Monitorización de las Páginas Web de los Institutos de la Comunidad de Madrid



Imagen que contiene Forma

Descripción generada automáticamente Imagen que contiene Texto

El contenido generado por IA puede ser incorrecto.

**Índice**

[1. Introducción 1](#_Toc191149721)

[2. Hipótesis y objetivos del proyecto 2](#_Toc191149722)

[2.1 Hipótesis 2](#_Toc191149723)

[2.2 Objetivos del proyecto 2](#_Toc191149724)

[3. Ciberataques 2](#_Toc191149725)

[3.1. Tipos de ciberataques 2](#_Toc191149726)

[3.1.1. Ataque de inyección SQL 3](#_Toc191149727)

[3.1.2. Ataque de Cross-Side Scripting 4](#_Toc191149728)

[3.1.3. Ataque de fuerza bruta 4](#_Toc191149729)

[3.1.4. Ataque de denegación de servicio (DDoS y DoS) 5](#_Toc191149730)

[4. Google Lighthouse 5](#_Toc191149731)

[4.1. Qué es Google Lighthouse 6](#_Toc191149732)

[4.1.1. Cómo funciona Google Lighthouse 6](#_Toc191149733)

[4.2. Performance 7](#_Toc191149734)

[4.2.1. Largest Contentful Paint (LCP) 7](#_Toc191149735)

[4.2.2. First Contentful Paint 7](#_Toc191149736)

[4.2.3. Time To Interactive (TTI) 7](#_Toc191149737)

[4.2.4. Total Blocking Time (TBT) 7](#_Toc191149738)

[4.2.5. Cumulative Layout Shift (CLS) 8](#_Toc191149739)

[4.2.6. Speed Index 8](#_Toc191149740)

[4.3. Accessibility 8](#_Toc191149741)

[4.4. Best Practices 8](#_Toc191149742)

[4.5. Search Engine Optimizitation (SEO) 9](#_Toc191149743)

[5. Test NTP 9](#_Toc191149744)

[6. Código 9](#_Toc191149745)

[7. Resultados y conclusiones 9](#_Toc191149746)

[7.1 Resultados 9](#_Toc191149747)

[7.2 Conclusiones 9](#_Toc191149748)

[8. Bibliografía y fuentes consultadas 9](#_Toc191149749)

**Plan de trabajo**

Se medirá el grado de ciberseguridad de los sitios web en “estatus de ciberseguridad”. Este estatus de seguridad será medido de forma indirecta, puesto que medir el grado de ciberseguridad de las páginas web mediante formas directas implicaría lanzar un ciberataque y medir si se está protegido ante ese ataque. Además, los medios directos son descartados porque serían considerados un ciberdelito.

Para obtener el estatus de ciberseguridad de las páginas web de los institutos de forma indirecta, se recurrirá a varias métricas. Estas métricas no miden directamente cuántas vulnerabilidades presenta un sitio web, pero permiten estimarlo. Si un sitio web muestra signos de estar mal programado u optimizado, es intuitivo pensar que el sitio web será vulnerable ante ciberataques. Sin embargo, cuando un sitio web presenta una buena optimización, buen diseño, …, etcétera, entonces es muy probable que este sitio web tenga mucha más protección que el del anterior ejemplo.

Para empezar, se comparará la hora del servidor de la página web con la hora oficial de España. Esta métrica es una más de las que no aportan información sobre el grado de ciberseguridad, pero que resulta muy útil ya que permite saber si el sitio web está siendo mantenido a menudo. Las páginas web que no presenten mantenimiento serán fácilmente detectadas por este protocolo, al desvincularse cada vez más y más con la hora oficial, sin ser puestas en hora de nuevo. A esta métrica se le da el nombre de “Test NTP”.

Después del Test NTP, es importante saber el grado de optimización y buen diseño de una página web, para estimar el grado de ciberseguridad. Es por eso por lo que se usará Google Lighthouse. Lighthouse ofrece mucha información sobre un sitio web, y además permite aislar sus medidas, lo que garantiza la libertad de asignar un distinto peso a cada métrica. Asimismo, esta herramienta tiene a su vez métricas que sí que otorgan cierto grado de ciberseguridad, como Best Practices.

Por último, se verificará si las páginas web presentan un certificado digital o certificado SSL. El certificado SSL es importante no solo para la página web sino también para el usuario, ya que asegura que la la información que se intercambia entre el usuario y la página web está cifrada y ningún tercero puede acceder a ella.

Para poder llevar a cabo el experimento de este proyecto, se necesita primero recolectar todas las URLs de ambas las páginas web oficiales y las aulas virtuales de todos los institutos de educación secundaria de toda la Comunidad de Madrid. Una vez hecho esto, entonces se escribirá varios programas en Python, en los que se realice escaneos diarios. Así, al cabo de cierto tiempo, se computará una media por cada medida de cada instituto. Con la media de cada medida de los institutos, se la dará un peso a cada media, determinando finalmente el estatus de ciberseguridad de cada instituto. Como el objetivo de este proyecto es conseguir una media de ciberseguridad generalizada, entonces primero se realizará una media de ciberseguridad de todos los institutos y luego se comparará cada media individual de un instituto a la media de todos los institutos. Si la media individual de un instituto es más baja que la media general, entonces se recomendará al instituto que tome las prácticas web de otros institutos cuyas medias sean más altas de lo normal. Si la situación es al revés, entonces se recomendará al instituto con la media más alta a que haga sus prácticas públicas a otros institutos con la media baja.

# 1. Introducción

Actualmente, estamos viviendo el florecimiento de la cuarta revolución industrial. Con el auge de Internet, no hay necesidad de gastar recursos en hacer llegar información a los demás, se puede crear una página web y así el mensaje que se quiera comunicar llegará más lejos que nunca, porque es accesible en casi todo el mundo.

Una de las grandes ventajas de Internet es la versatilidad que ofrece. Permite acceso instantáneo a información, conecta personas globalmente y ofrece múltiples plataformas para trabajar, educarse y socializar. También obsequia al usuario con más de un billón de páginas web (Internet Live Stats), que son vitales para el desarrollo de los negocios actualmente.

Pero, como todo, el Internet presenta desventajas. Dentro de Internet, nada es totalmente seguro. El usuario deberá ejercer su propio juicio para elegir de qué sitios web fiarse y de cuáles no, ya que siempre ha existido el intento de fraude entre los humanos. Algo similar ocurre con las páginas web. Gracias a que las ya presentadas páginas web están dentro de Internet, quedan expuestas inmediatamente ante ciberdelincuentes y hackers, que lanzan ciberataques en los que se obvia la protección del sitio web ilegalmente, se extrae datos personales, entre otros, e incluso se puede llegar a obtener acceso a el ordenador del desarrollador de la página web.

Los hackers y ciberdelincuentes constantemente desarrollan y perfeccionan nuevas estrategias para burlar la seguridad del sitio web. Por causa de esto, este proyecto trata de evolucionar contra ellos, surge de la necesidad de aportar ayuda a los establecimientos que están siendo atacados diariamente para que dejen de presentar vulnerabilidades ante ciberataques que toman control, manipulan o roban información del sitio web que luego usan estos ciberdelincuentes para realizar otras prácticas fraudulentas, como el phishing, la suplantación de identidad o incluso el fraude financiero. Precisamente, este proyecto se centrará en proteger a todos los institutos de la Comunidad de Madrid. Se obtendrá todas las URL de las páginas web y aulas virtuales de la totalidad de los institutos de educación secundaria (IES) que hay Comunidad de Madrid para, de esta forma, poder determinar cuáles son los institutos cuyas páginas web y aulas virtuales presenten una débil protección ante ataques de este tipo, y, finalmente, poder advertir a los respectivos institutos del riesgo que corren.

# 2. Hipótesis y objetivos del proyecto

## 2.1 Hipótesis

En el global de todas las URLs o direcciones de internet analizadas, existirán centros vulnerables y que comprometen al resto de institutos cuando comparten información entre ellos.

## 2.2 Objetivos del proyecto

El objetivo de este proyecto es diseñar una herramienta que permita analizar el estado de seguridad de las páginas web de todos los institutos de educación secundaria de la Comunidad de Madrid. Esta herramienta se obtendrá usando el valor de las métricas de Google Lighthouse, junto a los resultados del test de ntp y la revisión de la vigencia de los certificados digitales de las páginas web. Como resultado y conclusión de este proyecto, se quiere identificar qué institutos tienen problemas de ciberseguridad en sus páginas web para proponer soluciones que mejoren su funcionamiento, y con esto, conseguir una protección generalizada en todas las páginas web.

# 3. Ciberataques

Debido a que el foco principal de este proyecto es proteger a estas páginas web ante ciberataques, se debe saber a qué tipos de ciberataque están expuestos estos sitios web, cuáles son las amenazas de cada uno y cúales son los más peligrosos.

## 3.1. Tipos de ciberataques

Dentro del gran campo de los ataques informáticos, existen varias categorías dentro de ellos. Este proyecto se centra en los ciberataques cuyo objetivo es una página web.

### 3.1.1. Ataque de inyección SQL

Un ataque de inyección SQL es un tipo de ciberataque que requiere muy poco esfuerzo por parte del atacante pero que debe de ser tomado en cuenta por cualquier desarrollador de sito web. Este tipo de ataque se aprovecha de ciertas características que presenta el lenguaje de programación SQL, en español lenguaje de consulta estructurado. El lenguaje SQL es uno de los lenguajes de programación más ampliamente utilizado para las bases de datos, que, vistas desde la perspectiva de este proyecto, sirven para almacenar nombres de usuarios y contraseñas, entre otros datos. El llamado ataque de inyección SQL tiene una gran potencia porque permite al hacker cometer delitos importantes sin requerir mucho tiempo. Uno de estos delitos puede ser entrar como usuario sin necesidad de contraseña en el sitio que el atacante quiera, o eliminar todos los datos de una base de datos con tan solo escribir ciertos comandos de SQL que inhiben la seguridad impuesta por el creador del sitio web. Estos ataques no solo afectan a sitios web pequeños, como los que se tratan en este proyecto, sino también a grandes empresas como puede ser Sony, que sufrió un ataque de este tipo con grandes consecuencias en 2014, Heartland Payment Systems en 2008, TalkTalk en 2015 o British Airways en 2018.

Un ejemplo de un ataque de inyección SQL ante un sitio web muy vulnerable sería insertar un comando de SQL como: ‘ or 1=1 -- -. El orden de las cosas que suceden en este pequeño comando es el siguiente:

1. Se cierra comillas. Esto sirve para que el sitio web ya no detecte lo siguiente como una cadena (en este caso el nombre de un usuario), sino que, gracias a esta comilla, el sitio web ya está interpretando lo siguiente como código SQL.
2. or 1=1. Esto se escribe porque el sitio está intentando confirmar que el usuario que se inserte exista en la base de datos. Si el usuario coincide, entonces es True. Si nosotros decimos que también sirve que 1=1 para entrar como usuario en el sitio web, siempre se va a cumplir, entonces el hacker siempre entrará ante estas vulnerabilidades.
3. -- -. En el lenguaje de programación SQL, estas comillas convierten lo siguiente que se diga en la línea en un comentario. Cualquier intérprete de programación está diseñado para obviar completamente los comentarios, que, con buena intención, están diseñados para explicar lo que hace en cada línea de código para cualquier persona que esté leyendo el código. Con estas comillas se desactiva lo siguiente que se dice en la línea de código, que es para confirmar que el usuario se sabe su contraseña. Cuando esto se desactiva, entonces el hacker entra como usuario sin haber ingresado contraseña en la interfaz diseñada para los usuarios.

### 3.1.2. Ataque de Cross-Side Scripting

Estos ataques se parecen a los ataques de inyección SQL en tanto que también se aprovechan de un código con errores y vulnerabilidades, es decir, una página web mal hecha que da margen al atacante a aprovechar esos errores para beneficiarse de alguna manera. En este tipo de ciberataques, el atacante sabe que la página web es vulnerable y escribe un código de JavaScript dentro de una sección en la que se pueda escribir texto. Este código que inserta el atacante puede forzar un error dentro de la página web que crea una notificación que aparecerá siempre a todos los usuarios que entren en esa sección y es capaz de escribir mensajes que un usuario podría pensar que son de parte del sitio web, y por tanto se podría asumir que la información es fiable, y por ello el usuario obedecería a las instrucciones de lo que diga el texto. Pero el atacante también puede insertar un código malicioso que robe todas las cookies de usuarios autenticados del servidor y, con ello, prácticamente poder acceder a la información de todos los usuarios, incluso la del administrador. Un ejemplo podría ser aprovechar una vulnerabilidad en la sección de comentarios de una página web de forma que cuando un usuario quiera comentar algo le aparezca una notificación en forma de texto que diga que tiene que acceder con su cuenta de Google y redirigirle a un sitio web que simule ser Google, pero en verdad tenga un software malicioso que extraiga las credenciales del usuario. A los atacantes les interesa mucho la contraseña de un correo, por ejemplo, para luego realizar otras técnicas de fraude digital, como el phishing, o hacer spam en la dirección de correo electrónica. Estos ataques también son muy peligrosos, porque también requieren poco esfuerzo y además es difícil que el usuario que esté siendo atacado se dé cuenta que realmente está siendo atacado. Además, como se ha visto, también se puede robar la información de los usuarios sin siquiera ser advertido.

### 3.1.3. Ataque de fuerza bruta

Los ataques de fuerza bruta son otro tipo de ataque en los que se fuerza una contraseña, típicamente de un usuario, probando con una inmensa cantidad de contraseñas posibles. Normalmente, si una contraseña es débil, como “contraseña” entonces estos ataques la encontrarían con facilidad. Para mitigar estos ataques, se pueden usar captchas. Los captchas verifican que quien intenta acceder a su cuenta no es un robot. Por ejemplo, se requeriría identificar señales de tráfico, bicicletas y demás.

Sin embargo, este ataque no es efectivo contra contraseñas seguras, puesto que la máquina tiene que probar con todas las contraseñas posibles con caracteres especiales, números y etcétera. Un ejemplo de contraseña segura es “nRU8!uDTmUUCn#HyEsp4zG”. Estos ataques no deben ser menospreciados por su simplicidad y deberían ser tomados en cuenta a la hora de crear una contraseña de usuario.

### 3.1.4. Ataque de denegación de servicio (DDoS y DoS)

Un ataque de denegación de servicio es tal en el que un dispositivo o red de dispositivos sobrecarga a un servidor, como podría ser el de un sitio web, de forma que lo deshabilita. Es decir, que el servidor se colapsa porque no está preparado para recibir tantas peticiones. El término DoS significa “denegación de servicio” traducido al español, mientras que DDoS significa “denegación de servicio distribuida”. Este último se refiere a que la denegación de servicio se reparte entre miles de ordenadores. El hacker suele tomar control de estos mediante algún software malicioso. Los ataques de DoS presentan similitudes con los DDoS, pero esta vez es solo un dispositivo el que colapsa el servidor. Los ataques de denegación de servicio se dan constantemente a escala global, y siguen siendo una gran amenaza a pesar de sus más de 20 años de historia.

Existen soluciones comerciales que detectan este ataque y lo cortan de raíz, pero debido a su coste no son adquiridas por la Comunidad de Madrid.

# 4. Google Lighthouse

Una de las herramientas que se usará para este proyecto es Google Lighthouse. Esta interesante herramienta de Google fue creada para asegurar que todos los sitios web cumplan con los más recientes estándares web de Google y permite realizar un análisis de la calidad de la página web que se le proporcione.

Normalmente, Google Lighthouse es usado por desarrolladores web que quieren saber qué mejorar de su sitio web, si es de buena calidad, etcétera. Pero para los fines de este proyecto, Google Lighthouse se usará con otro enfoque. A partir de los análisis que dicha herramienta haga sobre la totalidad de las URL de las páginas web oficiales y las URL de todas las aulas virtuales de todos los institutos de educación secundaria de la Comunidad de Madrid, se sintetizará esta información junto con otras cuya obtención se explica más adelante, de modo que se pueda determinar finalmente qué institutos son más vulnerables o cuyo estatus de ciberseguridad sea más bajo que la media, y, por tanto, podrían ser atacados con más fácilidad. También se podrá saber qué institutos presentan mejores prácticas en sus páginas web para así implementar todas estas en los sitios web de los demás institutos, consiguiendo una protección generalizada, que es uno de los objetivos de este proyecto.

## 4.1. Qué es Google Lighthouse

Google Lighthouse es una herramienta automatizada de código abierto desarrollado por Google que sirve para mejorar la calidad de una página web.

### 4.1.1. Cómo funciona Google Lighthouse

Al proporcionar una URL a Lighthouse, esta realiza varias auditorías dentro de ella para luego poder entregar un informe al usuario de lo que haya encontrado Google Lighthouse. El principal propósito de estas auditorías es seguir los Core Web Vitals de Google.

Los Core Web Vitals son un conjunto de métricas que Google utiliza para medir la experiencia del usuario en las páginas web, específicamente en términos de velocidad de carga, interactividad y estabilidad visual. Estas métricas son importantes para el posicionamiento en los motores de búsqueda y para mejorar la experiencia del usuario. Los tres indicadores principales son First Input Delay (FID), que mide la interactividad de la página, es decir, el tiempo que tarda en responder a la primera interacción del usuario, Cumulative Layout Shift, e Interaction to Next Paint (INP). Esta última evalúa la capacidad de respuesta general de una página ante las interacciones del usuario.

Dentro del informe que entrega Lighthouse, se proporciona una puntuación del 1-100 en los siguientes parámetros:

* Performance
* Accessibility
* Best Practices
* Search Engine Optimization

## 4.2. Performance

Performance mide el tiempo que tarda en cargar el sitio web y el tiempo que pasa hasta que el usuario puede acceder a la página web. Dentro de Performance se hallan varias submétricas: LCP, FCP, TTI, TBT, CLS y Speed Index

### 4.2.1. Largest Contentful Paint (LCP)

LCP mide el tiempo que tarda en cargar el elemento más grande del sitio web. También es uno de los Core Web Vitals, porque la experiencia que tendría un usuario en la página web se podría ver mermada por el mero hecho de que haya un elemento muy grande en la página web que no se cargue, causando frustración en el usuario. Todo lleva a la posibilidad de que el usuario no quiera volver a entrar en dicha página web.

4.2.2. First Contentful Paint (FCP)

FCP mide el tiempo que tarda en cargar el primer elemento del sitio web. Esta métrica, aunque puede parecer simple, es vital para asegurar que el usuario obtenga una buena experiencia con el sitio web y acceda en más ocasiones.

4.2.3. Time To Interactive (TTI)

TTI mide el tiempo que tarda el sitio web en ser interactivo para el usuario. En otras palabras, es el intervalo de tiempo entre que el usuario realiza una acción que requiere de respuesta del sitio web y el sitio web la procesa y ejecuta su respuesta.

4.2.4. Total Blocking Time (TBT)

Mide el tiempo en el que el sitio web no capta cualquier tipo de acción por parte de usuario. Por ejemplo, un clic. Es muy poco recomendable tener un TBT alto, ya que es posible que la experiencia del usuario se vea totalmente arruinada al no poder interactuar correctamente con el sitio web. No se debe confudir con TTI, ya que en este parámetro el sitio web ya es interactivo para el usuario, y simplemente mide el tiempo de respuesta del sitio web.

### 4.2.5. Cumulative Layout Shift (CLS)

CLS es otra medida de Lighthouse que estudia cuánto cambia el diseño de la página web a lo largo del tiempo. El diseño de páginas que tengan un CLS bajo y saludable será estable mientras que el diseño de una página web con CLS alto cambiará mucho en poco tiempo, lo que resulta en una experiencia del usuario mucho peor ya que al usuario le será difícil saber cuándo ha terminado de cargar la página web.

4.2.6. Speed Index

Speed Index es una métrica que mide cómo de rápido el contenido de un sitio web se carga dentro del tiempo que tarda la página web en cargar totalmente. Cuando Google Lighthouse está realizando una auditoría para generar el informe solicitado, graba un vídeo que abarca desde que la página web empieza a cargar dentro del buscador hasta que termina de haberse cargado. Con ese video, Lighthouse es capaz de determinar cuánto tardó el contenido de la página en cargar.

## 4.3. Accessibility

Lo siguiente que estudia Google Lighthouse después de la Performance es Accesibility. La puntuación de Accesibility es un resumen sobre cómo de bien está optimizada y ajustada la página web para personas con discapacidades. Accesibility es el examen que hace Lighthouse para valorar la experiencia que tendrían usuarios de tecnologías adaptativas con el sitio web.

## 4.4. Best Practices

La métrica Best Practices de Lighthouse verifica si la web cumple con los más recientes estándares de desarrollo web. Además, realiza una auditoría corta de prácticas aceptadas generalmente de desarrollo web. Estas prácticas están normalmente orientadas hacia la seguridad del sitio web, como usar la última versión de las librerías de JavaScript, usar https, etcétera. A esta categoría se le dará más peso en la media final que otras dentro de performance, ya que no es tan importante para el foco de este proyecto cómo de atractiva la página web es para los usuarios, sino que prevalece la seguridad que tiene el sitio web, porque es lo que trata de para poner un freno a las intenciones del hacker.

## 4.5. Search Engine Optimizitation (SEO)

La última categoría de Google Lighthouse que se puntúa del 1-100 es SEO. Esta última medida estudia cómo de parecidas son las prácticas de SEO de la página web proporcionada a las prácticas recomendadas. Revisa aspectos técnicos como si la página es afín con el teléfono móvil y si tiene datos estructurados válidos, entre otros.

# 5. Test NTP

En el ámbito de la ciberseguridad, la precisión horaria de un servidor web es un aspecto crítico que puede revelar vulnerabilidades en la infraestructura de un sitio. El Test NTP tiene como objetivo evaluar si las páginas web de los institutos de educación secundaria de la Comunidad de Madrid están correctamente sincronizadas con servidores de tiempo oficiales, lo que permite detectar posibles fallos de configuración que puedan hacerlas más susceptibles a ciberataques.

La sincronización horaria no es solo una cuestión de precisión técnica, sino también un indicador del nivel de mantenimiento y seguridad de un servidor. Una página web cuya hora del sistema no está alineada con fuentes de tiempo confiables puede estar desactualizada, mal configurada o incluso abandonada, lo que la convierte en un blanco fácil para atacantes. Muchos ataques informáticos, como la falsificación de certificados SSL, la manipulación de logs y la explotación de vulnerabilidades en protocolos de autenticación, pueden aprovecharse de servidores con tiempos incorrectos.

Este test se realiza comparando la hora reportada por el servidor del instituto con la hora oficial de España, obtenida a través de un servidor NTP de referencia como hora.roa.es, gestionado por el Real Instituto y Observatorio de la Armada. Si la diferencia entre ambas horas es mínima (menos de cinco segundos), se puede inferir que el servidor está correctamente mantenido y sincronizado con una fuente confiable. Esto sugiere que los administradores del sitio están atentos a la seguridad del sistema y realizan configuraciones adecuadas para evitar riesgos derivados de la desincronización horaria.

Si la diferencia se encuentra entre cinco segundos y un minuto, puede indicar que el servidor no está recibiendo actualizaciones de tiempo de manera constante o que su servicio NTP está mal configurado. Esto puede ser una señal de mantenimiento deficiente y puede hacer que el sitio sea vulnerable a ciertos ataques, como la suplantación de identidad mediante certificados expirados.

Cuando la diferencia supera un minuto, se considera que el servidor está desincronizado, lo que es una clara señal de que no está siendo gestionado de manera adecuada. Los sistemas desincronizados suelen ser más propensos a sufrir ataques de tipo **replay**, en los cuales un atacante puede reutilizar credenciales o datos de sesión antiguos para obtener acceso indebido. También pueden ser vulnerables a la alteración de registros de auditoría, dificultando la detección de intrusiones y la respuesta a incidentes de seguridad.

Además, la falta de sincronización puede indicar que el servidor no ha recibido actualizaciones en un tiempo prolongado, lo que aumenta el riesgo de que el software y los servicios en ejecución contengan vulnerabilidades sin parchear. Los atacantes suelen escanear Internet en busca de servidores desactualizados con configuraciones débiles, y una diferencia horaria significativa puede ser una pista clara de que un sistema no está siendo supervisado regularmente.

Por estas razones, el Test NTP es una herramienta clave para evaluar no solo la sincronización horaria de un servidor, sino también el nivel de mantenimiento y seguridad de la página web de un instituto. Un servidor bien mantenido y sincronizado es menos propenso a sufrir ataques y ofrece mayor garantía de que sus sistemas de autenticación, cifrado y auditoría funcionan correctamente. En cambio, una desincronización importante es una señal de advertencia que indica la necesidad de revisar y reforzar la seguridad del sitio web.

# 6. Certificado

Posteriormente, se revisará la calidad y caducidad del certificado digital de las páginas web.

# 7. Programas usados

-Experimentación

-Indicios

# 8. Resultados y conclusiones

## 7.1 Resultados

## 7.2 Conclusiones

# 9. Bibliografía y fuentes consultadas

“Curso de PYTHON desde CERO (Completo)” YouTube, 23 ene 2023 <https://www.youtube.com/watch?v=nKPbfIU442g>. Acceso el 10/12/2024

<https://conrecursos.org/wp-content/uploads/2021/07/lista-codigo-centros-2020-2021.pdf> lista de todos los institutos, Acceso el 28/12/2024

“How to install and use Google Lighthouse CLI” Branda Smith, December 27, 2023

<https://www.oxyplug.com/optimization/how-to-install-and-use-google-lighthouse-cli/#what-is-google-lighthouse> Acceso el 29/01/2025

Heričko, T., Šumak, B., & Brdnik, S. (2021, September). Towards representative web performance measurements with google lighthouse. In *Proceedings of the 2021 7th Student Computer Science Research Conference* (p. 39). Acceso el 29/02/2025

Lisa Gibson / <https://digitalguider.com/blog/what-is-google-lighthouse-how-does-its-score-affect-seo> Acceso el 02/02/2025

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

<https://doi.org/10.1016/j.egyr.2021.08.126> Acceso el 02/02/2025

<https://es.semrush.com/blog/como-utilizar-google-lighthouse/> Acceso el 02/02/2025

<https://developer.chrome.com/docs/lighthouse/overview?hl=es-419> Acceso el 02/02/2025

[https://www.hostinger.es/tutoriales/core-web-vitals](https://www.hostinger.es/tutoriales/core-web-vitals%20Acceso%20el%2006/02/2025)  Acceso el 02/02/2025

<https://www.nivelics.com/blog/cuales-son-los-ciberataques-mas-frecuentes-en-los-sitios-web> Acceso el 08/02/2025

<https://www.youtube.com/watch?v=tdtAmH3ZSAI> Acceso el 08/02/2025

<https://www.youtube.com/watch?v=sRaSXV_IxFY> Acceso el 12/02/2025

[https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-certificado-digital-de-una-pagina-de-internet](https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-certificado-digital-de-una-pagina-de-internet%20Acceso%20el%2022/02/2024)  Acceso el 22/02/2025

<https://laadministracionaldia.inap.es/noticia.asp?id=1168657> Decreto 73/2017, de 8 de agosto, del Consejo de Gobierno, por el que se suprime el Instituto de Educación Secundaria “Escuela Técnico Profesional de la Salud de la Comunidad de Madrid” (BOCAM de 16 de agosto de 2017). Texto completo. Acceso el 23/03/2025