ANÁLISIS DE INDICADORES DE SEGURIDAD WEB Y SU IMPACTO EN EL POSICIONAMIENTO SEO EN MOTORES DE BÚSQUEDA

Ricardo Steven Ruiz Guerrero

Facultad de Ingeniería

Ingeniería en Sistemas

2025

Diego Fernando Loaiza Buitrago

Modalidad Diplomado

Universidad Santiago de Cali

Análisis de indicadores de seguridad web y su impacto en el posicionamiento SEO en motores de búsqueda

Analysis of web security indicators and their impact on SEO positioning in search engines

Ricardo Steven Ruiz Guerrero
Ricardo.ruiz00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de [Ingeniería en sistemas]

Resumen

En la actualidad existen diversos componentes que afectan el posicionamiento SEO de una página web en los motores de búsqueda, la mayoría de las empresas se enfocan en la experiencia de usuario, la usabilidad, el tiempo de carga u optimización de la página web, dejando de lado, la seguridad del aplicativo, desconociendo el alto impacto que tiene en el SEO. Este artículo explora los indicadores de ciberseguridad que tienen en cuenta los motores de búsqueda para el posicionamiento SEO de las aplicaciones web y el impacto negativo que se puede alcanzar si se descuidan estos indicadores.

Palabras Clave: Indicadores de ciberseguridad y SEO; Posicionamiento en buscadores y ciberseguridad; Impacto de la seguridad web en el SEO; Consideraciones de ciberseguridad para SEO; SEO y protección de aplicaciones web; Algoritmos de buscadores y ciberseguridad; Efectos de la seguridad web en el ranking de búsqueda; Factores de SEO y métricas de ciberseguridad; Amenazas cibernéticas y rendimiento SEO;

Abstract

Currently, there are various components that affect the SEO positioning of a webpage on search engines. Most companies focus on user experience, usability, webpage loading times, and optimization, neglecting the security of the application, unaware of its significant impact on SEO. This article explores the cybersecurity indicators considered by search engines for the SEO positioning of web applications and the negative impact that neglecting these indicators can have.

Keywords: Cybersecurity indicators and SEO; Search engine rankings and cybersecurity; Web security impact on SEO; Cybersecurity considerations for SEO; SEO and web application protection; Search engine algorithms and cybersecurity; Effects of web security on search ranking; SEO factors and cybersecurity metrics; Cyber threats and SEO performance; Web security and search engine optimization.

1. INTRODUCCIÓN

En el mundo digital en el que nos encontramos hoy en día, las aplicaciones web se han convertido en una herramienta indispensable para las empresas, gracias al potencial que brindan para poder llegar a cualquier parte del mundo, en esta necesidad de crecimiento ingresa un factor de posicionamiento de las marcas empresariales en internet especialmente en los motores de búsqueda, así mismo los motores de búsqueda tienen unos criterios de clasificación conocidos como SEO (search engine optimization). Los principios y estrategias básicas de SEO ayudan a los sitios web a mejorar su clasificación en los motores de búsqueda y aumentar la interacción del usuario. La optimización de motores de búsqueda tiene como objetivo ampliar la visibilidad de una empresa en los resultados de búsqueda orgánicos. Los motores de búsqueda tienen en cuenta elementos que incluyen etiquetas de título, palabras clave, etiquetas de imagen, estructura de enlaces internos y enlaces entrantes (también conocidos como vínculos de retroceso). Los motores de búsqueda también analizan la estructura y el diseño del sitio, el comportamiento de los visitantes y otros factores externos fuera del sitio para determinar qué tan alto debe estar su sitio en sus SERP (Search Engine Results) (Nicholson, 2019/2024), es decir página de resultados que nos muestra el motor de búsqueda, presentando dos tipos de contenido: resultados orgánicos y pagados. (Coppola, 2023)

Los esfuerzos de las empresas se enfocan en cubrir todos los aspectos antes mencionados, haciendo el mínimo

esfuerzo para salir lo más pronto al mercado y posicionarse rápidamente. Las empresas, en la mayoría de los casos olvidan un factor clave, la seguridad del sitio web; es indispensable contar con medidas de seguridad y criterios a tener en cuenta a la hora de monitorear el estado de los aplicativos web si se quiere garantizar una visibilidad completa en el mundo exterior, y es que no basta solo con tener un portal web con todas las características de usabilidad, portabilidad y eficiencia del desempeño, es muy importante la seguridad y la fiabilidad del aplicativo web.

Es muy común ver a las empresas enfocarse en las primeras características y dejar de lado la seguridad sus aplicativos webs ya que al realizar una prueba SEO, los criterios que este examen reflejan son el cumplimiento de protocolos SSL, arquitectura del código, usabilidad de la página y criterios basados en la experiencia de usuario. (Tsuei, 2018) La existencia de un certificado SSL en un sitio web es uno de los principales factores que contribuyen a mejorar la clasificación en los motores de búsqueda. (Ziakis, 2019)

La tranquilidad de contar con un protocolo https, puede hacer que más temas de seguridad sean descuidados, independientemente de la certificación HTTPS, las investigaciones muestran que la mayoría de los sitios web experimentaron un promedio de 58 ataques por día. Es más, hasta el 61% de todo el tráfico de Internet está automatizado, lo que significa que estos ataques no discriminan según el tamaño o la popularidad del sitio web en cuestión. (Chalk, 2019)

Como se mencionaba anteriormente, el impacto que tiene en el posicionamiento SEO no es tomado en cuenta por las empresas. Por ejemplo, uno de los motores de búsqueda más conocidos (Google) utiliza la seguridad web como un factor clave de clasificación. Si el sitio web no es seguro, es posible que Google lo penalice en sus resultados de búsqueda. Esto significa que el sitio web aparecerá más bajo en los resultados de búsqueda, lo que puede resultar en una pérdida de tráfico y clientes potenciales (Lahey, 2023)

Existen estudios que han evaluado indicadores para medir la seguridad de una página web enfocados en el posicionamiento SEO, estos describen que los indicadores pueden variar mucho del contexto del aplicativo y las necesidades de esta, pero generalmente coinciden en los parámetros definidos en la sección.

Este artículo tiene como objetivo identificar los indicadores de seguridad web que afectan el posicionamiento SEO, detallando cuáles son los ataques que influyen directamente en el posicionamiento y sus posibles medidas de prevención, minimizando así el riesgo de penalizaciones y optimizando el posicionamiento en los motores de búsqueda.

1.1 Indicadores de ciberseguridad para aplicaciones web

1.1.1 Número total de incidentes de ciberseguridad reportados

Este es el indicador básico del estado general de la ciberseguridad durante un período determinado. Para mantener los valores directamente comparables entre períodos, es posible que deba dividirlos por un factor variable, por ejemplo, proporcionando el número total de incidentes por aplicación o instalación. (Banach, 2020)

1.1.2 Vulnerabilidades recurrentes

La cantidad de vulnerabilidades recurrentes es una medida muy importante de la eficiencia del proceso de remediación, así como de la calidad de la educación de los desarrolladores. Si se redescubre la misma vulnerabilidad en el mismo activo web durante varios análisis de vulnerabilidad consecutivos, significa que no se está solucionando. (Sundar, 2017)

Se dice que si una vulnerabilidad es recurrente es por problemas en los recursos para solucionarlos o el recurso de personal poco calificado para llevar a cabo esta tarea, es importante estar monitoreando constantemente las aplicaciones web para estar al tanto de las ocurrencias ya que en la mayoría de los casos los usuarios nunca se dan cuenta de que sus páginas han sido víctimas de un ataque.

1.1.3 Cambios en la cantidad de incidentes de ciberseguridad reportados

Expresada como porcentaje, esta métrica brinda una descripción general rápida de la evolución de las ciber amenazas en dimensiones específicas. Puede utilizar esto para comparar períodos, unidades de negocio o aplicaciones y, nuevamente, puede agregar una clasificación de gravedad para proporcionar inteligencia adicional. (Banach, 2020)

1.1.4 Tiempo promedio para remediar

Otra métrica importante (nuevamente, útil para subdividirla en diferentes clases de gravedad) es el tiempo que normalmente se requiere para solucionar la vulnerabilidad. Estos datos de tiempo de respuesta se pueden adquirir directamente desde el escáner (tiempo entre el primer descubrimiento de la vulnerabilidad y la última aparición de esta vulnerabilidad) o desde una herramienta de gestión de vulnerabilidades/seguimiento de problemas. (Nidecki, 2021)

1.2 Relevancia del Posicionamiento SEO

Como se puede observar los indicadores recomendados por los estudios se centran en la cantidad de ataques, la recurrencia y la varianza de estos y que tiempo de respuesta que tiene el aplicativo frente a una vulnerabilidad explotada, estos indicadores se ven muy relación a los indicadores que tienen los motores de búsqueda para el posicionamiento SEO, debido a que si el aplicativo cuenta con un ataque sin resolver, inmediatamente se ve penalizado, estas penalizaciones varían dependiente del ataque que sufre el portal web y van desde un aviso al usuario advirtiendo que la pagina no es segura, una baja indexación, penalizaciones monetarias, hasta el bloqueo de la página. (google, 2024)

1.2.1 Lista negra

Los motores de búsqueda generan la mayor parte del tráfico de un sitio web, con el tiempo los propietarios de los aplicativos buscan perfeccionar su SEO, llegar a la lista negra de un motor de búsqueda o un antivirus puede ser muy severo para cualquier propietario de un aplicativo web. Para entender esto se debe conocer cómo trabajan los motores de búsqueda y es que cuando un usuario ingresa una consulta, Google busca en su propia base de datos, denominada índice, los resultados más adecuados para la consulta.

La Lista negra de Google (o, como algunos la llaman, la "lista de bloqueo") es un tipo de base de datos de sitios web completamente diferente que mantiene Google. Esta base de datos se compone de todos los sitios web que Google, otros motores de búsqueda e incluso las empresas de antivirus consideran inseguros para el público en general. Debido al gran volumen de sitios web que llenan Internet, sería imposible para Google compilar un índice de sitios inseguros con un proceso manual. En cambio, emplea rastreadores, bots y otras herramientas patentadas que exploran sitios web de forma independiente y agregan los peligrosos al índice de la lista negra. (SolidWP Editorial Team, 2021)

Con la gran cantidad de ataques cibernéticos y maliciosos que ocurren hoy en día, no sorprende que Google haya incluido en la lista negra (etiquetado como inseguros) alrededor de 10,000 sitios web todos los días. Una de las razones más comunes por las que un sitio web termina en la lista negra de Google es cuando es pirateado y está lleno de malware, spam y spyware. Si bien es posible que el propietario del sitio web no haya sido responsable del hackeo, lo más seguro es que será considerado responsable cuando su sitio se agregue a la lista negra de Google. (SolidWP Editorial Team, 2021)

Esto es especialmente alarmante teniendo en cuenta que el 9 por ciento, o hasta 1,7 millones de sitios web, tienen una vulnerabilidad importante que podría permitir la implementación de malware. Si está invertido en su visibilidad de búsqueda a largo plazo, opera en un mercado altamente competitivo o depende en gran medida del tráfico orgánico,

entonces la vigilancia para evitar un compromiso es crucial. (Bharathi, 2020)

1.2.2 Errores de rastreo

El término "Crawling errors" se refiere a los errores que surgen durante el proceso de rastreo que realizan los motores de búsqueda, como Googlebot, para indexar y entender el contenido de un sitio web.

Cuando los bots están rastreando un sitio web, pueden encontrar diversos problemas o errores que afectan la forma en que se muestra el sitio en los resultados de búsqueda o cómo es interpretado por los motores de búsqueda. Estos errores pueden ser causados por diversas razones, como problemas técnicos en el sitio, configuraciones incorrectas, o incluso intentos de acceso malicioso por parte de bots con intenciones dañinas, como el scraping de contenido o el robo de datos. Los errores de rastreo pueden incluir situaciones en las que un sitio web devuelve códigos de error como el 404 (página no encontrada) o 503 (servicio no disponible) para páginas que realmente existen y deberían ser accesibles. (Chalk, 2019)

1.2.3 Spam SEO

Más del 73% de los sitios pirateados en un estudio realizado por GoDaddy fueron atacados estrictamente con fines de spam, esto podría ser un acto de sabotaje deliberado o un intento indiscriminado de raspar, desfigurar o sacar provecho de un sitio web autorizado. (Chalk, 2019)

Generalmente, los actores maliciosos cargan sitios con spam para desalentar las visitas legítimas, los convierten en granjas de enlaces y atraen a los visitantes desprevenidos con malware o enlaces de phishing. Al obtener acceso a sitios web legítimos, los malos actores crean un camino hacia sus propiedades web fraudulentas. En lugar de clasificarse como lo hacen la mayoría de los sitios web legítimos, los malos actores se aprovechan de la credibilidad de un sitio normal a los ojos de los motores de búsqueda. (MacLeod, 2023)

1.3 Amenazas en sitios web

1.3.1 Inyección de código SQL

La inyección SQL es una de las vulnerabilidades más devastadoras que afectan a una empresa, ya que puede exponer toda la información confidencial almacenada en la base de datos de una aplicación, incluida información útil como nombres de usuario, contraseñas, nombres, direcciones, números de teléfono, y datos de la tarjeta de crédito. Entonces, ¿Qué es exactamente la inyección SQL? Es la técnica de inyección de lenguaje de consulta estructurado (SQL, structured query language) la cual consiste en utilizar este tipo de lenguaje para realizar consultas concatenadas a los servidores de bases de datos del CSP. Los atacantes pueden explotar estas vulnerabilidades para inyectar scripts (programas simples o secuencias de comandos que interactúan con el sistema operativo) maliciosos de modo que puedan obtener el acceso no autorizado a las bases de datos. (Gayoso Martinez, Arroyo Guardeño, & Hernandez Encinas, 2020)

1.3.2 Ataques de denegación de servicio (DoS) y distribuidos (DDoS)

Un ataque de denegación de servicio (DoS) es un tipo de ciberataque en el que un actor malintencionado pretende hacer que una computadora u otro dispositivo no esté disponible para los usuarios previstos interrumpiendo el funcionamiento normal del dispositivo. Los ataques DoS normalmente funcionan inundando una máquina objetivo con solicitudes hasta que el tráfico normal no puede procesarse, lo que resulta en denegación de servicio a usuarios adicionales. La diferencia distintiva entre DDoS y DoS es la cantidad de conexiones utilizadas en el ataque. (Cloudflare, 2024)

1.3.3 Manipulación de sesión

El ataque Session Hijacking consiste en la explotación del mecanismo de control de sesión web, que normalmente se gestiona mediante un token de sesión.

Debido a que la comunicación http utiliza muchas conexiones TCP diferentes, el servidor web necesita un método para reconocer las conexiones de cada usuario. El método más útil depende de un token que el servidor web envía al navegador del cliente después de una autenticación exitosa del cliente. Un token de sesión normalmente se compone de una cadena de ancho variable y podría usarse de diferentes maneras, como en la URL, en el encabezado de la solicitud http como una cookie, en otras partes del encabezado de la solicitud http, o incluso en el cuerpo de la solicitud http. (OWASP, 2024)

1.3.4 Cross-Site Scripting (XSS)

Los ataques de secuencias de comandos entre sitios (XSS) son un tipo de inyección en el que se inyectan secuencias de comandos maliciosas en sitios web que de otro modo serían benignos y confiables. Los ataques XSS ocurren cuando un atacante utiliza una aplicación web para enviar código malicioso, generalmente en forma de script del lado del navegador, a un usuario final diferente. Las fallas que permiten que estos ataques tengan éxito están bastante extendidas y ocurren en cualquier lugar donde una aplicación web utiliza información de un usuario dentro de la salida que genera sin validarla ni codificarla. (KirstenS, Cross Site Scripting (XSS), 2022)

1.3.5 Cross-Site Request Forgery (CSRF)

La falsificación de solicitudes entre sitios (CSRF) es un ataque que obliga a un usuario final a ejecutar acciones no deseadas en una aplicación web en la que está actualmente autenticado. Con un poco de ayuda de ingeniería social (como enviar un enlace por correo electrónico o chat), un atacante puede engañar a los usuarios de una aplicación web para que ejecuten acciones de su elección (KirstenS, Cross Site Request Forgery (CSRF), 2024)

1.4 Métodos de prevención

La seguridad es algo crucial para asegurar el éxito de la organización en sus portales web, actualmente las pruebas de seguridad son esenciales para las aplicaciones web y a la hora de desarrollar estas pruebas es mejor contar con guías de pruebas de seguridad conocidas y una de ellas es la guía de OWASP (Open Web Application Security Project).

1.4.1 Listas de testeo

Todas las herramientas y documentos de OWASP están abiertos a cualquier persona interesada en desarrollar aplicaciones seguras. La lista OWASP Top 10, así como miles de otras vulnerabilidades conocidas, se pueden detectar automáticamente con herramientas de prueba de seguridad de aplicaciones web o manualmente por expertos en seguridad. La guía de desarrollo le mostrará a su proyecto cómo diseñar y crear una aplicación segura, la guía de revisión de código le indicará cómo verificar la seguridad del código fuente de su aplicación y la guía de pruebas le mostrará cómo verificar la seguridad de su aplicación en ejecución. (Aydos, Aldan, Coşkun, & Soydan , 2022)

1.4.2 Pruebas caja blanca y caja negra

Las pruebas de caja negra y caja blanca se utilizan principalmente en el desarrollo de herramientas de prueba de seguridad para encontrar la mayoría de las vulnerabilidades y fallas de seguridad en las aplicaciones web. En las pruebas de caja negra, los casos de prueba se entregan al software y los resultados se verifican para predecir las vulnerabilidades o errores, mientras que se realizan pruebas de caja blanca para examinar el código defectuoso o vulnerable.

Muchas compañías para mantenerse en el comercio realizan estas pruebas para mantener su SEO positivo, Sin embargo, incluso las aplicaciones planificadas de sitios web estarán sujetas a errores o éxitos. Por lo tanto, una aplicación debe pasar por una prueba de software. Las pruebas de prueba que se llevarán a cabo, incluyendo Caja Blanca y Caja Negra, pueden concluir que la aplicación de comercio electrónico Shoopers basada en el sitio web se declara exitosa porque puede brindar conveniencia al administrador en cuanto a la expansión del mercado comercial. (Gustinov , 2023)

1.4.3 Monitoreo del sistema e identificación de hacks

Estar constantemente revisando el tráfico de la página ayuda a identificar el tráfico de bots ya sean malignos o de ayuda del motor de búsqueda y el tráfico de los clientes, es importante detectar cualquier anomalía rápidamente para poder reaccionar a tiempo impidiendo que la página sea incluida en una lista negra o víctima de otra penalización

Los hallazgos indican que el 70% de las infracciones afectan a numerosas organizaciones, incluida la industria de la salud. El análisis muestra la probabilidad de una violación de datos. Debido al mayor uso de aplicaciones informáticas, la seguridad del host y la red genera riesgo de violaciones de datos. Se pueden utilizar métodos de aprendizaje automático para encontrar estos ataques. Según la investigación, se utilizan modelos de aprendizaje automático para proteger el sitio web de fallas de seguridad. El conjunto de datos se puede obtener en Privacy Rights Clearinghouse. Las violaciones de datos se pueden reducir educando al personal sobre el uso de medidas de seguridad modernas. Esto puede ayudar a comprender el conocimiento de los ataques y la seguridad de los datos. Los modelos de aprendizaje automático como Random Forest, Decision Tree, k-means y Multi-layer Perceptron se utilizan para predecir las violaciones de datos. (K. Pujitha, G. Nandini, K. V. T. Sree, B. Nandini, & D. Radhika, 2023)

1.4.4 Complementos y extensiones

Mantener los plugin y componentes de la página web actualizados es crucial para reducir las vulnerabilidades debido que los atacantes buscan sitios elaborados con componentes como WordPress, debido a que presentan fallos más comunes que pueden ser explotados, es importante actualizar todos los componentes que usa la página para poder mitigar el daño, aunque no siempre puede ser beneficioso Si bien las actualizaciones de software son el método más recomendado para corregir errores y deficiencias relacionadas con el software, no siempre brindan una solución. Durante las actualizaciones de software, los errores y vulnerabilidades no se eliminan; en algunos casos, las nuevas actualizaciones causan nuevos problemas. (Ö. Aslan, Ö. Aslan, M. Ozkan-Okay, A. A. Yilmaz, & E. Akin, 2023)

Gráficos

basados en la información recopilada por owasp y su top diez de las amenazas más recurrentes que puede tener un sitio web, analizamos cada amenaza y la relacionamos con el impacto que pueden tener el posicionamiento seo, y al sitio web como tal.

Tabla 1. Amenazas y su impacto SEO

Amenaza OWASP 2021	Descripción	Impacto en SEO	Consecuencias para el Sitio Web
A01 - Control de Acceso Roto	Fallas que permiten a usuarios acceder a funciones o datos sin autorización	Crítico	Inclusión en lista negra
			Pérdida de datos sensibles
			Penalización inmediata en rankings
			Advertencias de seguridad a usuarios
A02 - Fallas Criptográficas	Fallos en la protección de datos sensibles, incluyendo problemas con HTTPS	Muy Alto	Advertencias de "No seguro" en navegadores
			Pérdida de confianza de usuarios
			Reducción en rankings por falta de HTTPS
			Menor tasa de conversión
A03 - Inyección	Incluye SQL, NoSQL, comandos OS y LDAP	Alto	Blacklisting por motores de búsqueda
			Inserción de spam SEO
			Pérdida de control sobre el contenido
			Posible eliminación del índice
A04 - Diseño Inseguro	Fallos en la arquitectura de seguridad desde el diseño	Medio-Alto	Errores de rastreo
			Problemas de rendimiento
			Impacto en Core Web Vitals
			Reducción gradual en rankings
A05 - Configuración Incorrecta de Seguridad	Configuraciones por defecto o incompletas de seguridad	Alto	Exposición de información sensible
			Errores en el rastreo
			Problemas de indexación

			Vulnerabilidad a ataques automatizados
A06 - Componentes Vulnerables y Desactualizados	Uso de componentes, librerías o software desactualizados	Medio-Alto	Vulnerabilidad a exploits conocidos
			Problemas de rendimiento
			Impacto en velocidad de carga
			Posibles penalizaciones por software malicioso
A07 - Fallas de Identificación y Autenticación	Problemas en la confirmación de identidad del usuario	Alto	Suplantación de identidad
			Spam en comentarios / contenido
			Manipulación de datos
			Pérdida de autoridad del dominio
A08 - Fallas en Integridad de Software y Datos	Infraestructura y actualizaciones sin verificación	Medio	Contenido manipulado
			Enlaces spam inyectados
			Redirecciones maliciosas
			Pérdida de confianza en SERP
A09 - Fallas en Registro y Monitoreo	Detección insuficiente de brechas de seguridad	Medio-Alto	Detección tardía de ataques
			Tiempo de respuesta lento ante incidentes
			Acumulación de penalizaciones
			Dificultad en recuperación SEO
A10 - Server-Side Request Forgery (SSRF)	Ataques que explotan la confianza en solicitudes del servidor	Alto	Acceso no autorizado a datos
			Exposición de API internas

			Problemas de rendimiento del servidor
			Caída del sitio y pérdida de ranking

Fuente: Adaptado de (OWASPFoundation, 2019/2023)

2. CONCLUSIONES

Con el fin de mantener un buen posicionamiento SEO es importante la experiencia de usuario, diseño de interfaz, velocidad del sitio, estructuración del HTML, entre otros. Sin embargo, todo el esfuerzo realizado en conservar las métricas comúnmente establecidas para el SEO de una página será en vano si no se implementa la seguridad adecuada para proteger la integridad de los usuarios.

Para un buen posicionamiento en los motores de búsqueda, el protocolo SSL es solo un requisito mínimo para garantizar la seguridad de una página web, es importante estar constantemente monitoreando el tráfico de la página, ya que los motores de búsqueda tardan un tiempo en encontrar si una aplicación web ha sido vulnerada o es propensa a un ataque, esto puede generar una ventana en la cual los propietarios pueden resolver los problemas de seguridad y evitar futuros inconvenientes, tales como: sanciones por parte del motor de búsqueda, clasificando la página web en una lista negra y en los peores casos, la eliminación del sitio.

Es imposible asegurar que una aplicación web esté libre de amenazas o de sufrir un ataque, sin embargo se pueden tomar medidas para mitigar los posibles daños, siempre y cuando se reaccione de manera correcta y en el tiempo adecuado para esto es importante el uso de herramientas para monitorear el tráfico y detectar los posibles ataques como por ejemplo: el uso de la inteligencia artificial para facilitar el aprendizaje de nuevas amenazas realizando pruebas de seguridad periódicas, realizar pruebas de caja negra, caja blanca y listas de chequeo para garantizar la seguridad de la página web. La prevención y monitoreo constante son esenciales para mantener un buen posicionamiento SEO.

Las consecuencias que pueden surgir de una vulnerabilidad están muy relacionadas a las implementaciones de respuesta y el tiempo con el cual son aplicadas, ya que la totalidad de vulnerabilidades pueden resultar en penalizaciones si no se resuelven a tiempo

Mantener el éxito y la expansión de un mercado electrónico es el balance entre conceptos de experiencia de usuario y seguridad del usuario.

3. REFERENCIAS

K. Pujitha, G. Nandini, K. V. T. Sree, B. Nandini, & D. Radhika. (2023). Cyber Hacking Breaches Prediction and Detection Using Machine Learning. *2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN)*.

Aydos, M., Aldan, Ç., Coşkun, E., & Soydan , A. (2022). Security testing of web applications: A systematic mapping of the literature. *Journal of King Saud University - Computer and Information Sciences, 34*(9), 6775-6792.

Banach, Z. (06 de 03 de 2020). *How to Define Cybersecurity Metrics for Web Applications*. Recuperado el 03 de 12 de 2023, de https://www.invicti.com/blog/web-security/define-cybersecurity-metrics-web-applications/

Bharathi, A. (01 de 04 de 2020). *COMPLEXITIES IN ENSURING CYBER SECURITY TO AVOID SEO INFRINGEMENTS.* Recuperado el 03 de 12 de 2023, de https://lawbhoomi.com/wp-content/uploads/2020/10/61484-414130_64325d1e72b34f70b3312563c48f7b70-1.pdf

Chalk, W. (06 de 02 de 2019). *Cybersecurity in SEO: How website security affects SEO performance*. (Search Engine Watch) Recuperado el 03 de 12 de 2023, de https://www.searchenginewatch.com/2019/02/07/how-website-security-affects-seo/

Clarke-Salt, J. (2009). *SQL Injection Attacks and Defense.* Syngress.

Cloudflare. (2024). *What is a denial-of-service (DoS) attack?* (Cloudflare) Recuperado el 04 de 12 de 2023, de https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

Coppola, M. (19 de 01 de 2023). *SERP: lo que debes saber sobre las páginas de resultados de Google*. (HubSpot) Recuperado el 04 de 12 de 2023, de https://blog.hubspot.es/marketing/serp

Dye, K. (2008). Website abuse for search engine optimisation. *Network Security*, 4-6.

Gayoso Martinez, V., Arroyo Guardeño, D., & Hernandez Encinas, L. (2020). *Ciberseguridad.* España: Los Libros de La Catarata.

google. (2024). *Informe de problemas de seguridad - Ayuda de Search Console*. (google) Recuperado el 03 de 12 de 2023, de https://support.google.com/webmasters/answer/9044101

Gustinov , M. (2023). Analysis of Web-Based E-Commerce Testing Using Black Box and White Box Methods. *International Journal of Information System and Innovation Management (IJISIM), 1*(1).

KirstenS. (s.f.). *Cross Site Request Forgery (CSRF)*. (OWASP) Recuperado el 04 de 12 de 2023

KirstenS. (s.f.). *Cross Site Scripting (XSS)*. (OWASP) Recuperado el 04 de 12 de 2023, de https://owasp.org/www-community/attacks/xss/

Lahey, C. (27 de 12 de 2023). *SEO Basics: How to Do SEO for Beginners*. Obtenido de Semrush: https://www.semrush.com/blog/seo-basics/

Lemos, J. Y. (2017). Search engine optimization to enhance user interaction. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. Palladam.

Nicholson, R. (s.f.). *The Ultimate Guide to SEO in 2024*. (HubSpot) Recuperado el 4 de 12 de 2023, de https://blog.hubspot.com/marketing/seo

Nidecki, T. A. (15 de 07 de 2021). *Cybersecurity metrics for web applications*. (Acunetix) Recuperado el 03 de 12 de 2023, de https://www.acunetix.com/blog/web-security-zone/cybersecurity-metrics-for-web-applications/

Ö. Aslan, Ö. Aslan, M. Ozkan-Okay, A. A. Yilmaz, & E. Akin. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics, 12*(6).

OWASP. (2024). *Session hijacking attack*. (fundacíon OWASP) Recuperado el 04 de 12 de 2023, de https://owasp.org/www-community/attacks/Session_hijacking_attack

SolidWP Editorial Team. (24 de 08 de 2021). *What is Google Blacklist? 6 Important Things to Know*. (SolidWP) Recuperado el 03 de 12 de 2023, de https://solidwp.com/blog/what-is-google-blacklist-6-important-things-to-know/

Sundar, V. (18 de 10 de 2017). *indusface*. Recuperado el 03 de 12 de 2023, de https://www.indusface.com/blog/web-application-security-metrics/

Tsuei, H.-J. W.-H.-T.-H. (2018). Improving search engine optimization (SEO) by using hybrid modified MCDM models. *Artificial Intelligence Review, 53*, 1-16.

Ziakis, C. a. (2019). Important Factors for Improving Google Search Rank. *Future Internet, 11*(2), 32.