Header Not Set	HTTP Strict Transport Security (HSTS) es un mecanismo de política de seguridad web mediante el cual un servidor web declara que los agentes de usuario conformes (como un navegador web) deben interactuar con él utilizando únicamente conexiones HTTPS seguras (es decir, HTTP superpuesto a TLS/SSL). HSTS es un protocolo de seguimiento de estándares del IETF (Internet Engineering Task Force) y se especifica en RFC 6797.
	Evidencia	-
	Solución	Verificar que el servidor web, servidor de aplicaciones etc., esté configurado para hacer cumplir "Strict-Transport-Security"
	Riesgo	Bajo
	CWE ID	319
	WASC ID	15

Tabla 33. Análisis de vulnerabilidad Strict-Transport-Security Header Not Set
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
A01:2021-Broken Access Control	Timestamp Disclosure - Unix	Una marca de tiempo fue revelada, por la aplicación/servidor web.
	Evidencia	1732584193
	Solución	Manualmente verificar si los datos del timestamp no son sensibles, y que los datos no pueden agregarse para revelar patrones explotables.

	Riesgo	Bajo
	CWE ID	200
	WASC ID	13

Tabla 34. Análisis de vulnerabilidad Timestamp Disclosure
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	**Vulnerabilidad**	**Descripción**
A05:2021-Security Misconfiguration	X-Content-Type-Options Header Missing	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen un rastreo MIME en el cuerpo de la respuesta, lo que potencialmente hace que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado.
	Evidencia	-
	Solución	Este problema todavía se aplica a las páginas de tipo de error (401, 403, 500, etc.), ya que esas páginas a menudo todavía se ven afectadas por problemas de inyección, en cuyo caso todavía existe la preocupación de que los navegadores detecten páginas que no corresponden a su tipo de contenido real. En el umbral "Alto", esta regla de análisis no alertará sobre respuestas de error del cliente o del servidor.
	Riesgo	Bajo
	CWE ID	693
	WASC ID	15

Tabla 35. Análisis de vulnerabilidad X-Content-Type-Options Header Missing
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
A01:2021-Broken Access Control	Information Disclosure - Suspicious Comments	La respuesta parece contener comentarios sospechosos que pueden ayudar a un atacante. Nota: Las coincidencias realizadas dentro de bloques o archivos de secuencias de comandos se refieren a todo el contenido, no solo a los comentarios.
WSTG-v42-INFO-05	Evidencia	admin
	Solución	Elimine todos los comentarios que devuelvan información que pueda ayudar a un atacante y solucione cualquier problema subyacente al que se refieran.
	Riesgo	Informativa
	CWE ID	200
	WASC ID	13

Tabla 36. Análissi de vulnerabilidad Information Disclosure - Suspicious Comments
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
Informativa	Modern Web Application	La aplicación parece ser una aplicación web moderna. Si necesita explorarlo automáticamente, entonces el Ajax Spider puede ser más efectivo que el estándar.
	Evidencia	-
	Solución	Se han encontrado enlaces que no tienen los atributos href tradicionales. Esta es una alerta informativa y por lo tanto no se requieren cambios.
	Riesgo	Informativa

Tabla 37. Análisis de vulnerabilidad Information Disclosure - Suspicious Comments
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
WSTG-v42-ATHN-06	Re-examine Cache-control Directives	El encabezado de control de caché no se ha configurado correctamente o falta, lo que permite que el navegador y los servidores proxy almacenen en caché el contenido. Para activos estáticos como css, js o archivos de imagen, esto podría ser la intención; sin embargo, se deben revisar los recursos para garantizar que no se almacene en caché ningún contenido confidencial.
	Evidencia	-
	Solución	Para contenido seguro, asegúrese de que el encabezado HTTP de control de caché esté configurado con “no-cache, no-store, must-revalidate” Si un activo debe almacenarse en caché, considere configurar las directivas "public, max-age, immutable".
	Riesgo	Informativa
	CWE ID	525
	WASC ID	13

Tabla 38.Análisis de vulnerabilidades Re-examine Cache-control Directives
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
WSTG-v42-ATHN-06	Retrieved from Cache	Este es principalmente un problema cuando los servidores de almacenamiento en caché, como los cachés "proxy", están configurados en la red local. Esta configuración suele encontrarse en entornos corporativos o educativos. La presencia del encabezado 'Age' indica que se está utilizando un servidor de almacenamiento en caché compatible con HTTP/1.1.
	Evidencia	Age: 524206
	Solución	Validar que la respuesta no contenga información sensible, personal o específica del usuario. Si es así, considere el uso de los siguientes encabezados de respuesta HTTP para limitar o evitar que otro usuario almacene y recupere el contenido de la memoria caché.
	Riesgo	Informativa
	CWE ID	-
	WASC ID	-

Tabla 39. Análisis de vulnerabilidades Retrieved from Cache
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

Indicador	Vulnerabilidad	Descripción
WSTG-v42-ATHN-06	Session Management Response Identified	Se ha identificado que la respuesta proporcionada contiene un token de gestión de sesión.
	Evidencia	-
	Solución	Se trata de una alerta informativa más que de una vulnerabilidad, por lo que no hay nada que solucionar.
	Riesgo	Informativa
	CWE ID	-
	WASC ID	-

Tabla 40. Análisis de vulnerabilidad Session Management Response Identified
Fuente: Escaneo de vulnerabilidades dominio utn.edu.ec (2023)

De acuerdo con los resultados del escáner de vulnerabilidades se presenta el tipo de riesgo y la solución que debe ser mitigado, estas correcciones se basan a nivel de desarrollo y de servidor las mismas que no están al alcance del objetivo de esta tesis, por lo que se procederá a direccionar a cada área del DDTI.

Técnica de reconocimiento y transferencia de zona

Propósito: Recopilar de información expuesta de la Universidad Técnica del Norte sin ingresar a su sitio web oficial, para esta técnica mediante el navegador web buscamos la directiva **site: utn.edu.ec**, nos permite realizar un descubrimiento en motores de búsqueda, e identificar los resultados indexados por Google, permite identificar diferentes subdominios asociados expuestos indirectamente en sitios web de terceros.

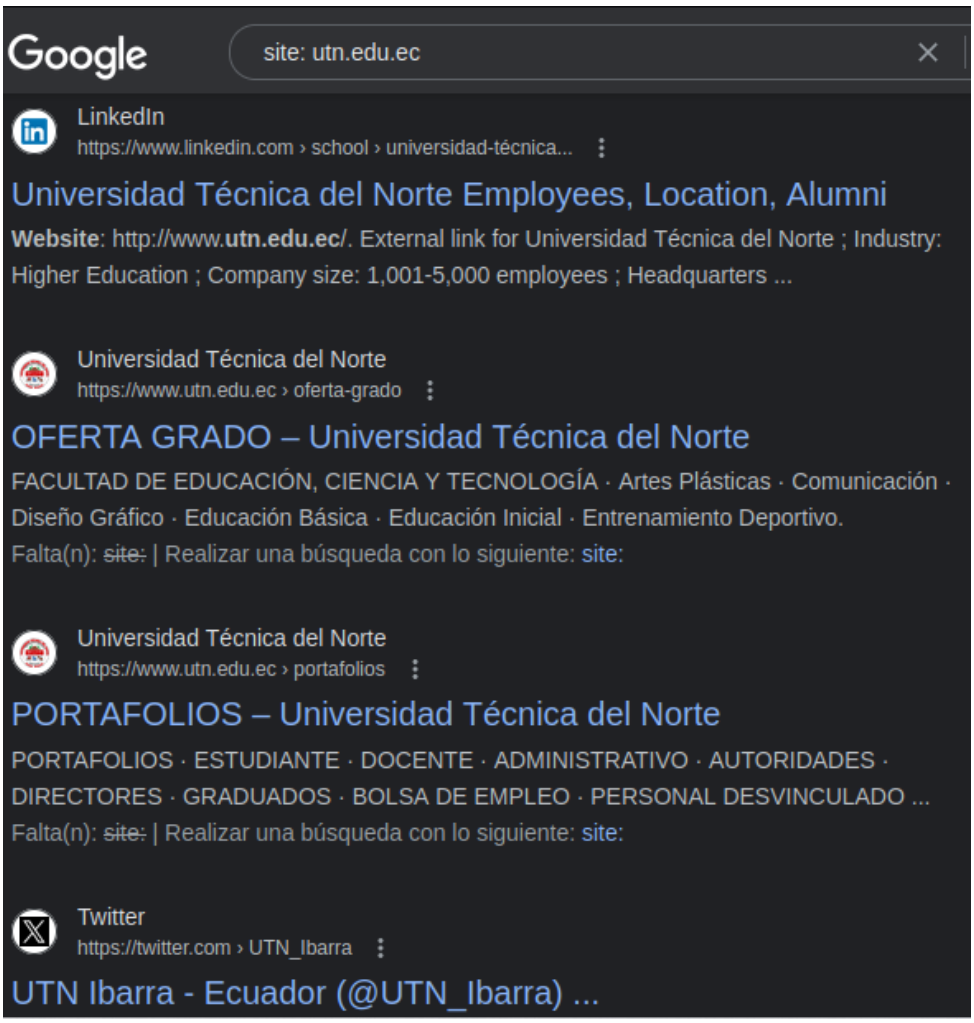


Figura 36. Búsqueda en Google dominio utn.edu.ec
Fuente: Autoría propia (2023)

Podemos identificar diversos enlaces que direccionan directamente a sitios web oficiales y redes sociales administrados por la UTN.

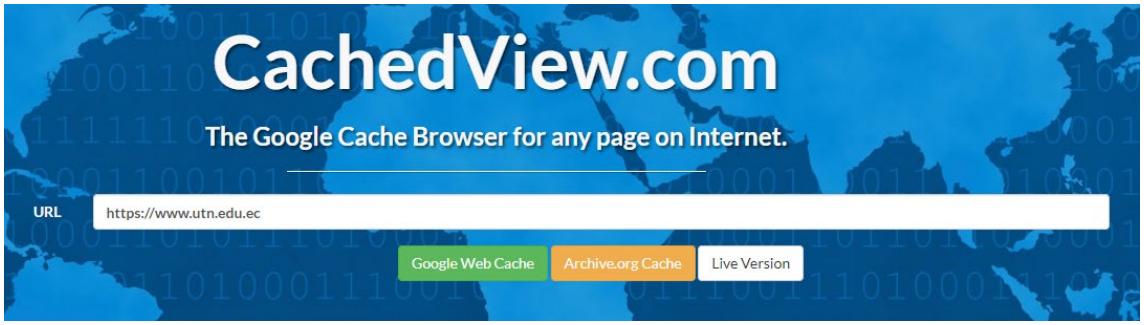


Figura 37. Directiva caché de Google
Fuente: Autoría propia (2023)

La directiva caché de Google muestra como Google almacenó en su caché el sitio web de utn.edu.ec (sin necesidad de visitar el sitio web original)

Otro tipo de peticiones utilizando Google Hacking Database https://www.exploit-db.com/google-hacking-database es una base de datos que utiliza el motor de búsqueda de Google para temas de hacking ético.

Escaneo de puertos utn.edu.ec

Escaneo de puertos sigiloso sobre la dirección Ip **190.15.133.224,** con la directiva -T5, el comando debe ejecutarse con los privilegios de root. Se puede visualizar los puertos abiertos dentro del servidor sin embargo el alcance de nuestra investigación, el puerto 80 está muy asociado a la aplicación web. Ahora necesitamos navegar en el sitio web que esta por detrás del puerto 80 mediante la herramienta de exploración inicial.

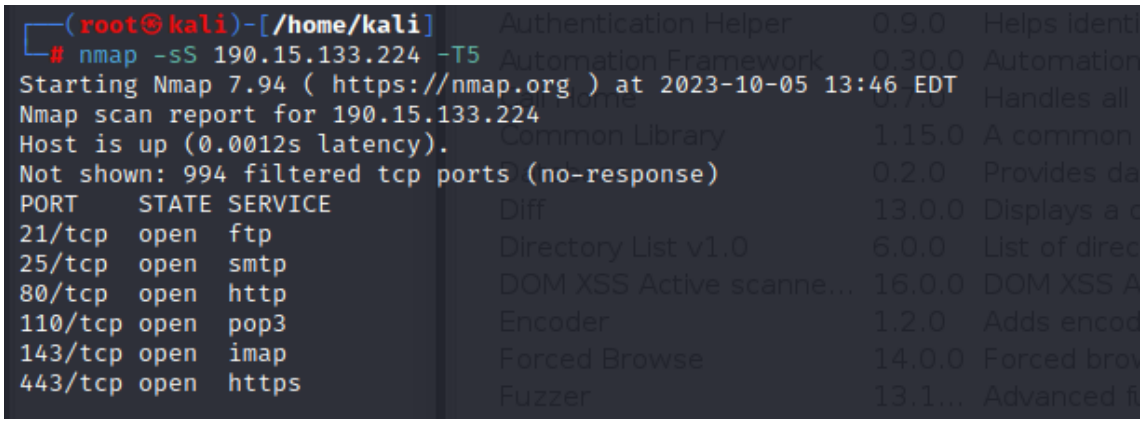


Figura 38. Escaneo de puertos dominio utn.edu.ec
Fuente: Autoría propia (2023)

Consultamos tipo de registro MX, podemos interpretar que la organización mantiene servidor de correo Microsoft mail.protection.outlook.com

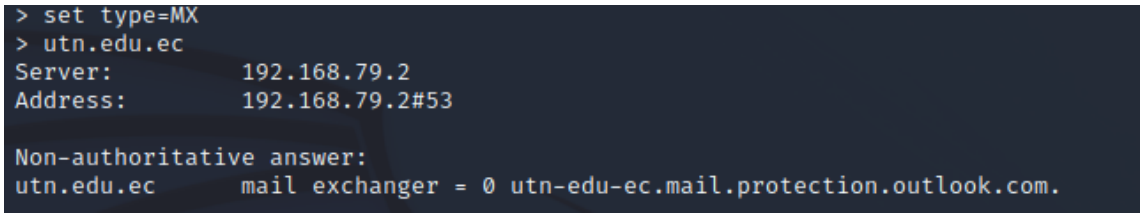


Figura 39. Registro MX de dominio utn.edu.ec
Fuente: Autoría propia (2023)

Obtener los nombres de dominio

```
┌──(kali㉿kali)-[~]
└─$ host -t NS utn.edu.ec
utn.edu.ec name server ns1.utn.edu.ec.
utn.edu.ec name server ns4.he.net.
utn.edu.ec name server ns1.he.net.
utn.edu.ec name server ns2.he.net.
utn.edu.ec name server ns3.he.net.
```

Figura 40. Figura 39. Nombres de dominio utn.edu.ec
Fuente: Autoría propia (2023)

Ahora hacemos ping al DNS ns1.utn.edu.ec

```
┌──(root㉿kali)-[/home/kali]
└─# ping ns1.utn.edu.ec
PING ns1.utn.edu.ec (192.100.198.26) 56(84) bytes of data.
64 bytes from 192.100.198.26 (192.100.198.26): icmp_seq=1 ttl=128 time=64
5 ms
64 bytes from 192.100.198.26 (192.100.198.26): icmp_seq=2 ttl=128 time=92
2 ms
64 bytes from 192.100.198.26 (192.100.198.26): icmp_seq=3 ttl=128 time=14
06 ms
```

Figura 41. Ping al DNS ns1.utn.edu.ec
Fuente: Autoría propia (2023)

Verificar con registro TXT quien está autorizado a enviar correos a nombre de la organización. Se puede verificar que solo miembros de dominio pueden enviar y todo el resto está denegado, es un buen control.

```
> set type=TXT
> utn.edu.ec
Server:         192.168.79.2
Address:        192.168.79.2#53

Non-authoritative answer:
utn.edu.ec      text = "adobe-idp-site-verification=e0f4e93e-3c87-4bda-96
0e-35811833a9c8"
utn.edu.ec      text = "v=spf1 include:spf.protection.outlook.com -all"
utn.edu.ec      text = "e0f4e93e-3c87-4bda-960e-35811833a9c8"
utn.edu.ec      text = "974b9fab-8bfb-47c4-b39b-fbe5b2dc3e6d"

Authoritative answers can be found from:
```

Figura 42. Verificar registro TXT dominio utn.edu.ec
Fuente: Autoría propia (2023)

Consultamos al servidor DNS, el comando responde con el listado de subdominios, lo que se hizo es una transferencia de zonas, no es crítico, pero si es una oportunidad de mejora para evitar que estén expuestas las direcciones.

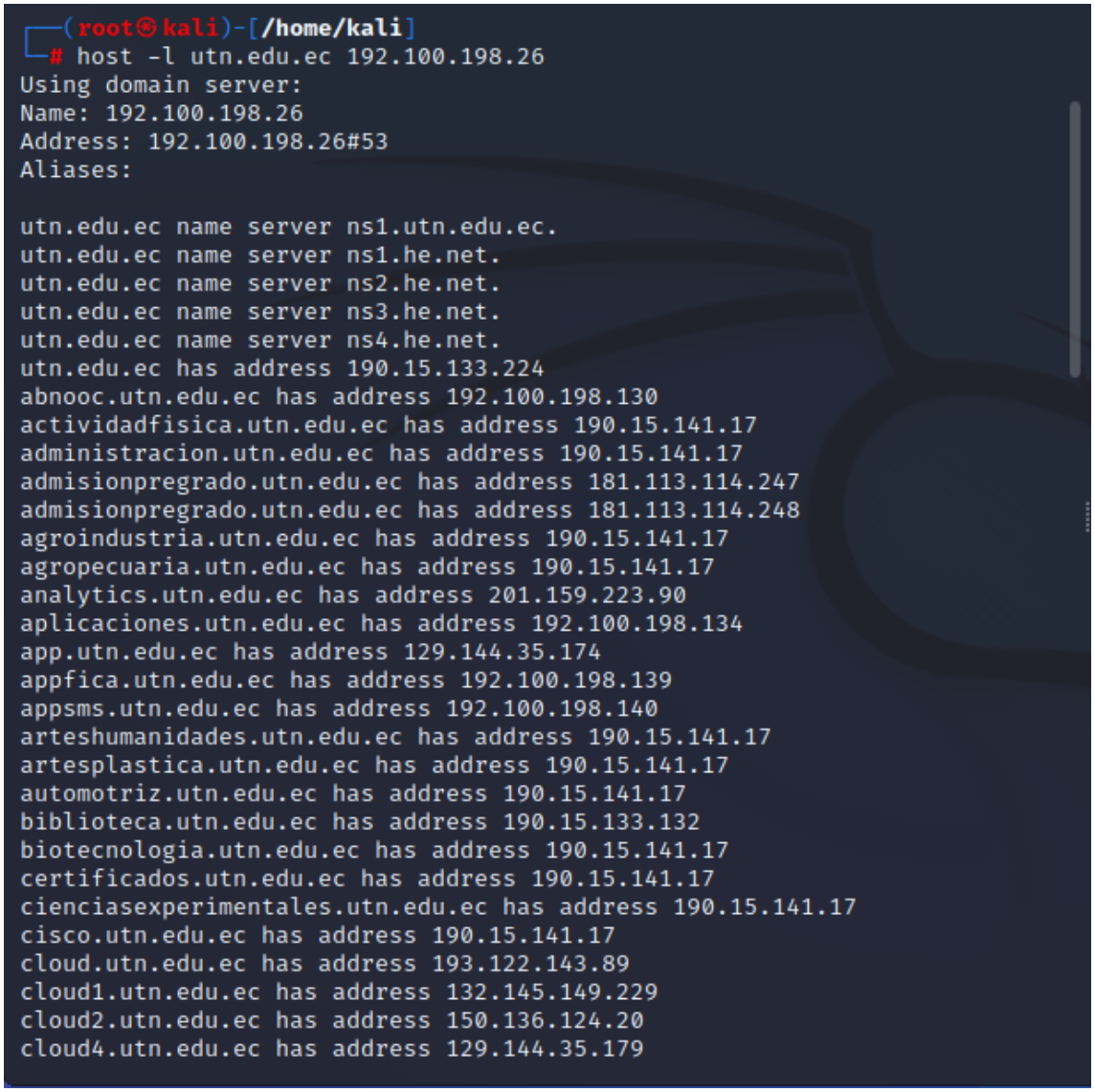


Figura 43. Listado de subdominios identificados
Fuente: Autoría propia (2023)

En este sentido se tomó acciones a nivel de administración de DNS, y se agregó en la configuración lo siguiente:

allow-transfer { none; };
Para no permitir las transferencias por defecto.

Meta archivos del servidor

Propósito: Revisar los metas archivos del servidor que por algún tipo de exposición de información se puede identificar desde los directorios de la aplicación o rutas y tratar de crear una lista de directorios, por lo general el archivo robot está en la raíz.

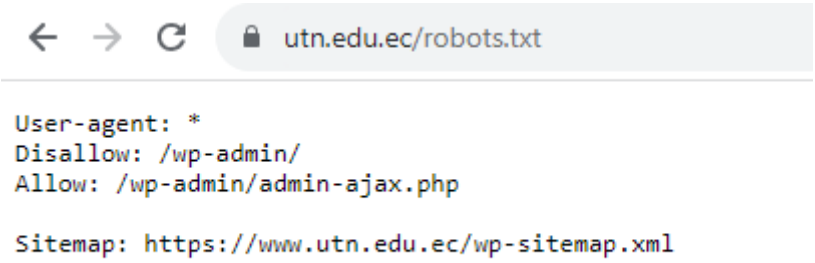


Tabla 41. Análisis de meta archivos dominio utn.edu.ec
Fuente: Autoría propia (2023)

Evaluación del WAF

Los informes pueden mostrar tendencias y patrones de ataques, la evaluación del WAF de un sitio web implica revisar su configuración, realizar pruebas de seguridad, monitorear registros, mantenerlo actualizado y garantizar que no afecte negativamente al rendimiento del sitio. La seguridad en línea es un proceso continuo, por lo que es importante revisar y mejorar regularmente la protección proporcionada por el WAF.

Crear y optimizar políticas de seguridad en tiempo real para ampliar la cobertura de seguridad contra ataques conocidos y desconocidos o de día cero y hacer todo esto con un mínimo de falsos positivos, para garantizar que no se bloquee el tráfico legítimo y no se impide que los usuarios accedan a la aplicación web.

Principales tipos de detección de ataques

El WAF inspecciona el tráfico a nivel de aplicación y detecta actividad maliciosa y potencial, basando en un conjunto de reglas siendo la principal funcionalidad que proporciona un WAF. Registrar todas las detecciones ayuda a identificar datos maliciosos y objetivos atacados, detectan una gran cantidad de ataques contra vulnerabilidades de aplicaciones web como ataques de inyección, navegación forzada, uso no autorizado o denegación de servicios. Según el proyecto de criterios de evaluación de Firewall de OWASP (2013) es importante que el WAF admita la detección de todo el tráfico que lo atraviesa; en general el propósito del WAF es bloquear tráfico malicioso.

Reportes del WAF

En un reporte de un Web Application Firewall (WAF), los "**eventos**" se refieren a las ocurrencias individuales o incidentes de tráfico web que han sido detectados y registrados por el WAF como posibles amenazas o actividades sospechosas. Los **"porcentajes"** se refieren a la distribución o proporción de eventos en función de diferentes categorías o características.

El desglose diario de los tipos de ataques detectados con más frecuencia en el mes de septiembre 2023.

Fecha	Tipo de ataque	Eventos	Porcentajes
2023-09-24	Reputación Ip	296	58.50
	Divulgación de información	209	41.30
	Ataques genéricos	1	0.20
	Subtotal (3)	506	7.53
2023-09-25	Reputación Ip	534	55.86
	Divulgación de información	405	42.36
	Exploits conocidos	11	1.15
	Other (1)	6	0.63
	Subtotal (4)	956	14.22
2023-09-26	Ataques genéricos	1119	46.55
	Reputación Ip	659	27.41
	Divulgación de información	429	17.85
	Other (4)	197	8.19
	Subtotal (7)	2404	35.76
2023-09-27	Divulgación de información	354	84.09
	Reputación Ip	64	15.20
	Ataques genéricos	2	0.48
	Other (1)	1	0.24
	Subtotal (4)	421	6.26
2023-09-28	Ataques genéricos	1453	76.23
	Divulgación de información	213	11.18
	SQL Injection	152	7.97
	Other (3)	88	4.62
	Subtotal (6)	1906	28.35
2023-09-29	Reputación Ip	68	56.20
	Divulgación de información	44	36.36
	Exploits conocidos	8	6.61
	Other (1)	1	0.83
	Subtotal (4)	121	1.80
Other(1)		408	6.07

Tabla 42. Tipos de ataques detectados por el WAF con más frecuencia en el mes de septiembre 2023
Fuente: Reporte WAF UTN (2023)

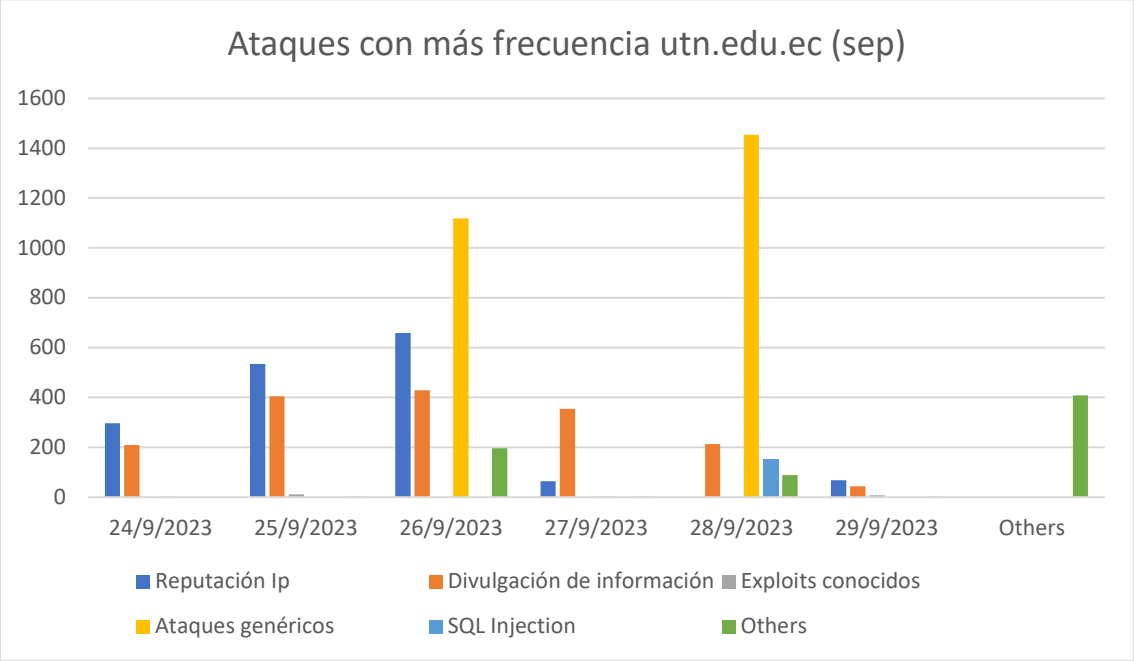


Figura 44. Reporte WAF- ataques más frecuentes periodo: 2023-09-24 hasta 2023-09-30
Fuente: Reporte WAF UTN

Análisis

Según el desglose de septiembre, podemos evidenciar que en su mayoría son ataques genéricos que supera los 14 mil eventos diarios, es decir que el WAF si detectó una actividad sospechosa o potencialmente maliciosa en el tráfico web, pero no ha identificado el tipo de ataque específico; seguido del ataque Reputación Ip que sobre pasa los 600 eventos diarios que se convierten en intentos maliciosos en la gestión de redes.

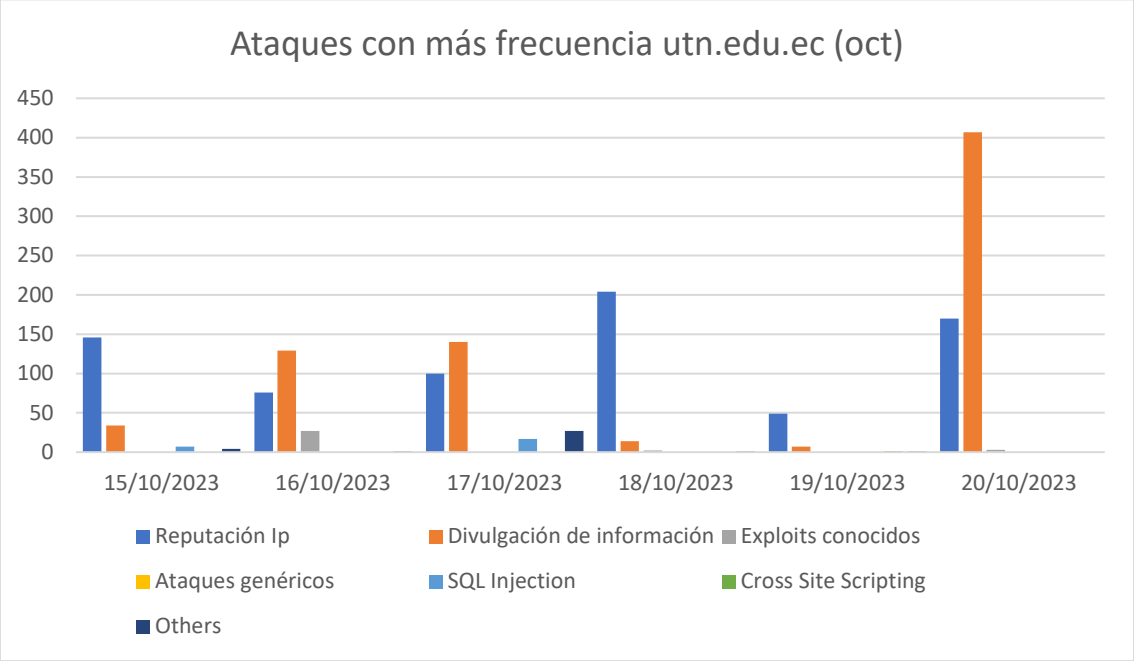


Figura 45. Ataques más frecuentes periodo octubre 15 al 20 de octubre 2023
Fuente: Reporte WAF UTN 2023

Análisis

Según el desglose de octubre, podemos evidenciar que en su mayoría son ataques de divulgación de información, son eventos en los que datos confidenciales o privados son expuestos o revelados sin autorización. Estos ataques pueden tener graves consecuencias para la seguridad.

Fuentes más frecuentes de ataques

Top Attack Sources		
Source	Events	Percent
190.107.236.163	326	18.40
180.254.70.33	311	17.55
190.107.236.172	177	9.99
190.107.236.176	164	9.26
186.159.16.90	96	5.42
220.250.48.131	38	2.14
Other(227)	660	37.25
Total(233)	**1772**	**100.00**

Figura 46. Direcciones Ip con más intentos de ataque
Fuente: Reporte WAF - UTN

Países de origen con más intentos de ataque

Top Triggered Source Countries		
Source Country	Events	Percent
Ecuador	671	37.87
Indonesia	312	17.61
United States	207	11.68
Colombia	96	5.42
Netherlands	81	4.57
Germany	81	4.57
Other(37)	324	18.28
Total(43)	**1772**	**100.00**

Figura 47. Países de origen con más intentos de ataque
Fuente: Reporte WAF - UTN

Host con más intentos de ataques

Top Attacked Http Host		
Http Host	Events	Percent
www.utn.edu.ec	817	46.11
estudiante.utn.edu.ec	385	21.73
colegio.utn.edu.ec	341	19.24
biblioteca.utn.edu.ec	72	4.06
estudiante.utn.edu.ec:443	61	3.44
posgrado.utn.edu.ec	47	2.65
Other(9)	49	2.77
Total(15)	**1772**	**100.00**

Figura 48. Host con más intentos de ataque.
Fuente: Reporte WAF -UTN

CONCLUSIONES Y RECOMENDACIONES

Se enfoca las principales conclusiones del estudio en función de los objetivos planteados y los resultados alcanzados, de la misma forma se menciona las recomendaciones.

CONCLUSIONES

- El dominio utn.edu.ec registra un impresionante flujo de tráfico mensual, superando las 180,000 sesiones mensuales. Esta cifra refleja la significativa presencia de usuarios que interactúan con el sitio web de la Universidad Técnica del Norte, dado el volumen sustancial de visitas mensuales, la institución reconoció la necesidad imperante de garantizar la seguridad de las aplicaciones web.

- Se caracterizó los principales tipos de ataque detectados por el WAF, donde se puede evidenciar que su gran mayoría son ataques genéricos, esto significa que el WAF ha detectado una actividad sospechosa o potencialmente maliciosa en el tráfico web, pero no ha identificado el tipo de ataque específico, también reconoció ataques de reputación de Ip, divulgación de información, SQL Injection, Cross-Site Scripting y exploits conocidos, estos datos pueden variar según filtros por mes, lo que significa que el WAF si inspecciona las solicitudes y respuestas HTTP, pero no reconoce las amenazas desconocidas es por eso que muestra como ataques genéricos.

- Es importante reconocer el Web Application Firewall (WAF) tiene sus limitaciones y según los resultados obtenidos no logra identificar todas las amenazas cibernéticas de manera exhaustiva, es decir que un WAF por sí solo no es suficiente, se debe complementar con otra solución de detección como un IDS (Intrusion Inspection System), que es un Sistema de Detección de Intrusiones.

- Como parte del proceso de evaluación del WAF se realizaron pruebas de seguridad con la herramienta OWASP ZAP, las mismas que se ejecutaron con ética y responsabilidad, clasificando las vulnerabilidades según su gravedad,

obteniendo como resultado un nivel medio – bajo - informativo de riesgo, lo que ayuda a los evaluadores de seguridad y desarrolladores a priorizar las correcciones.

- El reporte del WAF, se desglosa cada mes, con el número de eventos de ataques frecuentes identificadas como maliciosos, estos reportes son una herramienta crucial para el administrador web porque proporcionan información detallada sobre la seguridad y el rendimiento de una aplicación web. Ayuda a detectar amenazas, tomar decisiones informadas, cumplir con regulaciones y mejorar continuamente la seguridad y el rendimiento de la aplicación web.

RECOMENDACIONES

- Fortalecer el recurso humano en el área de seguridad informática, por lo menos contar con 2 profesionales, especializados tanto en SGSI, normas ISO, OWASP, NIST, para efectivizar un equipo de trabajo mancomunado en el bienestar y seguridad de la información en la Universidad Técnica del Norte.

- Es importante investigar y analizar los eventos de ataques genéricos para determinar si representan una amenaza real y si es necesario ajustar las reglas del WAF para una detección más específica ya que el WAF ha detectado una actividad sospechosa en el tráfico web, pero no ha clasificado el ataque y requiere una revisión adicional para determinar su naturaleza y gravedad.

- Al administrador web se recomienda realizar las correcciones o parches de seguridad que se evidencia en el escaneo de vulnerabilidades a fin de reducir el riesgo de ataque.

- Para una futura migración del servidor web de la Universidad Técnica del Norte, se recomienda reemplazar el servidor web de Apache por un servidor Nginx, mejorando su eficiencia en el manejo de una gran cantidad de conexiones simultáneas con un bajo uso de memoria. Esto hace que Nginx sea particularmente adecuado para sitios web de alto tráfico.

- Para un estudio posterior se podría implementar un IDS Sistema de Detección de Intrusiones que permita detectar ataques al servidor web y una vez detectado sea notificado al administrador del sistema mediante un Telegram bot.

- Para una futura investigación se recomienda considerar la optimización de sitios web para motores de búsqueda y realizar un estudio exhaustivo sobre las mejores prácticas de SEO y como la analítica web puede utilizarse para medir y mejorar la visibilidad y contribuya al campo de estudio en SEO y analítica web de la UTN.

REFERENCIAS BIBLIOGRÁFICAS

Agus, T., Osman, G., & Onno W, P. (2023). A real-time hypertext transfer protocol intrusion detection system on web server. *TELKOMNIKA Telecommunication Computing Electronics and Control, 21*(3), 566-573. https://doi.org/http://doi.org/10.12928/telkomnika.v21i3.24938

Akamai. (18 de Abril de 2023). *Akamai*. Akamai: https://www.akamai.com/es/blog/security/the-rise-of-application-and-api-attacks

Baca, G. (2016). Introducción a la seguridad informática. México: Grupo Editorial Patria.

Bagus, J. C. (4 de mayo de 2023). WordPress: A content management: https://www.theseus.fi/bitstream/handle/10024/802467/Bagus_John.pdf?sequence=5

Bonilla. (2018). http://bdigital.dgse.uaa.mx:8080/xmlui/bitstream/handle/11317/1519/428955.pdf?sequence=1&isAllowed=y

Caicedo, A. (2022). *Herramientas firewall basadas en tecnologías OpenSource.* Repositorio Digital.

Carlos Vega, O., Noblecilla, E. T., & Gonzaga, F. G. (2022). Análisis de factores de seguridad informática mediante la metodología OWASP v4.2: Caso de estudio ISTJOL. *Espíritu Emprendedor TES 2022, vol 6*(Nro 1), 70-88. https://doi.org/10.33970/eetes.v6.n1.2022.293

Celaya Luna, A. (2014). Posicionamiento web (SEO/SEM). En *Posicionamiento web (SEO/SEM)* (pág. https://elibro.net/es/ereader/utnorte/56047?page=8). Editorial ICB.

Cisco Networking Academy. (2022). *Cisco*. Cisco: https://www.cisco.com/

Cloudflare. (2022). *Protección WAF*. https://www.cloudflare.com/es-es/application-services/products/waf/

Culot, G., & Fabio, F. (2019). Addressing Industry 4.0 Cybersecurity Challenges. *IEEE ENGINEERING MANAGEMENT REVIEW, 47*(3), 79-86. https://doi.org/0000-0003-1130-8759

Cybersecurity Insiders. (Julio de 2023). *Cloud Security Report*. 2023 Cloud Security Report: https://resources.checkpoint.com/cyber-security-resources/2023-cloud-security-report

F5. (2023). *Aplicaciones web*. https://www.f5.com/es_es/glossary/web-application-firewall-waf

Fortinet. (2023). *Cortafuegos de aplicaciones web*. Fortinet: https://www.fortinet.com/products/web-application-firewall/fortiweb

Gangineni, J., & Tasmiya, M. (2023). Cloud Computing using OWASP: Open Web Application Security Project . *Proceedings of the 7th International Conference on Intelligent Computing and Control Systems (ICICCS-2023)*(https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10142457), 740 - 743.

García, J. (2015). *Creación de páginas web con Joomla*. https://riunet.upv.es/bitstream/handle/10251/67699/IPP-Garc%c3%ada%20-%20CREACI%c3%93N%20DE%20P%c3%81GINAS%20WEB%20CON%20CONTENIDO%20MULTIMEDIA%20UTILIZANDO%20JOOMLA%203.3..pdf?sequence=2&isAllowed=y

González, H. (2018). Capacidades de las metodologías de pruebas de penetración para. *Revista Cubana de Ciencias Informáticas, 12*, 52-65.

Guevara-Vega, C. P., Cárdenas-Hernández, W. A., Landeta, P. A., Rea-Peñafiel, X. M., & Quiña-Mera, J. A. (2022). Software Test Management to Improve Software Product Quality. *Applied Technologies*. https://doi.org/10.1007/978-3-031-03884-6_31

Guevara-Vega, C., Guzmán-Chamorro, E., Guevara-Vega, V., Andrade, A., & Quiña-Mera, J. (2019). Functional Requirement Management Automation and the Impact on Software Projects: Case Study in Ecuador. *Advances in Intelligent Systems and Computing*. https://doi.org/10.1007/978-3-030-11890-7_31

Herrero, L. (2022). *Hacking Ético, Curso de Especialización de Ciberseguridad en Entornos de las Tecnologías de la información.* Madrid: RA-MA.

Jahanavi, G., & Mubeen, T. (2023). Cloud Computing using OWASP: Open Web Application Security Project. *Proceedings of the 7th International Conference on Intelligent Computing and Control Systems (ICICCS-2023)*, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10142457.

Kinsta. (Noviembre de 2022). *Nginx vs Apache: Lucha entre Servidores Web*. https://kinsta.com/es/blog/nginx-vs-apache/

LOES. (2018). *LEY ORGANICA DE EDUCACION SUPERIOR, Registro Oficial Suplemento 298 de 12-oct.-2010.*

López. (2010). Seguridad informática. Editex S.A.

Marulanda, M., & Díaz, J. (2018). *APLICACIÓN DE LA METODOLOGÍA DE PRUEBAS OWASP.* OPEN WEB SECURITY PROJECT:

https://repository.unad.edu.co/bitstream/handle/10596/20479/1060648494.pdf?sequence=3&isAllowed=y

Napse. (30 de marzo de 2023). *Napse*. https://www.computerweekly.com/es/noticias/365534243/El-respaldo-es-clave-para-el-retail

Narváez, A., & Chaparro, F. (2022). Repositorio digital UNIVERSIDAD PILOTO DE COLOMBIA: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12064/Proyecto%20implementacion%20WAF%2008092022.pdf?sequence=5&isAllowed=y

ONU. (17 de mayo de 2023). *Los países menos desarrollados necesitan una mayor inversión digital*. Naciones Unidas: https://www.un.org/es/observances/telecommunication-day

OWASP. (2017). *Los diez riesgos de seguridad de aplicaciones web más críticos.* OWASP: https://owasp.org

OWASP. (2021). *Guía de pruebas de seguridad web de OWASP*. Contribuciones: https://owasp.org/www-project-web-security-testing-guide/

OWASP. (2021). *OWASP Mutillidae II*. Mutillidae II: https://owasp.org/www-project-mutillidae-ii/

OWASP. (2021). *The Ten Most Critical Web Application Security Risks.* OWASP Top Ten: https://owasp.org/www-project-top-ten/

Palacios, A. (2020). Seguridad informática (Edición 2020). Ediciones Paraninfo, S.A.

Palma Pérez, N. (2020). Eficiencia de los servidores web Apache 2 y Nginx. *Serie Científica de la Universidad de las Ciencias Informáticas, Vol. 13, Nº. 9, 2020*(13), págs. 97-112. Citar https://dialnet.unirioja.es/servlet/articulo?codigo=8590292

Pavón. (2019). Análisis de sistemas WAF.

PEPDI. (2019). *Gestión Académica.* Plan Estratégico Prospectivo de desarrollo institucional: https://transparencia.utn.edu.ec/

Picado, F., & Pérez, M. (2021). Administración de servicios web: Anatomía del internet. En F. Picado, & M. Pérez, *Administración de servicios web: Anatomía del internet.* Alfaomega Colombia S.A / Alpha Editorial.

PR Newswire. (2007). *LiteSpeed Technologies Releases High-Performance Apache Replacement Web Server*.

Quiña-Mera, A., Landeta, D. F., Rea-Peñafiel, X. M., & Guevara-Vega, C. (2021). Quality Evaluation of a Spring Cloud Microservices Architecture

Implementation. *Communication, Smart Technologies and Innovation for Society*. https://doi.org/10.1007/978-981-16-4126-8_66

Registrospublicos. (9 de 11 de 2021). *Ley de Protección de Datos Personales.* https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

Rodríguez, M. (2021). Wordpress. Obtenido de freidercreativo. wordpress. com/creatividad-y-pensamiento-creativo/elementosde-la-creatividad.

Sevillano, F. (2021). *Ciberseguridad Industrial.* Bogotá: RA-MA.

Villada Romero, J. (2016). Instalación y configuración del software de servidor web (UF1271). IC Editorial.

Yanney, E., Simpson, T., & Boadi1, K. S. (2023). Using Performance Metrics to Guide the Selection of a Website. *Information and Knowledge Management, 13*(1). https://www.researchgate.net/profile/Timothy-Simpson-8/publication/368328635_Using_Performance_Metrics_to_Guide_the_Selection_of_a_Website_Content_Management_System_-The_Case_of_Joomla_Drupal_and_WordPress/links/63e27526642523756393fd34/Using-Performance-

Yunapanta, E. (2022). *Estudio comparativo del rendimiento de los servidores web IIS y APACHE*. UNIVERSIDAD TÉCNICA DE BABAHOYO: http://dspace.utb.edu.ec/bitstream/handle/49000/14259/E-UTB-FAFI-SIST.INF-000148.pdf?sequence=1&isAllowed=y

Anexos

Anexo 1 Cuestionario al personal Nivel Operativo.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

Objetivo: Recopilar datos y opiniones de personal del Nivel Operativo de la Dirección de Desarrollo Tecnológico e Informático de la UTN para el proyecto de investigación: "WEB APPLICATION FIREWALL (WAF) COMO SOLUCIÓN DE SEGURIDAD MEDIANTE LA METODOLOGÍA OWASP PARA LA PROTECCIÓN DE APLICACIONES EN EL SERVIDOR WEB DE LA UNIVERSIDAD TÉCNICA DEL NORTE."

Consentimiento informado

- Acepta participar en la investigación descrita de forma libre y voluntaria. Su participación puede ser suspendida en cualquier momento, sin que esto traiga ningún tipo de consecuencias negativas para usted o a la institución. Este estudio no presenta riesgos identificables para su integridad física o psicológica.
- Los datos solicitados para la aplicación de este cuestionario son anónimos y serán manejados bajo absoluta confidencialidad. Estos datos estarán guardados en archivo electrónico, codificados con clave de acceso y custodiados por el Investigador Responsable.
- Ante cualquier duda, puede comunicarse con el responsable de esta investigación, Ing. Gabriela Elizabeth Cárdenas Rosero, mediante correo electrónico gecardenas@utn.edu.ec.

Lea detenidamente las preguntas y escoja la alternativa que usted considere conveniente.

Datos informativos

1. Género
   - ○ Masculino
   - ○ Femenino
   - ○ Otro

2. Nivel Operativo
   - ○ Laboratorista
   - ○ Desarrollo de software
   - ○ Gestión web
   - ○ Redes y Telecomunicaciones

CUESTIONARIO

1. ¿La alta dirección entiende participa y toma decisiones relacionadas con la seguridad de la información?

   - ○ Muy frecuente
   - ○ Frecuente
   - ○ Poco frecuente
   - ○ Nunca

2. ¿Se han asignado recursos, tanto financieros como humanos, para implementar y mantener medidas de seguridad informática efectivas?

- O Siempre
- O Casi siempre
- O A veces
- O Casi nunca
- O Nunca

3. ¿Está familiarizado con Open Web Application Security Project (OWASP) top 10?

- O Si
- O No

4. ¿Qué nivel de conocimiento tiene sobre las vulnerabilidades más comunes de Open Web Application Security Project (OWASP) top 10?

- O Excelente
- O Muy Bueno
- O Bueno
- O Regular
- O Deficiente

5. ¿Con que frecuencia ha utilizado un Sistema de Gestión de Contenido (CMS) de código abierto (por ejemplo, WordPress, Joomla, Drupal) ?

- O Muy frecuente
- O Frecuente
- O Poco frecuente
- O Nunca

6. ¿Cree usted que los Content Management System (CMS) presentan vulnerabilidades o fallos de seguridad?

- O Si
- O No

7. ¿Está de acuerdo que la metodología OWASP es importante para la seguridad de las aplicaciones web?

- O Totalmente de acuerdo
- O De acuerdo
- O Ni de acuerdo ni en desacuerdo
- O En desacuerdo

8. ¿Con qué frecuencia ha utilizado herramientas de pentesting para evaluar la seguridad de sistemas, redes y aplicaciones web?

- O Muy frecuente
- O Frecuente
- O Poco frecuente
- O Nunca

9. ¿Qué nivel de experiencia tiene con aplicaciones en la nube?

- O Excelente
- O Muy bueno
- O Bueno
- O Regular
- O Deficiente

10. ¿Cuáles amenazas de seguridad en la nube usted conoce?

- O Configuración incorrecta de la nube
- O Malware en la nube
- O Acceso no autorizado
- O Ataques de denegación de Servicio (DoS)
- O API inseguras
- O Otra

11. ¿Está de acuerdo en la implementación de una capa adicional de seguridad para proteger las aplicaciones web contra posibles amenazas y vulnerabilidades en el servidor web de la UTN?

- O Totalmente de acuerdo
- O De acuerdo
- O Ni de acuerdo ni en desacuerdo
- O En desacuerdo

12. ¿Recomendaría el uso de una aplicación de código abierto para realizar pruebas de pentesting en el servidor web de la UTN?

- O Muy frecuente
- O Frecuente
- O Poco frecuente
- O Nunca

13. ¿Está de acuerdo que se utilice la metodología OWASP para identificar y corregir vulnerabilidades en el servidor web de la UTN?

- O Totalmente de acuerdo
- O De acuerdo
- O Ni de acuerdo ni en desacuerdo
- O En desacuerdo

Anexo 2. VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN POR EXPERTOS EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
(CUESTIONARIO - ENCUESTA)

Proyecto:	Web Application Firewall (WAF) como solución de seguridad mediante la Metodología OWASP para la protección de aplicaciones en el servidor web de la Universidad Técnica Del Norte.
Autor:	Ing. Gabriela Elizabeth Cárdenas Rosero
Objetivo:	Evaluar la efectividad Web Application Firewall (WAF) como solución de seguridad mediante la metodología OWASP para detectar y bloquear los ataques en el servidor web de la UTN.

Fecha de envío para la evaluación del experto:	16 de agosto 2023
Fecha de revisión del experto:	22 de agosto 2023

En la siguiente matriz marque con una X el criterio de evaluación según corresponda en cada ítem. De ser necesario realice la observación en el apartado correspondiente.

INSTRUMENTO DE EVALUACIÓN CUALITATIVO			
ITEMS	**CRITERIOS DE EVALUACIÓN**		
	MUCHO	**POCO**	**NADA**
Instrucción breve, clara y completa.	X		
Formulación clara de cada pregunta.	X		
Comprensión de cada pregunta.	X		
Coherencia de las preguntas en relación con el objetivo.	X		
Relevancia del contenido	X		
Orden y secuencia de las preguntas	X		
Número de preguntas óptimo	X		

Observaciones:

Revisar documentación que estén relacionadas a pentesting en WSTG para aplicaciones Web y corregir vulnerabilidades y verificar el flujo de desarrollo seguro de programación de acuerdo con la metodología OWASP SAMM.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
(CUESTIONARIO - ENCUESTA)

A continuación, marque con una X en el criterio de evaluación según el análisis de cada pregunta que conforma el cuestionario, las cuales se encuentran representadas en el siguiente instrumento de evaluación como ítem. De ser necesario realice la observación en el casillero correspondiente.

INSTRUMENTO DE EVALUACIÓN CUANTITATIVO				
CRITERIOS DE EVALUACIÓN				OBSERVACIONES
Ítem	Dejar	Modificar	Eliminar	
1				
2				
3		X		Cambiar de metodología a vulnerabilidades más comunes.
4				
5				
6				
7		X		Verificar las amenazas
8				
9				
10				

RAMIRO FABRICIO PULGAR MONTERO

Ing. Ramiro Pulgar. Msc

C.C.: 0602525958

Apellidos y nombres completos	PULGAR MONTERO RAMIRO FABRICIO
Título académico	MAGISTER EN CIBERSEGURIDAD
Institución de Educación Superior	UNIVERSIDAD INTERNACIONAL DEL ECUADOR
Correo electrónico	ramiro.pulgar@bluehatcorp.com
Teléfono	0992751705

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
(CUESTIONARIO - ENCUESTA)

Proyecto:	Web Application Firewall (WAF) como solución de seguridad mediante la Metodología OWASP para la protección de aplicaciones en el servidor web de la Universidad Técnica Del Norte.
Autor:	Ing. Gabriela Elizabeth Cárdenas Rosero
Objetivo:	Evaluar la efectividad Web Application Firewall (WAF) como solución de seguridad mediante la metodología OWASP para detectar y bloquear los ataques en el servidor web de la UTN.

Fecha de envío para la evaluación del experto:	1 de septiembre 2023
Fecha de revisión del experto:	04-09-2023

En la siguiente matriz marque con una X el criterio de evaluación según corresponda en cada ítem. De ser necesario realice la observación en el apartado correspondiente.

INSTRUMENTO DE EVALUACIÓN CUALITATIVO			
ITEMS	**CRITERIOS DE EVALUACIÓN**		
	MUCHO	**POCO**	**NADA**
Instrucción breve, clara y completa.	X		
Formulación clara de cada pregunta.		X	
Comprensión de cada pregunta.		X	
Coherencia de las preguntas en relación con el objetivo.	X		
Relevancia del contenido	X		
Orden y secuencia de las preguntas		X	
Número de preguntas óptimo		X	

Observaciones:

Mejorar la formulación de preguntas, limitar seguridad sobre aplicaciones web

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
(CUESTIONARIO - ENCUESTA)

A continuación, marque con una X en el criterio de evaluación según el análisis de cada pregunta que conforma el cuestionario, las cuales se encuentran representadas en el siguiente instrumento de evaluación como ítem. De ser necesario realice la observación en el casillero correspondiente.

INSTRUMENTO DE EVALUACIÓN CUANTITATIVO				
CRITERIOS DE EVALUACIÓN				OBSERVACIONES
Ítem	Dejar	Modificar	Eliminar	
1		X		
2		X		
3	X			Anteceder una pregunta de conocimiento sobre OWASP
4	X			Anteceder una pregunta de conocimiento sobre CMS
5		X		
6		X		
7		X		Anteceder una pregunta de conocimiento sobre CLOUD
8	X			
9	X			
10		X		

0401200951
MARCO
REMIGIO PUSDA
CHULDE

Firmado digitalmente por 0401200951 MARCO REMIGIO PUSDA CHULDE
Fecha: 2023.09.04 11:00:01 -05'00'

Ing. Marco Pusdá. Msc

C.C.: 0401200951

Apellidos y nombres completos	PUSDA CHULDE MARCO REMIGIO
Título académico	Magister en Seguridad y Evaluación de Sistemas Tecnológicos
Institución de Educación Superior	Universidad Técnica del Norte
Correo electrónico	mrpusda@utn.edu.ec
Teléfono	0991486941