UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI

VICERRECTORADO DE INVESTIGACIÓN

ESCUELA DE POSGRADO

MAESTRIA EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

MODELO PREDICTIVO MACHINE LEARNING DE CALIDAD DE APLICACIONES Y SEGURIDAD WEB DE UNIVERSIDADES DEL PERÚ, AÑO 2020

PRESENTADA POR:

JUAN CARLOS JIMENEZ FLORES

ASESOR

Mg. ALBERTO ENRIQUE COHAILA BARRIOS

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

CON MENCIÓN EN SEGURIDAD Y AUDITORIA INFORMÁTICA

MOQUEGUA – PERÚ

2022

TABLA DE CONTENIDOS

ÍNDICE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El **objetivo** principal fue determinar la diferencia de medias de dos tratamientos del modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las universidades del Perú, año 2020. El **método** de investigación fue aplicada científica, nivel predictivo y diseño experimental puro. Población, 142 universidades peruanas, con una muestra de 104 y un error aleatorio de 5%. **Instrumento**, algoritmos de machine learning, Web.dev y webhint. **Resultado**, el mejor algoritmo eficiente fue Linear Regression para el modelo predictivo machine learning, con coeficiente de determinación 1,00 e índice Kappa en la categoría muy buena para la predicción de seguridad web. El modelo predictivo fue $\hat{Y} = 9{,}526 - 0{,}0016X_1 - 0{,}0039X_2 + 0{,}0033X_3 + 0{,}0060X_4 - 0{,}9328X_5$ para la calidad de aplicaciones y seguridad web. Es verdadera la hipótesis nula porque existe suficiente evidencia estadística de que las medias no difieren, porque es igual a cero, en el nivel de significancia de 0,05 y existe una relación de 99,99% de que el algoritmo predictivo Linear Regression de machine learning es más eficiente y los para los parámetros aprendizaje peso (W), es verdadero la hipótesis alterna porque valor-p es menor a alfa, que significa que la media de los pesos de aprendizaje o regresores, es diferente de cero, por lo que el modelo tiene una relación de 98,00% de coeficiente de determinación. **Conclusión**, la relación entre las variables de investigación fue de 99,99% para modelo predictivo y la diferencia de medias con tratamiento X y Y fue de 0,0002219.

.

Palabras claves: Machine learning; calidad de software web; seguridad web, modelo predictivo.

ABSTRACT

The main objective was to determine the difference in means of two treatments of the trained machine learning predictive model between the quality of applications and web security of the universities of Peru, year 2020. The research method was applied scientific, predictive level and pure experimental design. Population, 142 peruvian universities, with a sample of 104 and a random error of 5%. Instrument, machine learning algorithms, Web.dev and webhint. As a result, the best efficient algorithm was linear regression for the machine learning predictive model, with a coefficient of determination 1.00 and a Kappa index in the very good category for predicting web security. The predictive model was $\hat{Y} = 9.526 - 0.0016X_1 - 0.0039X_2 + 0.0033X_3 + 0.0060X_4 - 0.9328X_5$ for application quality and web security. The null hypothesis is true because there is sufficient statistical evidence that the means do not differ, because it is equal to zero, at the 0.05 level of significance and there is a 99.99% relationship that the predictive algorithm Linear regression of machine learning is more efficient and those for the weight (W) learning parameters, the alternate hypothesis is true because p-value is less than alpha, which means that the mean of the learning weights or regressors is different from zero, so the model has a 98.00% coefficient of determination. Conclusion, the relationship between the research variables was 99.99% for the predictive model and the difference in means with treatment X and Y was 0.0002219.

Keywords: Machine learning; quality of web software; web security, predictive model.

INTRODUCCIÓN

La calidad software y seguridad web de las universidades garantizan que no sea vulnerables (no hay agujeros / fallas de seguridad) a piratas informáticos de acceder a la base de datos y al panel de administración del sitio web. Para evitar la vulnerabilidad del software del sitio web, los programadores deben desarrollar scripts que cumplan con los requisitos de seguridad web para que el software sea inaccesible y, por lo tanto, confiable. Existen diferentes tipos de herramientas, por ejemplo, XSpider, Acunetix Web Vulnerability Scanner, utilidades para detectar inyecciones de SQL, XSS, RFI. También debe verificar los códigos fuente del sitio web utilizando análisis de código estático (RIPS) y si se detecta alguna vulnerabilidad, debe rectificarse para evitar su explotación.

La creciente popularidad de Machine Learning y la inteligencia artificial atrajo la atención de partes maliciosas que comenzaron a lanzar ataques contra sitios web que albergan información vital como números de tarjetas de crédito, contraseñas, entre otros datos personales, o en su defecto liberar malware con el fin de destruir archivos o retener ordenadores como rehenes.

En Perú, la nueva ley Universitaria 30220, habla acerca de la calidad académica y como función la investigación, utilizando tecnología de internet para la gestión académica y administrativa en las universidades públicas, asociativas y societarias, encontrando que estas no invierten en la calidad de aplicaciones web para medir su usabilidad, funcionalidad, fiabilidad y eficiencia.

Asimismo, en la seguridad web, las características más relevantes a medir son abridor de rechazo de enlaces externos, usar HTTPS, encabezados HTTP no permitidos, sin URL relativas al protocolo, sin bibliotecas vulnerables, utilice la integridad de los subrecursos, prueba de servidor SSL, utilice el encabezado `Strict-

Transport-Security`, encabezado "Set-Cookie" válido y utilice el encabezado `X-Content-Type-Options`. Los instrumentos tecnológicos que se utilizaron para pretest fueron web.dev, webhint y para modelamiento Microsoft Azure Machine Learning Studio (classic).

El problema de investigación formulado fue: ¿Cuál es el coeficiente de determinación y diferencia de medias del modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las Universidades del Perú, año 2020?

El objetivo fue Diseñar y determinar el coeficiente de determinación y diferencia de medias del modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las Universidades del Perú, año 2020.

El informe de investigación está organizado por capítulos. Capítulo I, problema de la investigación. Capítulo II, marco teórico. Capítulo III, método Capítulo IV, presentación y análisis de resultados. Capítulo IV conclusiones y recomendaciones; y finalmente Bibligrafía y anexos.

CAPÍTULO I
EL PROBLEMA DE LA INVESTIGACIÓN

1.1 Descripción de la realidad problemática

La calidad de software web es una de las preocupaciones tradicionales por que la World Wide Web fue originalmente creada para mostrar información a internautas que utilizan sitios web sencillos que consisten principalmente en documentos de texto con hipervínculos. Las aplicaciones web modernas funcionan a gran escala, como aplicaciones de software para comercio electrónico, distribución de información, entretenimiento, colaboración, investigación y muchas otras actividades. Se ejecutan en plataformas de hardware distribuidas y equipos heterogéneos.

Desde Julio del 2014, está vigente la nueva ley Universitaria 30220, resaltando el principio de calidad académica en función a la investigación, por ende las universidades peruanas deben y tienen que invertir en seguridad web y calidad de aplicaciones, esto en contraste con la realidad no se cumple en la mayoría de universidades, por ende no detectan ataques frecuentes como las inyecciones SQL, donde el atacante encuentra una vulnerabilidad del sistema para usar el código de la aplicación accediendo a la base de datos.

La Autenticación y gestión de sesiones rotos, es uno de los varios problemas en relación a la seguridad de la información el cual se encarga del mantenimiento de la identidad del usuario, si acaso las credenciales de autenticación, así como también los identificadores de sesión no se encuentren protegidos, son vulnerables a ataques informáticos como el secuestro de una sesión activa asumiendo la identidad del usuario.

En cuanto a la inseguridad de referencias de objetos directos de una aplicación web, se expone la referencia a un objeto de implementación interno como lo son los archivos, registros de base de datos, directorios y claves.

La mala configuración de seguridad, abarca varios tipos de vulnerabilidades, todas centradas en la falta de mantenimiento a la configuración de la aplicación web. La mala configuración de la seguridad les da a los piratas informáticos acceso a datos o funciones privados y puede resultar en un compromiso total del sistema. La falsificación de solicitud en todo el sitio (CSRF), es el ataque malintencionado, el cual consiste en engañar al usuario para que este realice una acción sin la intención de realizar. Un sitio web de terceros enviará una solicitud a una aplicación web en la que el usuario ya se encuentra registrado (por ejemplo, su banco). El atacante puede acceder a la funcionalidad a través del navegador web ya autenticado de la víctima. Los objetivos incluyen aplicaciones web como redes sociales, correos electrónicos, banca en línea e interfaces web para dispositivos de red.

1.1.1 Antecedentes del problema

Las universidades, tiene poco conocimiento de calidad y seguridad de sitios web, porque:

- No recaban y clasifican información sobre errores y defectos del software.
- No intentan rastrear cada defecto y error desde la causa que dieron su inicio (por ejemplo, no conformidad con las especificaciones, error de diseño, violación de los estándares, mala comunicación con el cliente, etc.).
- No usan, el uso del Principio de Pareto (80% de los defectos se debe a 20% de todas las causas posibles), se identifica 20% de las causas de errores y defectos.
- No identifican las pocas causas vitales, para subsanar los problemas que dan origen a los defectos y errores.

1.1.2 Problemática de la investigación

Las universidades peruanas, son un agente de cambio y transformadora de los discentes universitarios y de las capacidades modificadas para insertar a las organizaciones públicas y privadas como profesionales competitivos globalmente y a la sociedad peruana, sin embargo, actualmente las universidades no cuentan con una calidad de aplicaciones en sus páginas web, careciendo también de políticas en la seguridad de su información, es por ello que los ciberdelincuentes como los denominados hackers utilizan bots maliciosos para el robo de información, como los datos sensibles desde contraseñas, datos personales, cuentas bancarias, hasta la destrucción de datos o en su defecto inhabilitar los sistemas y redes por completo. Una universidad que no cuente con sistemas de inteligencia artificial que detecten a tiempo estos ataques, son un blanco perfecto para estos ciberdelincuentes.

1.2 Definición del problema

1.2.1 Problema General

¿Cuál es la diferencia de medias de dos tratamientos del modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las universidades del Perú, año 2020?

1.2.2 Problemas derivados

¿Cuál, es el mejor algoritmo del modelo predictivo de machine learning entrenado más eficiente basado en las métricas entre la calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas?

¿Cuál es la diferencia de los pesos pronosticados ($\widehat{W}_i$) de aprendizaje para una regresión significativa del modelo predictivo de machine learning entre calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

Determinar la diferencia de medias de dos tratamientos del modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las Universidades del Perú, año 2020.

1.3.2 Objetivos específicos

a) Determinar, el mejor algoritmo el modelo predictivo de machine learning entrenado más eficiente basado en las métricas entre la calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

b) Determinar, la diferencia de pesos pronosticados ($\widehat{W}_i$) de aprendizaje para una regresión significativa del modelo predictivo de machine learning entre calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

1.4 Justificación e importancia de la investigación

La conveniencia, es la utilidad de la investigación, que servirá para apreciar la concordancia de atributos del modelo predictivo machine learning de calidad de aplicaciones y seguridad web, es decir que tan seguras son las páginas web de las universidades.

Relevancia social o la trascendencia para la sociedad, es la aplicación de seguridad web a 142 universidades peruanas del año 2020, que albergan más de un millón de estudiantes de Pregrado y Posgrado de acuerdo al censo de 2010 de ex ANR. Se determinarán, algoritmos predictivos de machine learning más eficientes, mostrando concordancia de atributos entre calidad de aplicaciones y seguridad web de las universidades del Perú.

Las implicancias prácticas, ayudarán a resolver varios problemas, describiendo y determinando, la concordancia y nivel entre seguridad de sitios web y visibilidad e identidad de las Universidades públicas, asociativas y societarias del Perú. Además, se evaluará, la concordancia y nivel de calidad de las aplicaciones web en cuanto a rendimiento, accesibilidad, mejores prácticas y perfeccionar los motores de búsqueda con la seguridad de sitios web de las universidades públicas, asociativas y societarias del Perú.

1.5 Variables

1.5.1 Identificación de las variables

Y = Modelo predictivo machine learning de seguridad web

X_1 = Algoritmos predictivos machine learning

X_2 = Calidad de aplicaciones web

1.5.2 Operacionalización de variable algoritmos predictivos machine learning

Definición conceptual

Machine learning, es una técnica de ciencia de datos que permite a las computadoras, utilizar datos existentes para prever tendencias, resultados y comportamientos futuros. Mediante el aprendizaje automático, las computadoras aprenden sin necesidad de programarlos explícitamente.

Definición operacional

Para la implementación de los modelos predictivos de machine learning de regresión lineal bayesiano, Decisión de regresión forestal, regresión lineal, regresión de la red neuronal y Regresión del árbol de decisión impulsada, el entrenamiento será utilizando el diseñador de Azure Machine learning (versión free) para preparar los datos, entrenar, probar, implementar, administrar y realizar un seguimiento de los modelos de aprendizaje automático, evaluando cada algoritmo con índice kappa.

1.5.3 Operacionalización de variable, calidad de aplicaciones web

Definición conceptual

La calidad del diseño de aplicaciones web, es el grado en el que el diseño cumple las funciones y características especificadas en el modelo de requerimientos en las

dimensiones calidad del desempeño, calidad de las características, confiabilidad, conformidad, durabilidad, servicio, estética y percepción (Pressman, 2010)

Definición operacional

La calidad de aplicaciones web, se medirá de acuerdo a los indicadores rendimiento o performance, accesibilidad, buenas prácticas y SEO, utilizando Software de auditoría de sitios web "web.dev", teniendo como escala porcentual de 0 – 100, donde Bueno (90 – 100), Necesita mejorar (50 – 89) y Deficiente (0 – 49).

Variable	Indicadores	Instrumento	Escala de medida
X_2 = Calidad de aplicaciones web	• Rendimiento • Accesibilidad • Buenas prácticas • SEO	Sofware de auditoría de sitios web web.dev	0 – 100 90 – 100 Bueno 50 – 89 Necesita mejorar 0 – 49 Deficiente

1.5.4 Operacionalización de variable seguridad de sitios web

Definición conceptual

La seguridad del software es una actividad del aseguramiento del software que se centra en la identificación y evaluación de los peligros potenciales que podrían afectarlo negativamente y que podrían ocasionar que falle todo el sistema.

Definición operacional

La seguridad de sitios web, se evaluará con los indicadores abridor de repudio, https-only, encabezados no rechazados, URL-relativas-sin-protocolo, sri, estricta seguridad de transporte, validar conjunto de encabezado de cookie, X opciones de tipo de contenido, bibliotecas-javascript-no-vulnerables, sslab, teniendo como escala desde 0 hasta 100, donde Deficiente (90 – 100), Necesita mejorar (50 – 89) y Bueno (0 – 49).

Variable	Dimensiones	Indicadores	Instrumento	Escala de medida
Y = Seguridad de sitios web	Modelo Predictivo: X_1 = Algoritmos predictivos machine learning	Métricas: • Error absoluto medio • Error cuadrático medio • Error absoluto relativo • Error al cuadrado relativo • Coeficiente de determinación	Diagrama del modelo de aprendizaje automático	Índice de Kappa 0,00 - 0,20 Pobre 0,21 - 0,40 Débil 0,41 - 0,60 Moderada 0,61 - 0,80 Buena 0,81 - 1,00 Muy buena
	X_2 = Seguridad sitios web	• disown-opener • https-only • no-disallowed-headers • no-protocol-relative-urls • sri • strict-transport-security • validate-set-cookie-header • x-content-type-options • no- vulnerable-javascript-librar • ssllabs.	Sofware de auditoría de sitios web "webhint"	0 - 4,9 Deficiente 5,0 - 8,9 Necesita mejorar 9,0 - 10,0 Bueno

1.6 Hipótesis

1.6.1 Hipótesis general

H_0: No existe una diferencia de medias de dos tratamientos del modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las Universidades del Perú, año 2020.

H_1: Existe una diferencia de medias de dos tratamientos del modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las Universidades del Perú, año 2020.

1.6.2 Hipótesis Derivadas o Secundarias

Primera

H_0: No existe una diferencia de medias del mejor algoritmo predictivo de machine learning entrenado más eficiente basados en las métricas entre la calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

H_1: Existe una diferencia de medias del mejor algoritmo predictivo de machine learning entrenado más eficiente basados en las métricas entre la calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

Segunda

H_0: No existe diferencia de pesos pronosticados ($\widehat{W}_i$) de aprendizaje para una regresión significativa para el modelo predictivo de machine learning entre calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

H_1: Existe diferencia de pesos pronosticados ($\widehat{W}_i$) de aprendizaje para una regresión significativa para el modelo predictivo de machine learning entre calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Internacionales

Como antecedentes internacionales, se presenta el artículo científico de Gallagher et al., (2022), quienes examinan dos tipos de ataques de machine learning en modelos financieros de series temporales, los cuales son Fast Gradient Signed Method y Label Flip en un arquitectura de tendencia, en otras palabras, un modelo de red neuronal unidimensional para la clasificación de series temporales. Los resultados muestran que la arquitectura era susceptible a estos ataques en consecuencia la precisión del clasificador se vio significativamente afectada.

Así mismo, Alani & Tawfik (2022) presentan en su artículo científico un sistema de detección de URL de phishing basado en Machine Learning, teniendo como resultado que Random Forest presentó el mejor rendimiento con una precisión muy alta de 97,5%.

Además, Ahammad et al., (2022) en su artículo científico que tuvo como objetivo proporcionar una solución para detectar sitios web con URL phishing con la ayuda de algoritmos de aprendizaje automático. Para esto se creó un modelo de

aprendizaje automático para detectar si una URL es maliciosa o no, se utilizaron algoritmos como Decision Trees, Random Forests, Light GBM, Logistic Regression y Support Vector Machine (SVM).

Por otro lado Hurst et al., (2022) investigadores del Reino Unido abordan el tema de gestión eficiente de datos de pacientes mediante la integración del Machine Learning, sin embargo, se observó que existen peligros inherentes a la digitalización de registros de los pacientes. Teniendo en cuenta la naturaleza confidencial de estos datos, que corren peligro de amenazas externas y ataques internos. En atención a este tipo de amenazas, esta investigación se centró en la detección del uso indebido de datos internos. El enfoque implica el uso de clasificación supervisada (árbol de decisión, bosque aleatorio y máquina de vectores de soporte) basada en datos del mundo real pre-etiquetados recopilados de un hospital con sede en el Reino Unido para la detección del uso indebido de datos de. Los resultados demuestran que al emplear Machine Learning para analizar el acceso a los datos de registro de salud electrónicos, la detección de anomalías se puede lograr con una precisión de 0,9896 de un conjunto de prueba y 0,9908 del conjunto de validación utilizando un clasificador de máquina de vector de soporte.

Del mismo modo Berghout et al., (2022) en su artículo científico sobre Machine Learning para la ciberseguridad de redes inteligentes, el autor menciona que el ML es una de las principales tecnologías de IA capaz de detectar, identificar y responder mitigando ataques de adversarios en las redes inteligentes. En este contexto, el objetivo principal de su artículo fue revisar diferentes herramientas de ML utilizadas en los últimos años para el análisis de ciberataques. También proporciona pautas importantes sobre la selección del modelo ML como una

solución global al construir un modelo predictivo de ataques. Por lo tanto, desarrolló una clasificación detallada con respecto a la tríada de seguridad de datos, es decir, Confidencialidad, Integridad y Disponibilidad dentro de diferentes tipos de ciber amenazas, sistemas y conjuntos de datos.

Como lo señala Karasan (2022) en su libro para desarrolladores, programadores que exploran el aprendizaje automático basado en Python y los modelos de aprendizaje profundo para evaluar el riesgo financiero. Se explora un modelo de volatilidad para medir los grados de riesgo, usando regresión de vectores de soporte, redes neuronales y depp leaning. Revisando los modelos de riesgo de mercado, mediante el uso de técnicas de aprendizaje automático, con una técnica de agrupamiento para la clasificación de riesgos, para luego aplicar la estimación bayesiana. Se usa modelos de aprendizaje automático para la detección de fraude, identificando el riesgo corporativo usando la métrica de la caída del precio de las acciones.

2.1.2 Nacionales

En la tesis de Valverde (2018), sobre riesgos de seguridad en los Websites con efecto en la gestión de la información, la investigación tuvo como resultado que el 53% de las entidades presentan problemas con las websites, existiendo niveles significativos de inseguridad y penetración de crackers no pudiendo ser controlado por las medianas empresas en la ciudad de Lima Metropolitana.

Del mismo modo Taboada (2021) en su tesis de maestría sobre seguridad de la información en la mejora de los activos de información financiera, propuso un modelo de seguridad de la información dando como resultado, 72% de

confiabilidad, lo cual es válido y contribuirá a la mejora de la seguridad de la información financiera.

Por otro lado, la investigación de Huerta (2020) sobre un Sistema de gestión de la seguridad de la información en la mejora de un proceso de gestión del riesgo de un empresa consultora, el estudio concluye que luego de la implementación de dicho sistema este influye de manera positiva en el proceso de gestión de riesgos de la consultora, los hallazgos de la prueba T de student dieron un valor de 4,614, en la comparación de medias de pre y post - test, con un valor de significancia 0,000 en el indicador de riesgo.

En tanto, Manrique (2022) propuso un metodología de ciberseguridad en la mejora de la gestión de tecnología de información, permitiendo mejorar los aspectos de confiabilidad, disponibilidad e integridad de los sistemas de información, estos basados en controles, políticas y mecanismos de seguridad basados en la Norma ISO/IEC27032, permitiendo que la unidad de estudio ingrese al nivel de transformación digital, permitiendo que este sea más eficiente en sus servicios digitales, además de contar con más seguridad de su información tanto física como virtual.

Finalmente, Narro (2021) en su investigación sobre sistema de gestión de seguridad de la información con relación a la gestión de riesgos informáticos de una universidad pública concluye que estos se relacionan de manera inversa. A su vez se recomienda hacer uso de la metodología MAGERIT, que proporciona cuatro secciones para la búsqueda de puntos de peligro en la gestión de riesgos de la universidad, los cuales deberán ser tratados con técnicas de la metodología SRUM.

2.2 Bases teóricas

2.2.1 Ingeniería web

2.2.1.1 Categorías

Para (Chopra, 2016), las aplicaciones web pueden variar desde una aplicación de banca en línea tradicional hasta una aplicación de centro comercial en línea, que será más compleja. A continuación, se detallan las diferentes categorías de aplicaciones web:

1. Sitios web centrados en documentos: Estos sitios web son muy simples y consisten en un grupo de páginas web que básicamente se almacenan en un servidor web. El cliente simplemente envía la solicitud al servidor y la respuesta se envía al cliente en muy poco tiempo. Sin embargo, este tipo de sitios web se pueden piratear fácilmente. Por ejemplo, los sitios web estáticos como simplemente páginas de inicio, webcasts y aplicaciones web simples pertenecen a esta categoría. Por otro lado, las aplicaciones web interactivas también existen hoy en día como una aplicación basada en ajax, donde los controles se cargan y descargan dinámicamente.

2. Aplicaciones web transaccionales: Siempre que utilizamos el término "aplicación web", implica que la aplicación es bastante compleja, ya que también involucra bases de datos en su back-end para almacenar los datos web de los clientes de manera eficiente y consistente. Entonces, ahora, SQL también debería funcionar. La idea no es solo leer datos sino también manipularlos. Por ejemplo, centro comercial en línea, reserva de aerolíneas en línea, banca en línea, etc.

3. Aplicaciones web basadas en flujo de trabajo: estas aplicaciones permiten un manejo sencillo de los flujos de trabajo dentro o entre diferentes organizaciones.

Por tanto, existe la necesidad de interoperabilidad entre ellos. Por lo tanto, es necesario gestionar los flujos de trabajo tanto intra como entre trabajos. Los problemas aquí incluyen la complejidad de los servicios web, las empresas participantes y sus flujos de trabajo. Este tipo de aplicaciones web requieren una cierta estructuración de procesos automatizados. Por otro lado, las aplicaciones web colaborativas son útiles para fines de cooperación en operaciones no estructuradas, es decir, groupware. Aquí, la comunicación necesaria es muy alta. Hoy en día, la Web social también es muy común. Los weblogs o sistemas de filtrado colaborativo nos ayudan a encontrar los recursos relacionados y las personas con intereses similares.

4. Aplicaciones web orientadas a portales: los portales son los ejes centrales que actúan como un punto de acceso a la web. Algunos ejemplos de portales son portales generales como Yahoo, Netscape, y también, portales especializados como portales de negocios, portales de mercados, etc. Los portales de negocios brindan información a los empleados a través de Intranet o Extranet. Los portales de mercado pueden ser portales de mercado horizontales o verticales. Los portales horizontales operan en el mercado de empresa a consumidor (B2C). Los portales verticales involucran empresas de un solo sector.

5. Aplicaciones web ubicuas: Prestan servicios según la demanda del cliente como mostrar temperaturas en la pantalla de los celulares de los clientes, visualizaciones del menú del día, etc. Ha llegado el día en que las aplicaciones ubicuas dominan el mercado al igual que la Web semántica que presenta información para humanos y eso también, en una forma legible por máquina.

2.2.1.2 Características de las aplicaciones web

Las siguientes son las características de las aplicaciones web, en general:

- Ellas evolucionan constantemente porque la información contenida y presentada por el sitio web también cambiará. Los requisitos web son inestables. Su estructura y funcionalidad cambian con el tiempo, y la gestión de esta naturaleza de aplicación web en constante cambio es en sí misma un desafío administrativo, técnico y organizativo.
- Los contenidos web como texto, gráficos y multimedia son ahora parte del software web. La forma en que se presentan estos contenidos repercute en el rendimiento y el tiempo de respuesta del sistema.
- Si conocemos a los usuarios finales, es posible organizar sesiones de formación para ellos sobre cómo utilizar cualquier aplicación web. Pero, si la aplicación web está diseñada para diferentes tipos de usuarios (usuarios anónimos) que tienen diferentes expectativas, entonces dichos usuarios deben estar satisfechos y esto es muy difícil. Esto es así porque ni siquiera podemos ofrecerles capacitaciones. Como resultado, la interacción humano-Web (HWI) también se vuelve muy compleja.
- Hoy en día, casi todos los sistemas basados en la Web funcionan con bases de datos. Estos sitios web se conocen en realidad como aplicaciones web. Estas aplicaciones se actualizan con mucha frecuencia, puede ser cada hora.
- Las aplicaciones web necesitan una mejor apariencia, ya que necesitan mejores formas y controles.

- Las aplicaciones web tienen un programa de desarrollo comprimido y restricciones de tiempo estrictas. Entonces, el proceso de desarrollo no puede llevarse durante muchos años.
- Las ramificaciones de fallas o insatisfacción de los usuarios de las aplicaciones web se pueden observar más en los sistemas basados en la web que en los sistemas tradicionales.
- La percepción de los desarrolladores web jóvenes también es diferente en lo que respecta a la calidad web. Esto también puede causar confusiones.
- La tecnología cambia todos los días y también estos sistemas web. Surgen nuevos lenguajes (XML, AJAX), nuevos estándares web y nuevos sistemas operativos (SO). Esto complica la arquitectura de la Web y, por tanto, se observan más errores. Esto implica que la seguridad de la Web también está en juego.
- El desarrollo web utiliza tecnología y estándares de vanguardia y diversos, e integra diferentes componentes como software tradicional y no tradicional.
- Las aplicaciones web deben implementarse en diferentes tipos de medios de entrega, como diferentes tipos de dispositivos de visualización, formatos y redes de hardware y software que funcionan a una velocidad muy rápida.
- Es fácil piratear y atacar cualquier sistema web hoy en día, ya que debido a la complejidad de los sistemas web, su seguridad también está en juego.

2.2.1.3 Tecnología web

La comunicación entre las computadoras, es mucho más compleja que la comunicación entre las personas, los ordenadores necesitan de códigos a manera de

dialogo, es por ello que las tecnologías web utilizan un lenguaje de marcado y paquetes multimedia para poder comunicarse entre sí.

a) Navegadores

Son aplicaciones que hacen uso de internet para luego interpretar información que será mostrada en forma que el usuario pueda entenderla. Estos son los más populares:

- Google Chrome.
- Safari.
- Firefox
- Internet Explorer y otros.

b) Lenguajes de programación web-servidor

- **Java**: Lenguaje de programación orientado a objetos. Java es conveniente para web y dispositivos móviles. En particular, para implementar el back-end de aplicaciones web, API o escribir aplicaciones de Android. Java es un lenguaje de programación para proyectos altamente cargados. Es decir, aquellos con una cantidad de usuarios bastante grande y alta actividad, y cientos de miles de personas pueden usar el sitio todos los días. En concreto, se habla de aplicaciones web. Y esto es alrededor del 80% de los proyectos que se utilizan actualmente en el mundo. Además, una gran cantidad de código de desarrollo y listo para usar que se puede reutilizar está relacionado precisamente con la escritura de aplicaciones web. Por supuesto, las aplicaciones web no solo se implementan en el lenguaje de programación Java. Se pueden escribir tanto en Python como en Node.

- **PHP**: Lenguaje de secuencias de comandos, fue creado para generar páginas HTML en el lado del servidor web. PHP es uno de los lenguajes más comunes utilizados en el campo del desarrollo web (junto con Java, .NET, Perl, Python, Ruby). PHP es compatible con la gran mayoría de los proveedores de alojamiento. Este lenguaje es interpretado por el servidor web en código HTML, que se transmite al cliente. A diferencia de lenguajes de programación de secuencias de comandos como JavaScript, el usuario no tiene acceso al código PHP, lo que es una ventaja desde el punto de vista de la seguridad, pero perjudica significativamente la interactividad de las páginas. Pero nada prohíbe usar PHP para generar códigos JavaScript que ya están ejecutados en el lado del cliente.

  PHP es un lenguaje que se puede incrustar directamente en el código html de las páginas, que, a su vez, será procesado correctamente por el intérprete de PHP. El motor de PHP simplemente comienza a ejecutar código después de la primera secuencia de escape y continúa hasta que encuentra una secuencia de escape uniforme (Butler & Yank, 2017).

- **Python**: Este lenguaje de programación es el preferido por los especialistas en seguridad informática, que pueden automatizar pruebas para ir probando si un sistema es vulnerable (Álvarez, 2019). De igual manera se puede utilizar el lenguaje Python en el internet de las cosas para programar controladores o servidores. Pero los campos en donde es más relevante este lenguaje son la educación, la ciencia de datos y la inteligencia artificial. En la educación pues el lenguaje preferido para

enseñar a programar por ser un lenguaje sencillo. En la ciencia de datos, Python tiene librerías muy conocidas como SciPy, MunPy o Pandas. En machine learning la librería más utilizada es TensorFlow, PyTorch y Keras que es un API para el desarrollo del deeplearning utilizado por organizaciones como la NASA y el CERN.

- **C++**: Lenguaje compilado de nivel medio pues combina la programación estructurada de los lenguajes de alto nivel con la flexibilidad del ensamblador. C++ es un lenguaje de propósito general, lo que significa que no está hecho para hace de un solo dominio más aún se utiliza para resolver una amplia variedad de problemas (Grid, 2020).
- **C#**: Es uno de los lenguajes más poderosos, de rápido desarrollo y demanda en la industria de TI. En este momento, una gran variedad de aplicaciones está escritas en él, desde pequeños programas de escritorio hasta grandes portales web y servicios web que atienden a millones de usuarios todos los días.

  C# es un lenguaje con una sintaxis similar a C y está cerca en este sentido de C++ y Java. Por lo tanto, si está familiarizado con uno de estos lenguajes, será más fácil dominar C#.(Bancila, Rialdi, Sharma, & Esposito, 2020).

  Este está orientado a objetos y ha tomado mucho de Java y C++ en este sentido. Por ejemplo, C# admite polimorfismo, herencia, sobrecarga de operadores y escritura estática. El enfoque orientado a objetos nos permite resolver los problemas de construir aplicaciones

grandes, pero al mismo tiempo flexibles, escalables y extensibles. Y C# sigue desarrollándose activamente, y con cada nueva versión aparecen más y más funcionalidades interesantes.

c) Lenguaje de programación web-cliente

- **JavaScript**: El lenguaje de scripts dinámico orientado a objetos no guarda relación con Java a pesar de su nombre, aunque ambos comparten el hecho de estar escritos en C. Actualmente, JavaScript no se utiliza exclusivamente en navegadores web, sino también en microcontroladores y en servidores. Este lenguaje de programación web presenta una escritura dinámica y no tiene clases. Por ello, los programadores pueden elegir entre programación orientada a objetos, de procedimiento o funcional, lo que aporta versatilidad a este lenguaje de programación (Minnick & Holland, 2015).
- **HTML**: Lenguaje de marcado estándar para la creación de páginas web. HTML significa lenguaje de marcado de hipertexto. Este lenguaje describe la estructura de una página web. HTML consiste en una serie de elementos, los cuales le dicen al navegador cómo mostrar el contenido, están representados por etiquetas: las etiquetas HTML etiquetan partes de contenido como "encabezado", "párrafo", "tabla", etc. Los navegadores no muestran las etiquetas HTML, pero las utilizan para representar el contenido de la página.(Tent, 2020).
- **Css:** Es la tecnología principal que se utiliza para crear hermosas interfaces de usuario web, los archivos de hojas de estilo en sí

mismos suelen ser bastante feos; dejó caótico y desestructurado debido a la falta de un enfoque arquitectónico coherente. Al abordar la estructura de sus hojas de estilo de la misma manera que lo hace con el código, es posible crear reglas de estilo que sean limpias y fáciles de leer (Dowden & Dowden, 2020).

2.2.1.4 Arquitectura de aplicaciones web

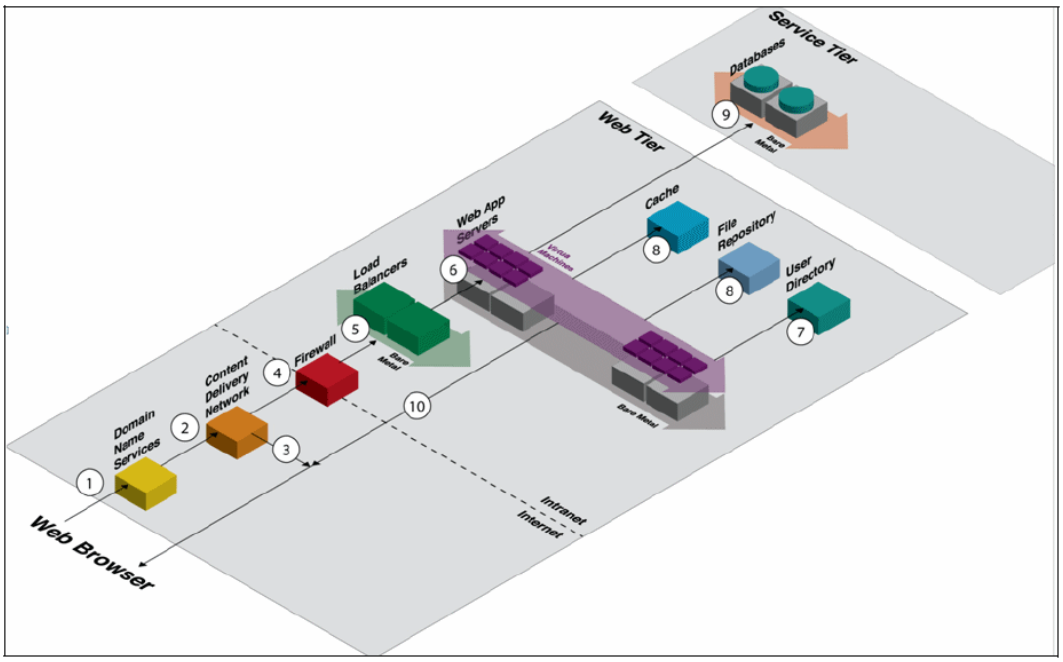


Ilustración 1: Web application hosting reference architecture. *IBM*

En la ilustración 1, para (Fred et al., 2015) los componentes de la arquitectura de referencia de alojamiento de aplicaciones web son los siguientes:

1. Domain Name Services: Las solicitudes de usuarios entrantes son manejadas inicialmente por los Servicios de nombres de dominio, que enrutan su tráfico a los puntos finales de la infraestructura adecuada.
2. Content Delivery Networks: Las redes de distribución de contenido proporcionan la menor latencia y la mayor velocidad para crear una experiencia de usuario excepcional para todo el contenido de su aplicación estática.

3. Firewalls: Los firewalls proporcionan un límite para ayudar a mantener alejados a los intrusos mientras su aplicación web funciona sin problemas.
4. Load Balancers: Los balaneadores de carga, permite la configuración y la flexibilidad para administrar el tráfico y los recursos uso de los nodos del servidor en su entorno para que ningún dispositivo se vea abrumado.
5. Web App Server: El componente del servidor de aplicaciones web es el corazón de su aplicación web, que ofrece sus servicios aplicación a los usuarios. Construya su infraestructura de servidor utilizando alto rendimiento contenedores, máquinas virtuales o tiempos de ejecución basados en Cloud Foundry, todos los cuales pueden igualmente integrado en la arquitectura.
6. User Registry Services: Los servicios de registro de usuarios permiten la autorización y autenticación para proteger los recursos a través de su aplicación.
7. Session and Data Caching: El almacenamiento en caché de datos y sesiones garantiza el acceso a datos de baja latencia y evita la pérdida de datos durante experiencia de usuario sólida. Además, con los servicios de almacenamiento, puede personalizar y tener control total sobre una solución SAN o NAS que se adapte a sus necesidades de almacenamiento.
8. Managed Database Services: Los servicios de bases de datos administradas brindan soporte de bases de datos de alto rendimiento, al tiempo que permiten que se concentre en su aplicación y no en el mantenimiento de la base de datos. Estas bases de datos varían desde bases de datos SQL estándar hasta bases de datos NoSQL más nuevas y servicios de big data.

2.2.2 Calidad de aplicaciones web

La evaluación de calidad de software web, se realiza de acuerdo a las dimensiones de contenido, la función, la estructura, usabilidad, navegabilidad, rendimiento, compatibilidad, interoperabilidad y seguridad, según (Pressman, 2010). Por otro lado, consideran que la calidad de aplicaciones web es la valuación que hacen los usuarios a las funciones del sitio web (Elbaz, 2022).

Sun et al., (2021), sugirieron cinco atributos principales, que miden la calidad de la Web: Todos estos cinco atributos forman un árbol de requisitos de calidad y se muestran en la ilustración 2.

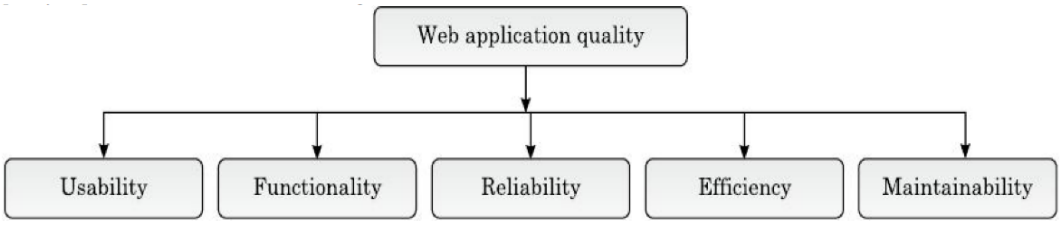


Ilustración 2: Árbol de requisitos de calidad de la aplicación web

1. Usabilidad: Incluye lo siguiente:

a) Comprensibilidad global.

b) Funciones de ayuda y comentarios online.

c) Interfaz con características estéticas.

d) Características especiales.

2. Funcionalidad: Incluye lo siguiente:

a) Capacidad de búsqueda y recuperación.

b) Funciones de navegación.

c) Funciones relacionadas con el dominio de la aplicación.

3. Fiabilidad: Incluye lo siguiente:

a) Procesamiento correcto del enlace.

b) Recuperación de errores.

c) Validación y recuperación de las entradas del usuario.

4. Eficiencia: Incluye lo siguiente:

a) Desempeño del tiempo de respuesta.

b) Velocidad para la generación de páginas

c) Velocidad para la generación de gráficas.

5. Mantenibilidad: Incluye lo siguiente:

a) Facilidad de corrección.

b) Adaptabilidad.

c) Extensibilidad.

2.2.2.1 Indicadores de calidad

Según Web.dev, los indicadores de calidad para aplicaciones web son:

- **Rendimiento:** Se hacen pruebas para garantizar que la página esté optimizada para que los usuarios puedan visualizar el contenido de la página interactuar. Algunas métricas tomadas en cuenta son: Tiempo de aparición de primer contenido, índice de velocidad, tiempo para interactuar y tiempo total de bloqueo.
- **Accesibilidad:** Se refiere a la facilidad de acceso al contenido y navegación del sitio web de manera eficaz. Algunas métricas tomadas en cuenta son: Atributo id en etiquetas no son únicos, botones no tienen un nombre accesible, múltiples etiquetas para elemento de formulario, imágenes no cuentan con descripción.

- **Mejores prácticas:** Se refiere al estado del código del sitio web. Algunas métricas tomadas en cuenta son: No usar HTTPS, uso de APIs obsoletas, imágenes con aspecto incorrecto, mostrar errores del navegador en consola.
- **Optimización de motores de búsqueda:** Se refiere al posicionamiento en motores de búsqueda. Algunas métricas tomadas en cuenta son: Elemento título del documento, etiqueta meta del sitio, texto descriptivo para enlaces.

2.2.2.2 Rendimiento y test del software de aplicación

Las pruebas de rendimiento del software se utilizan para determinar la tasa de transferencia o eficacia de una computadora, red, programa de software o dispositivo. Este proceso puede involucrar pruebas cuantitativas realizadas en un laboratorio, como medir el tiempo de respuesta o la cantidad de millones de instrucciones por segundo con el que funciona un sistema.

La prueba de rendimiento mide la capacidad de respuesta, confiabilidad, rendimiento, interoperabilidad y escalabilidad de un sistema o aplicación bajo una determinada carga de trabajo. Las pruebas pueden ser realizado en aplicaciones de software, recursos del sistema, componentes de aplicaciones específicas, bases de datos y mucho más. Normalmente implica un conjunto de pruebas automatizado, ya que esto permite simulaciones fáciles y repetibles de una variedad de cargas normales, máximas y excepcionales condiciones. Tales formas de prueba ayudan a verificar si un sistema o aplicación cumple con las especificaciones reclamadas por su proveedor. El proceso puede comparar aplicaciones en términos de parámetros como velocidad, tasa de transferencia de datos, rendimiento, ancho de banda, eficiencia o fiabilidad. Las pruebas de rendimiento también pueden ayudar como herramienta de diagnóstico a determinar los cuellos de botella y puntos únicos de

falla. A menudo se lleva a cabo en un entorno controlado y en junto con las pruebas de estrés; un proceso para determinar la capacidad de un sistema o aplicación para mantener un cierto nivel de eficacia en condiciones desfavorables (Erinle, 2017).

2.2.3 Seguridad de sitios web

La seguridad de software, es una actividad del aseguramiento del software que se centra en la identificación y evaluación de los peligros potenciales que podrían afectarlo negativamente y que podrían ocasionar que falle todo el sistema, según (Sommerville, 2005). Por otro lado, Hua, Ronald y Nathan (2005), aseguran que, en un entorno de aplicación web, la seguridad trata de proteger la confidencialidad, integridad y disponibilidad de los activos web de una organización, así como la reputación de la organización.

La garantía de la seguridad está relacionada con establecer un nivel de confianza en el sistema que podría variar desde muy bajo hasta muy alto. Para (Parnas, Van Schouwen, & Kwan, 1990), sugieren cinco tipos de revisiones para sistemas críticos de seguridad:

a) Revisión para corregir la función que se pretende.
b) Revisión para una estructura comprensible y mantenible.
c) Revisión para verificar que el algoritmo y el diseño de las estructuras de datos son consistentes con el comportamiento especificado.
d) Revisión de la consistencia del código y del diseño del algoritmo y de la estructura de datos.
e) Revisión de la adecuación de los casos de prueba del sistema

En la seguridad de sistemas informáticos web, también interviene los navegadores de acuerdo con el ranking de navegadores más utilizados con el siguiente detalle:

FUNCIONES	1	2	3	4	5	6
	Google Chrome	Safari	Firefox	Internet Explorer	Microsoft Edge	Opera
Sincronización en la nube	Si	Si	Si	No	Si	Si
Gestor de descargas	Si	Si	Si	Si	Si	Si
Navegación privada	Si	Si	Si	Si	Si	Si
Modo de pantalla completa	Si	No	Si	Si	Si	Si
Pestañas verticales	Si	No	Si	No	No	Si
Extensiones personalizadas	Si	No	Si	Si	No	Si

Desde una perspectiva de seguridad de datos, los objetivos y las fallas generalmente se definen en términos de la denominada tríada de confidencialidad, integridad y disponibilidad. La tríada CIA (de sus siglas en inglés) se puede resumir brevemente como: los datos solo deben estar disponibles para usuarios autorizados, los datos deben ser correctos y actualizados. Si uno de estos principios se rompe, generalmente se trata de un incidente de seguridad. La tríada de la CIA se aplica directamente al acceso malicioso, la alteración o la destrucción de los datos de entrenamiento del sistema de IA. Pero puede ser un poco más difícil ver cómo la tríada de la CIA se aplica a un sistema de IA que emite decisiones o predicciones, y los ataques de ML tienden a combinar las preocupaciones tradicionales de privacidad de datos y seguridad informática de manera confusa. Entonces, repasemos un ejemplo de cada uno.

La confidencialidad de un sistema de IA puede verse violada por un ataque de inversión en el que un mal actor interactúa con una interfaz de programación en aplicaciones API de manera adecuada, pero utiliza técnicas de IA explicable (XAI) para extraer información sobre su modelo y datos de entrenamiento a partir de sus

datos de entrada enviados y las predicciones de su sistema. En un ataque de inferencia de membresía más peligroso y sofisticado, se pueden extraer filas individuales de datos de entrenamiento, hasta conjuntos de datos de entrenamiento completos, de las API del sistema de IA u otros puntos finales. Tenga en cuenta que estos ataques pueden ocurrir sin acceso no autorizado a archivos de capacitación o bases de datos, pero dan como resultado los mismos daños a la seguridad y privacidad para sus usuarios o para su organización, incluidas responsabilidades legales graves.

La integridad de un sistema de IA puede verse comprometida por varios medios, como ataques de envenenamiento de datos o ataques de ejemplo adversarios. En un ataque de envenenamiento de datos, un miembro de la organización cambia sutilmente los datos de capacitación del sistema para alterar las predicciones del sistema a su favor. Solo se debe manipular una pequeña proporción de los datos de entrenamiento para cambiar los resultados del sistema, y las técnicas especializadas del aprendizaje activo y otros campos pueden ayudar a los atacantes a hacerlo con mayor eficiencia. Cuando los sistemas de IA aplican millones de reglas o parámetros a miles de funciones de entrada que interactúan, se vuelve casi imposible comprender todas las diferentes predicciones que podría hacer un sistema de IA. En un ejemplo de ataque contradictorio un atacante externo se aprovecha de mecanismos demasiado complejos al encontrar filas extrañas de datos (ejemplos contradictorios) que evocan resultados inesperados e inadecuados del sistema de IA y, por lo general, para beneficiarse a sí mismo en sus gastos.

La disponibilidad de un sistema de IA se viola cuando los usuarios no pueden acceder a los servicios que esperan. Esto puede ser una consecuencia de los

ataques anteriores que derribaron el sistema, de ataques de denegación de servicio más estándar o de discriminación algorítmica. Las personas dependen cada vez más de los sistemas de IA en su vida diaria, y cuando estos modelos se relacionan con decisiones de alto impacto en el gobierno, las finanzas o el empleo, la caída de un sistema de IA puede privar a los usuarios de servicios esenciales. Lamentablemente, muchos sistemas de IA también exhiben discriminación errónea en los resultados y la precisión de los grupos demográficos históricamente marginados. Es menos probable que las minorías experimenten los mismos niveles de disponibilidad de ofertas de crédito automatizadas o escáneres de currículum. Más directamente aterrador, es más probable que experimenten predicciones defectuosas por parte de los sistemas de reconocimiento facial, incluidos los que se utilizan en contextos de seguridad o aplicación de la ley.

Estas son solo algunas de las formas en que un sistema de IA puede experimentar problemas de seguridad.

2.2.3.1 Principales ataque web y sus contramedidas

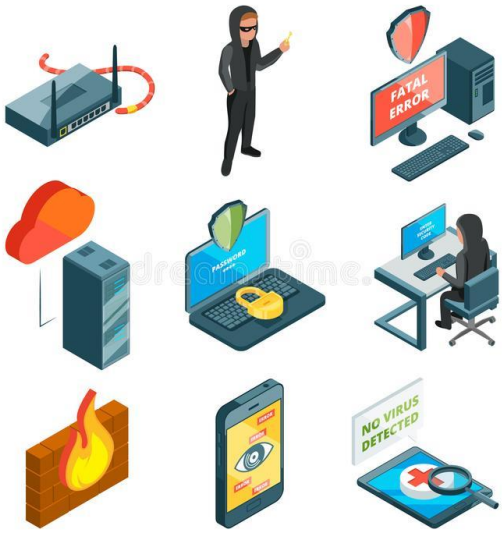
Para (Gutiérrez del Moral, 2014), en este mundo globalizado mediante el uso de internet, necesariamente se debe implementar contramedidas a los ataques de ciberseguridad, como:

- Seguridad en aplicaciones web
- Protocolo http
- Vulnerabilidad XSS
- Vulnerabilidad CSRF
- Path traversal

- Null byte
- OS commanding
- LFI (Local file inclusión)
- RFI (Remote file inclusión)
- Informationn disciosure
- SQL injection

Ilustración 3:

Símbolo utilizados para fomentar la seguridad



2.2.3.2 Control de seguridad de sitios web

La seguridad puede considerarse lo más importante para probar porque sea lo que sea que nosotros y nuestros usuarios estamos haciendo, si la seguridad de la misma se ve comprometida, nosotros y nuestros usuarios estamos comprometidos y pueden ser dañados de varias maneras, desde la pérdida de datos (y la privacidad) a la pérdida del servicio en sí, y posiblemente mucho más. Nos mantenemos y caemos con la seguridad de los servicios que ofrecemos. La seguridad es fundamental, pero también es difícil a la luz del control de calidad del sitio web. Por un caso, los sitios

web, en lugar de las aplicaciones, podrían o no tratar con ninguna información personal y confidencial o incluso pedir a sus usuarios que proporcionen dicha información. Por otro, la seguridad no es trivial de probar y no necesariamente se evalúa todo desde el exterior. Esto nos lleva a la situación en la que, aunque la seguridad es tan crucial, no hay mucho que agregar fuera del contexto de seguridad de la información dedicada (Meiert, 2016).

2.2.3.3 Indicadores de seguridad de sitios web

Según la documentación proporcionada por webhint.io, herramienta empleada durante la presente investigación, se definen los indicadores de la siguiente manera:

- **disown-opener:** disown-opener comprueba si el atributo rel se especifica con los valores noopener y noreferrer (o solo noopener si todos los navegadores específicos lo admiten) en los elementos a y area que tienen target = "_ blank" y enlazan a otros orígenes.
- **https-only:** HTTPS es importante para garantizar la integridad del contenido. Incluso cuando su sitio no tiene información confidencial, un atacante puede cambiar el contenido o inyectar scripts maliciosos (como un minero criptográfico para usar la potencia de la CPU de su usuario).
- **no-disallowed-headers:** Es importante no enviar encabezados que a menudo son configurados por servidores, frameworks y lenguajes del lado del servidor (por ejemplo: ASP.NET, PHP), que por defecto tienen valores que contienen información sobre la tecnología que los configura: su nombre, número de versión, etc; debido a que no aportan a la experiencia

del usuario y expone información a posibles atacantes sobre la pila de tecnología que se está utilizando

- **no-protocol-relative-urls:** advierte contra el uso de URL relativas al esquema (comúnmente conocidas como URL relativas al protocolo). Si se utilizan URL relativas al protocolo para enlaces CDN, su dominio no está en la lista de precarga HSTS del navegador y la primera solicitud no se realiza a través de HTTP, existe un alto riesgo de ataques de intermediario.
- **sri:** Significa integridad de los subrecursos (Sub-resource integrity). Este indicador advierte sobre la solicitud de scripts u hojas de estilo sin utilizar la integridad de los recursos secundarios. Una práctica común en el desarrollo web moderno es utilizar recursos de terceros de CDN o diferentes servicios (análisis, anuncios, etc.). Sin embargo, hacerlo puede aumentar la superficie de ataque de su sitio web / aplicación.
- **strict-transport-security:** Este indicador advierte contra el uso de recursos sin HTTPS. Es importante debido a que si un sitio web acepta una conexión a través de HTTP y luego redirige a HTTPS, abre oportunidades para un ataque "man-in-the-middle", cuando la redirección podría ser explotada y llevar al usuario a un sitio malicioso.
- **validate-set-cookie-header:** Este indicador valida el encabezado set-cookie y confirma que las directivas Secure y HttpOnly se establecen cuando se envían desde una fuente segura (HTTPS).
- **x-content-type-options:** Este indicador verifica que todos los recursos se proporcionen con el encabezado de respuesta HTTP X-Content-Type-Options: nosniff. Es importante debido a que el sitio web / la aplicación

puede ser expuesto a ataques basados en confusión de tipo MIME que provocan problemas de seguridad, especialmente en el caso de servidores que alojan contenido que no es de confianza.

- **no-vulnerable-javascript-libraries:** Este indicador comprueba las vulnerabilidades conocidas dentro de las bibliotecas y marcos de JavaScript del lado del cliente detectados en un sitio web.
- **ssllabs:** Denominado prueba del servidor SSL. Este indicador es importante debido a que realiza un profundo de la configuración SSL del sitio mediante la prueba del servidor SSL de SSL Labs.

2.2.4 Inteligencia artificial

La inteligencia artificial (IA) es un conjunto de herramientas tecnológicas y algoritmos que nos brindan predicciones, recomendaciones y decisiones sobre cambios en el mundo digital y real, en base a diversos datos. En general, debe realizar tareas que antes se pensaba que solo podían realizar los humanos.

La IA consta de dos subconjuntos principales: aprendizaje automático (ML) y aprendizaje profundo (DL). El punto de ambos es aprender a distinguir entre cosas diferentes. Es fácil para nosotros como humanos hacer esto incluso sin tener una comprensión clara de qué procesos biológicos están teniendo lugar en nuestro cerebro en este momento. Las máquinas hacen esto gracias a ML y DL (Miranda, 2015)

La inteligencia artificial es una técnica que permite a las máquinas aprender y trabajar de forma independiente. El potencial para la adopción de IA es enorme y las empresas se están dando cuenta.

2.2.4.1 Machine learning

El aprendizaje automático o machine learning es una rama de la inteligencia artificial (IA) que busca ayudar a los sistemas a aprender por sí mismos en base a los datos sin ninguna intervención humana manifiesta. ML usa diferentes algoritmos que usan datos para descubrir cómo mejorar, predecir y describir los datos.

El aprendizaje profundo es un tipo de inteligencia artificial y un método de aprendizaje automático basado en el concepto de redes neuronales artificiales. Estas redes ayudan a las máquinas a aprender en base a datos, especialmente de los datos no estructurados. Se utiliza con mayor frecuencia en visión por computadora, imagen como también reconocimiento de voz.

2.2.4.2 Tipos de aprendizaje

El Machine Learning o Aprendizaje Automático es un tipo de inteligencia artificial (IA) que proporciona a las computadoras la capacidad de aprender, sin ser programadas explícitamente. Este aprendizaje se centra en el desarrollo de programas informáticos que pueden cambiar cuando se exponen a nuevos datos (Muzaffar et al., 2022).

Dentro del Machine Learning existen tres enfoques para aprender, el aprendizaje supervisado, aprendizaje no supervisado y aprendizaje por reforzamiento (Ashtari et al., 2022).

a) Aprendizaje supervisado

El aprendizaje supervisado generalmente comienza con un conjunto establecido de datos y una cierta comprensión de cómo se clasifican esos datos; por ejemplo, si le damos abundante información de imágenes de animales

(perros y gatos), y etiquetamos cada imagen como perro o gato, entonces el sistema aprenderá a identificar un gato o un perro en otra imagen cualquiera distinta con la que fue entrenado (Hurwitz & Kirsh, 2018)

Como vimos anteriormente, el aprendizaje supervisado está destinado a encontrar patrones en los datos que correspondan a una etiqueta que define el significado de los datos; por ejemplo, podría haber millones de imágenes de animales e incluir una explicación de qué es cada animal y luego puede crear una aplicación de aprendizaje automático que distinga a un animal de otro.

Existes dos tipos principales de problemas del Aprendizaje Automático supervisado, denominados clasificación y regresión (Andreas y Sarah, 2017).

Hurwitz & Kirsh (2018) afirman que cuando la etiqueta es constante, es una regresión; y cuando los datos provienen de un conjunto finito de valores, se conoce como clasificación. En esencia, utilizar la regresión para el aprendizaje supervisado lo ayuda a comprender la correlación entre las variables. Un ejemplo de aprendizaje supervisado, mediante el uso del análisis de regresión, es el pronóstico del tiempo; el pronóstico del tiempo tiene en cuenta los patrones climáticos históricos conocidos y las condiciones actuales para proporcionar una predicción sobre el clima y otro ejemplo de aprendizaje supervisado, mediante el uso de análisis de clasificación sería la clasificación de animales.

b) Aprendizaje no supervisado

El aprendizaje no supervisado es más adecuado cuando el problema requiere una gran cantidad de datos sin etiqueta; por ejemplo, le damos abundante información de imágenes de (gatos y perros), pero no le decimos al sistema que

son gatos o perros, por lo que la comprensión del significado detrás de estas imágenes, requiere algoritmos que puedan comenzar a comprender el significado de las imágenes para poder clasificar los “gatos o perros” en cualquier otra imagen.

c) Aprendizaje por reforzamiento

El aprendizaje por reforzamiento es un modelo de aprendizaje conductual, donde el algoritmo recibe retroalimentación del análisis de los datos para que el usuario sea guiado hacia el mejor resultado; es decir, se aprende con estímulos de ponderación alta si se acerca al objetivo o ponderaciones menores si comete errores (Hurwitz y Kirsch, 2018).

2.2.4.3 Modelos de machine learning

Esta área de estudio ha recibido multitud de definiciones a lo largo del tiempo. (El Naqa, Li, & Murphy, 2015), lo define como un campo de estudio que dota a las computadoras la habilidad de aprender sin estar explícitamente programada. De igual forma Ethem Alpaydin (como se citó en Naqa, Li y Murphy, 2015) indica que machine learning es el campo de la programación de computadoras para optimizar algún criterio de rendimiento usando datos de ejemplo o experiencia pasada.

Los modelos de regresión de machine learning que se utilizaron para el entrenamiento fueron:

a) Regresión lineal bayesiana
b) Regresión del árbol de decisiones impulsada
c) Decisión Regresión forestal
d) Regresión lineal
e) Regresión de la red neuronal

2.2.4.4 Métricas de machine learning

Las métricas devueltas para los modelos de regresión generalmente están diseñadas para estimar la cantidad de error. Un modelo se considera que se ajusta bien a los datos si la diferencia entre los valores observados y los pronosticados son pequeños. Sin embargo, mirando en el patrón de los residuos (la diferencia entre cualquier punto predicho y su correspondiente real valor) puede decirle un sesgo potencial sobre el modelo (Lopez, 2018)

El error absoluto medio (MAE: Mean absolute error)

Mide qué tan cerca están las predicciones de los resultados reales; por lo tanto, un menor puntaje es mejor. Se calcula como la sumatoria de valor absoluto de la diferencia entre el valor absoluto y estimado, multiplicado por la inversa del tamaño de la muestra.

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \widehat{y_i}\,|$$

Donde:

n = Tamaño de la muestra

y_i = Valor real

$\widehat{y_i}$ = Valor estimado

El error cuadrático medio (RMSE: Root mean squared error)

Crea un valor único que resume el error en el modelo. Es la sumatoria por cuadrado de la diferencia entre los valores reales y estimados, multiplicado por la inversa de del tamaño de la muestra, la métrica ignora la diferencia entre la predicción excesiva y la predicción insuficiente.

$$RSME = \sqrt{\frac{\sum_{i=1}^{n}\left(y_i - \widehat{y_i}\right)^2}{n}}$$

n = Tamaño de la muestra

y_i = Valor real

$\widehat{y_i}$ = Valor estimado

El error absoluto relativo (RAE: Relative absolute error)

Es una diferencia absoluta relativa entre los valores esperados y reales; relativo porque la diferencia de medias se divide por la media aritmética.

$$RAE = \frac{\sum_{i=1}^{n}\left|y_i - \widehat{y_i}\right|}{\sum_{i=1}^{n}\left|\bar{y} - y_i\right|}$$

Donde:

n = Tamaño de la muestra

y_i = Valor real

$\widehat{y_i}$ = Valor estimado

$\bar{y}$ = Promedio valor real

El error al cuadrado relativo (RSE: Relative squared error)

Normaliza de manera similar el error al cuadrado total de los valores predichos por dividiendo por el error cuadrado total de los valores reales.

$$RSE = \frac{\sum_{i=1}^{n}\left(y_i - \widehat{y_i}\right)^2}{\sum_{i=1}^{n}\left(\bar{y} - y_i\right)^2}$$

Donde:

n = Tamaño de la muestra

y_i = Valor real

$\widehat{y_i}$ = Valor estimado

$\bar{y}$ = Promedio valor real

El coeficiente de determinación (R2)

a menudo denominado R^2, representa el poder predictivo del modelo como valor entre 0 y 1. Cero significa que el modelo es aleatorio (no explica nada); 1 significa que hay un ajuste perfecto. Sin embargo, se debe tener precaución al interpretar los valores de R, ya que los valores bajos pueden ser totalmente normales y altos. Los valores pueden ser sospechosos.

$$R^2 = 1 - \frac{\sum_{i=1}^{n}\left(y_i - \widehat{y}_i\right)^2}{\sum_{i=1}^{n}\left(y_i - \overline{y}_i\right)^2}$$

$$R^2 = 1 - \frac{MSE_p}{MSE_M}$$

Donde:

n = Tamaño de la muestra

y_i = Valor real

$\widehat{y}_i$ = Valor estimado

$\bar{y}$ = Promedio valor real

MSE_p = Error cuadrático medio de los valores estimados

MSE_M = Error cuadrático medio de la muestra

2.2.4.5 Deep learning

El Deep Learning, el Machine Learning y la Inteligencia Artificial, son conceptos que están íntimamente ligado, como subconjuntos como se muestra en la figura 1 (Chollet, 2018).

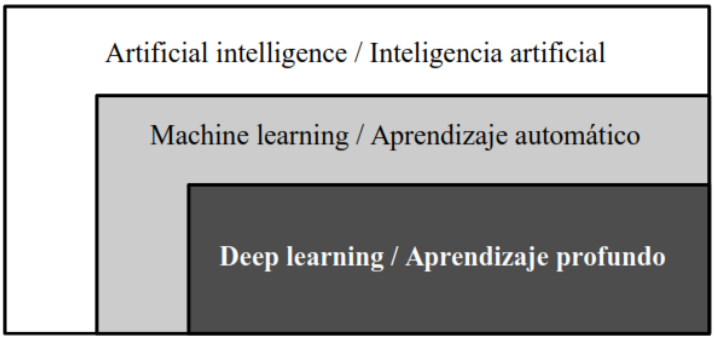
Artificial intelligence / Inteligencia artificial

Machine learning / Aprendizaje automático

Deep learning / Aprendizaje profundo

Ilustración 2:

Inteligencia Artificial, Machine Learning y Deep Learning



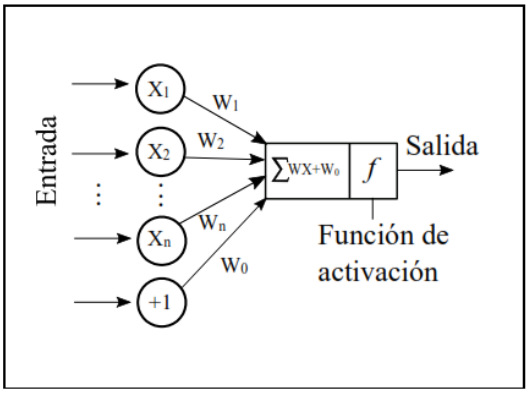
2.2.4.6 Redes Neuronales Artificiales (RNA)

Ponce (2010) afirma que las RNA se definen como sistemas de mapeos no lineales cuya estructura se basa en principios observados en los sistemas nerviosos de humanos y animales.

La idea detrás de una Red Neuronal Artificial es simular el comportamiento de una red neuronal biológica. Para ello se emula con fórmulas matemáticas una neurona a la que le van a llegar señales de entrada con distintos pesos, que se sumarán, y se emitirá una señal de salida que dependerá de una determinada función de activación como se muestra en la Ilustracion 2 (Ponce, 2010).

Ilustración 2

Neurona Artificial



Existen diferentes tipos de funciones de activación las más relevantes para esta investigación son: Sigmoid (Sigmoide) y ReLU (Rectified Lineal Unit).

Sigmoid: $f(x) = \frac{2}{1+e^{-2x}} - 1$

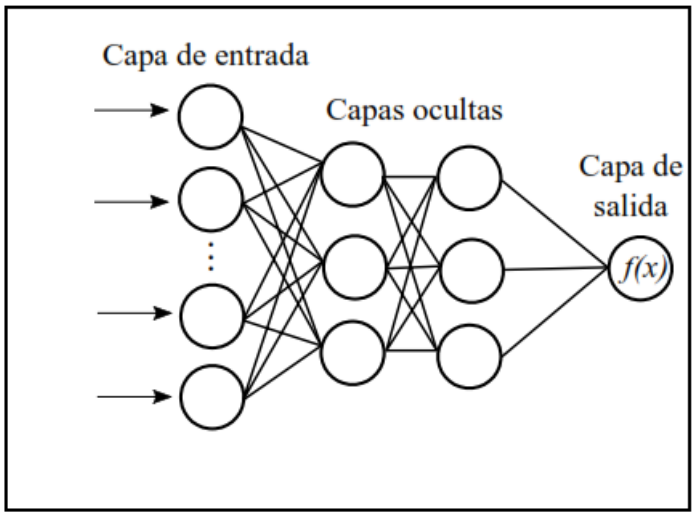
ReLU: $f(x) = \max(0, x) = \begin{cases} 0 \; for \; x < 0 \\ x \; for \; x \geq 0 \end{cases}$

Una red neuronal artificial estará formada por un conjunto de neuronas, y que se somete a un proceso de aprendizaje, para enseñarle a reconocer formas (clasificación) o hacer predicciones (Regresión).

La función ReLU se usa en las capas de entrada y ocultas; mientras que, en la capa de salida se usa la función Sigmoid para la identificación de personas.

Ilustración 3:

Red Neuronal Artificial



Cada unidad recibe entradas de otros nodos y genera una salida simple escalar que depende de la información local disponible, guardada internamente o que llega a través de las conexiones con pesos. Pueden realizarse muchas funciones complejas dependiendo de las conexiones.

2.3 Marco conceptual

Modelo predictivo

Es un sistema, que explota ciencia de datos para la predicción de resultados a partir de un modelo de datos.

Métricas de predicción

Es la evaluación y realización de los modelos de aprendizaje automático

Algoritmos de aprendizaje automático

Es parte de inteligencia artificial que proporciona a las computadoras la capacidad de aprender, sin ser programadas explícitamente, utilizando algoritmos supervisados, semi-supervisados, no supervisados y de refuerzo.

Machine learning

El aprendizaje automático, se puede describir como sistemas informáticos que mejoran con la experiencia. También puede ser descrito como un método para convertir datos en software (Barnes, 2015).

ChatBot

Programa de computadora que usa una técnica de aprendizaje automático reconocimiento de voz y lenguaje natural procesamiento (NLP) para llevar a cabo una conversación inteligente con una persona (Jimenez, Jimenez, Jimenez, & Jimenez, 2020).

Dominios de seguridad

Son configuraciones de autenticación, mapeo de seguridad y auditoria propia del servidor de aplicaciones e implementan la especificación JAAS (Java authentication and authorization service) de seguridad declarativa (Candel, 2019).

Calidad sitios web

Implica los medios para determinar, si cumplen con nuestras expectativas y en qué grado nuestros sitios web cumplen con las mejores prácticas profesionales.

Accesibilidad

Diseño de productos, dispositivos, servicios o entornos para personas o usuarios.

CAPÍTULO III
MÉTODO

3.1 Tipo de investigación

- Propósito : Aplicada científica
- Alcance o nivel : Predictiva
- Objeto de estudio según variables: Experimental puro
- Fuente de datos : Documental y de campo
- Estudio de las variables : Cuantitativas
- Fuente de información : Secundaria
- Tiempo de medición variables : Sincrónica
- Toma de datos : Retrospectiva
- Medición de variables : Transversal
- Según método lógico : Hipótesis-deductiva Ex post facto
- Área : TICs y Sistemas cognitivos

3.2 Diseño de la investigación

La investigación experimental es un enfoque científico de la investigación, donde una o más variables independientes se manipulan y se aplican a una o más

variables dependientes para medir su efecto sobre estas últimas. El efecto de las variables independientes sobre las variables dependientes se suele observar y registrar sacar una conclusión razonable sobre la relación entre estos 2 tipos de variables (Montgomery, 2005).

El diseño para experimentos puros según (Sampieri, 2018), R es random o aleatorio, G_1 grupo experimental, G_2 grupo de control, X es el estímulo, O_1 y 0_3 observaciones pre test, O_3 y 0_4 , observaciones post test y - sin estímulo, como se observa en la ilustración 2.

Ilustración 4:

Diseño de un experimento puro con pretest y post test

Grupo experimental	RG_1	O_1	X	O_2
Grupo de control	RG_2	O_3	-	O_4

3.3 Población y muestra

En la tabla de información uno, se muestra una población finita para el estudio de seguridad datos web de universidades del Perú, año 2020.

Tabla 1
Población de Universidades públicas y privadas del Perú

UNIVERSIDADES	TOTAL	NIC (%)
Privadas asociativas	40	27,97
Privadas societarias	52	36,6
Públicas	50	35,66
Total	142	100,00

De dicha población, se seleccionó una muestra representativa mediante la técnica de muestreo probabilística simple. Para determinar el tamaño de la muestra se aplicó la fórmula siguiente: (Sierra, 1991)

$$n = \frac{Z^2\ P\ Q\ N}{E^2(N-1) + Z^2\ P\ Q} \quad (1)$$

Dónde:

N = Tamaño de la población

n = Tamaño de la muestra necesaria

$Z^2 = (1{,}96)^2$

P = Probabilidad de que el evento ocurra 50%

Q = Probabilidad de que el evento no ocurra 50%

E = $0{,}05\ \ o\ 5\%$

Reemplazando valores en la ecuación 1:

$$n = \frac{(1{,}96)^2(0{,}5)(0{,}5)(142)}{(0{,}05)^2(142-1) + (1{,}96)^2(0{,}5)(0{,}5)} = 104$$

Tabla 2
Distribución de la población muestreada en grupos

UNIVERSIDADES	G1	G2	TOTAL
Públicas	18	18	36
Privadas societarias	19	19	38
Privadas asociativas	15	15	30
Total	52	52	104

La muestra de 104 Universidades se distribuyó en dos grupos, donde, el grupo experimental es G1 y el grupo no experimental fue G2, cada grupo estuvo

conformado por 52 universidades Públicas y Privadas, como se apreciar en la tabla 2.

3.4 Técnicas e instrumentos de recolección de datos

3.4.1 Técnica

- Análisis documental: Fuentes secundarias (Textos, artículos y otros)
- Observación experimental

3.4.2 Descripción de los instrumentos de recolección de datos

Calidad de aplicaciones web

La evaluación de la calidad de aplicaciones web en las universidades del Perú, se calificó por Universidades Asociativas, Societarias y Públicas.

Tabla 3

Codificación de los niveles de la calidad de aplicaciones web

Código	Intervalo	Nivel	Indicador	Universidades
1	90 – 100	Bueno	• Rendimiento • Accesibilidad • Buenas prácticas • SEO	• Asociativas • Societarias • Públicas
2	50 – 89	Necesita Mejorar		
3	0 - 49	Deficiente		

Nota: https://developers.google.com/web escoger herramienta web.dev

La tabla 3 presenta los indicadores de rendimiento, accesibilidad, buenas prácticas y SEO, se evaluaron en los niveles bueno si el resultado estaba en el intervalo de 90 a 100 y se asignó código 1. El nivel necesita mejorar, si el resultado estaba en el intervalo de 50 a 89 y se asignó código 2. Finalmente, el nivel deficiente, si el resultado fue en el intervalo entre 0 a 49 y el código asignado fue 3, (Goolge, 2020).

Tabla 4

Codificación de los niveles de seguridad de sitios web

Código	Seguridad	Nic Seguridad	Nivel	Indicador
1	9,0 – 10,0	90 – 100	Bueno	
2	5,0 – 8,9	50 – 89	Necesita Mejorar	• Seguridad del sitio web
3	0 – 4,9	0 – 49	Deficiente	

Nota: https://developer.microsoft.com/es-es/microsoft-edge/tools/ escoger herramienta webhint

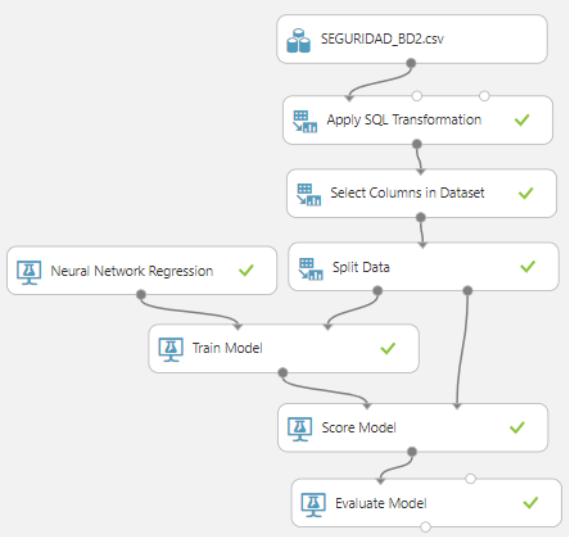
En la tabla 4, se observa la codificación del indicador Seguridad de sitios web para las Universidades Peruanas. El nivel deficiente se codificó como 1 en un intervalo de puntuación de 9,0 a 10,0 y en términos porcentuales entre 90 a 100. Se codificó como 2 al nivel se necesita mejorar en intervalo de puntuación de 5,0 a 8,9 y entre 50 a 89 en términos porcentuales. El nivel bueno se codificó como 3, en el intervalo de puntuación entre 0 a 4,9 y en porcentuales fue 0 a 49, (Microsoft, 2020).

Machine learning

En la ilustración 2, se muestran los módulos básicos que fueron utilizados en el modelo predictivo con machine learning.

Ilustración 5

Modelo básico de machine learning



A continuación de describen, el funcionamiento de cada módulo de machine learning:

a) Seguridad_BD2.cvs

La base de datos contiene la población de N = 142 registros de las Universidades del Perú con la información detallada de las variables de investigación en el formato csv (Comma separated values), es decir, cada registro está separado por comas (,).

b) Apple SQL transformation

Se realizaron dos consultas a la base de datos con N = 142 Universidades con Apple SQL transformation:

- Selección del tipo de Universidad de la tabla t1 y TIPO

  /*Select * from t1 where t1.TIPO = 'ASOCIATIVA'*/;

  /*Select * from t1 where t1.TIPO = 'SOCIETARIA'*/;

  /*Select * from t1 where t1.TIPO = 'PUBLICA'*/;

  Select * from t1; /*TODAS LAS UNIVERSIDADES*/;

- Selección de la muestra de Universidades de la tabla t1 en un intervalo por tipo de Universidad y las muestras de población (n).

  /*Select * from t1 LIMIT 0, 30*/; /*ASOCIATIVA n = 30 */;

  /*Select * from t1 LIMIT 0, 38*/; /*SOCIETARIA n = 38 */;

  /*Select * from t1 LIMIT 0, 36*/; /*PUBLICA n = 36 */;

  Select * from t1 LIMIT 0, 104; /TODA LA MUESTRA n = 104 */

c) Select columna in Dataset

Es un módulo para elegir un subconjunto de columnas para usar en operaciones posteriores. Se seleccionó las opciones sin columna, include, nombre de las

columnas: PERFOMANCE, ACCESSIBILITY, BEST PRACTICES, SEO, HINTs y PASSED.

d) Split Data

El módulo se utiliza para dividir datos aleatoriamente (Randomize) de un conjunto de datos en dos conjuntos distintos conjuntos de entrenamiento experimental (G1) al 50% y grupo de control (G2) también al 50%.

e) Neural Network Regression

El módulo crea un modelo de regresión mediante un algoritmo de red neuronal personalizable. La regresión de redes neuronales es un método de aprendizaje supervisado y, por lo tanto, requiere un conjunto de datos etiquetado, que incluye una columna de etiqueta. Dado que un modelo de regresión predice un valor numérico, la columna de etiqueta debe ser un tipo de datos numéricos.

f) Train Model

Genera predicciones mediante un modelo de regresión o clasificación entrenado. Se seleccionó las opciones sin columna, include, nombre de la columna: PASSED para la predicción de seguridad de sitios web.

g) Score Model

Adjunta al experimento, un modelo entrenado desde Train Model y un conjunto de datos que contenga nuevos datos de entrada proveniente de Split data, el cincuenta por ciento del grupo de control (G2) del experimento no entrenado.

h) Evaluate Model

Su uso es para medir la precisión de uno o dos modelos entrenados. Proporcionas un conjunto de datos que contiene puntuaciones generadas: Mean Absolute Error, Root Mean Squared Error, Relative Absolute Error, Relative

Squared Error y Coefficient of Determination a partir de un modelo, calculando un conjunto de métricas de evaluación.

i) Execute R Script

Reporta en una única interfaz, los resultados de varios modelos de experimentos entrenados. Las instrucciones dadas fueron:

```
dataset1 <- maml.mapInputPort(1) # class: data.frame
dataset2 <- maml.mapInputPort(2) # class: data.frame
data.set = rbind(dataset1, dataset2);
plot(data.set);
maml.mapOutputPort("data.set");
```

Métricas de machine learning

Para evaluar, los algoritmos de machine learning, se utilizaron las siguientes métricas:

Métrica	Significado de la métrica	Modelo formal de la métrica
MAE	El error absoluto medio	$MAE = \frac{1}{n}\sum_{i=1}^{n}\lvert y_i - \hat{y_i}\rvert$
RMSE	El error cuadrático medio	$RSME = \sqrt{\frac{\sum_{i=1}^{n}(y_i - \hat{y_i})^2}{n}}$
RAE	El error absoluto relativo	$RAE = \frac{\sum_{i=1}^{n}\lvert y_i - \hat{y_i}\rvert}{\sum_{i=1}^{n}\lvert \bar{y} - y_i\rvert}$
RSE	El error al cuadrado relativo	$RSE = \frac{\sum_{i=1}^{n}(y_i - \hat{y_i})^2}{\sum_{i=1}^{n}(\bar{y} - y_i)^2}$
R^2	Coeficiente de determinación	$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_i - \hat{y_i})^2}{\sum_{i=1}^{n}(y_i - \bar{y_i})^2}$ $R^2 = 1 - \frac{MSE_p}{MSE_M}$

En la tabla 5, se muestra el modelo de (Altman & York, 1991), cinco categorías sobre índice kappa, por tanto, las interpretaciones de los resultados de predicción con algoritmos de aprendizaje automático, serán bajo esta clasificación, por ser más completa.

Tabla 5

Métricas de machine learning e interpretación del índice Kappa

Código	Algoritmo	Métricas	Valor k	Concordancia
1	Bayesian linear regression	• MAE • RMSE • RAE • RSE • R^2	0,0 - 0,20	Pobre
2	Decision Forest Regression		0,21 - 0,40	Débil
3	Linear regression Neural Network Regression		0,41 - 0,60	Moderada
4	Boosted Decision Tree		0,61 - 0,80	Buena
5	Regression		0,81 - 1,00	Muy buena

Cada uno de los algoritmos de machine learning, fueron evaluados de acuerdo con las métricas MAE (El error absoluto medio), RMSE (El error cuadrático medio), RAE (El error absoluto relativo), RSE (El error al cuadrado relativo) y R^2 (Coeficiente de determinación) previamente entrenados utilizando software especializado. Se seleccionó solamente un algoritmo entre los propuestos de acuerdo con la interpretación del índice Kappa. Si, la métrica de machine learning R^2, está ubicado en el intervalo 0,61 a 0,80 entonces la concordancia es buena. Si, la concordancia fue muy buena entonces la métrica R^2 se ubicó en el intervalo 0,81 a 1,00. Preferentemente se seleccionó a aquel algoritmo que presente el índice Kappa de concordancia muy buena para la predicción, como se muestra en la tabla 4.

3.5 Técnicas de procesamiento y análisis de datos

3.5.1 Procesamiento de datos

a) Tabla de métricas de aprendizaje automático

b) Histogramas

c) Circulares

3.5.2 Análisis estadístico de los datos

En cuanto al análisis de las variables de investigación, se utilizaron métricas para la evaluación de los modelos predictivos de machine learning, análisis de varianza (ANOVA) y t-student para la prueba de hipótesis, se presentan las tablas de distribución estadística en el anexo 8.

3.5.2.1 Prueba de hipótesis

Para su demostración se formuló un procedimiento de cinco pasos que sistematiza la prueba de hipótesis según (Lind, Mason, & Marchal, 2004):

a) Plantear las hipótesis nula y alternativa H_0 y H_1

Predicción con algoritmo entrenado	Modelo predictivo Machine learning
H_0: $\mu_x = \mu_y$	H_0: $W_i = 0$; *i= 0, 1, 2, 3, 4 y 5*
H_1: $\mu_x \neq \mu_y$	H_1: $W_i \neq 0$

b) Selección del nivel de significancia

$\alpha = 0{,}05$

c) Seleccionar estadístico de prueba de hipótesis

c.1. T-Student para algoritmo entrenado

Prueba o datos	Tratamiento de seguridad web	
	A	B
1	Y_{A1}	Y_{B1}
2	Y_{A2}	Y_{B2}
3	Y_{A3}	Y_{B3}
…		
n	Y_{An}	Y_{Bn}

$$t_0 = \frac{\overline{X} - \overline{Y}}{\hat{S}_R^2 \sqrt{\frac{1}{n_x} + \frac{1}{n_y}}} \quad (2)$$

$$gl = n_x + n_y - 2$$

Donde:

gl = Grados de libertad

$\hat{S}_R^2$ = Varianza residual, representado por la ecuación 3.

$\overline{X}$ = Promedio con proceso o tratamiento X = A

$\overline{Y}$= Promedio con proceso o tratamiento Y = B

n_x = Muestras aleatorias del proceso X

n_y = Muestras aleatorias del proceso Y

$$\hat{S}_R^2 = \frac{n_x - 1}{n - 2}\hat{S}_1^2 + \frac{n_y - 1}{n - 2}\hat{S}_2^2 \quad (3)$$

c.2 Análisis de varianza para el modelo predictivo machine learning basado en pesos (W) de la ecuación 4.

$$\hat{y}_i = W_0 + W_1 x_{1i} + W_2 x_{2i} + \ ... + W_K x_{Ki} + \varepsilon_i \quad (4)$$

Fuentes de variación	Suma de cuadrados	Grados de libertad	Varianzas	F	Valor-p
Explicada	$\sum(\hat{y}_i - \bar{y})^2$	k	$\hat{S}_E^2$	$\hat{S}_E^2 / \hat{S}_R^2$	
Residual	$\sum(y_i - \hat{y}_i)^2$	n-k-1	$\hat{S}_R^2$		
Total	$\sum(y_i - \bar{y})^2$	n-1			

d) Regla de decisión

T-Student

$$Aceptar\ Modelo\ predictivo\ machine\ learning =$$

$$\begin{cases} H_0: Si,\ Valor - p > \alpha; \\ H_1: Si,\ \ Valor - p < \alpha \end{cases}$$

Análisis de varianza

$$Aceptar\ pesos\ de\ aprendizaje(W) = \begin{cases} H_0: Si, & Valor - p > \alpha \\ H_1: Si, & Valor - p < \alpha \end{cases}$$

e) Toma de decisión

Aceptar o rechazar hipótesis nula

CAPÍTULO IV

PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

4.1 Presentación de resultados por variables

4.1.1 Calidad de aplicaciones web

Los resultados del grupo experimental (G1) y grupo de control (G2) de la variable de investigación calidad de aplicaciones web de las universidades peruanas, fueron evaluados los indicadores Perfomance, accesibility, Best-practices y Seo en las categorías deficiente, necesita mejorar y bueno.

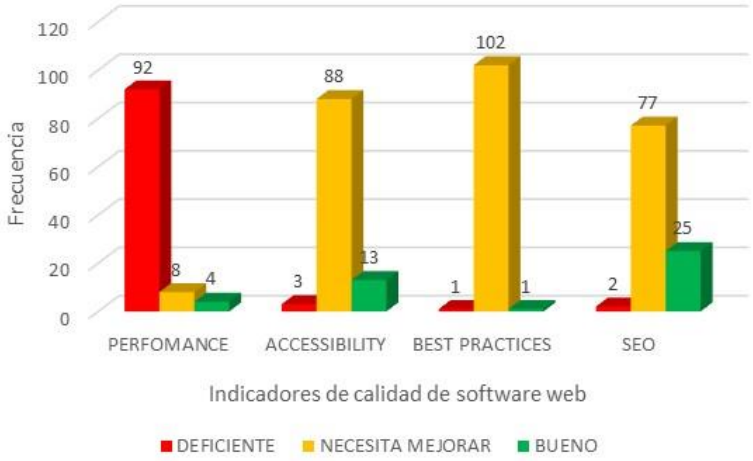
Tabla 6

Calidad de aplicaciones y los indicadores categorizados

Categoria	Performance	Accesibility	Best-Practices	Seo	Total
Deficiente	92 88,46%	3 2,88%	1 0,96%	2 1,92%	98 23,56%
Mejorar	8 7,69%	88 84,62%	102 98,08%	77 74,04%	275 66,11%
Bueno	4 3,85%	13 12,5%	1 0,96%	25 24,04%	43 10,34%
Total	104 100%	104 100%	104 100%	104 100%	416 100%

Ilustración 6

Frecuencia de los indicadores de calidad web de las Universidades Peruanas



En la ilustración 4 y tabla 6, los indicadores de calidad web que predominan en perfomance fue la categoría deficiente con 92 que representa al 88,46% de Universidades. En accesibility predomina la categoría necesita mejorar con 88 que representa al 84,62% de Universidades. Asimismo, en best-practices, predomina la categoría necesita mejorar con 102 que representa al 98,08% de Universidades y finalmente en el indicador Seo, predomina la categoría necesita mejorar con 77 que representa al 74,04% por tanto el 66,11% Universidades Peruanas están en la categoría mejorar o regular.

4.1.2 Seguridad de sitios web

Tabla 7

Frecuencia de falla en la seguridad por indicadores de las Universidades del Perú

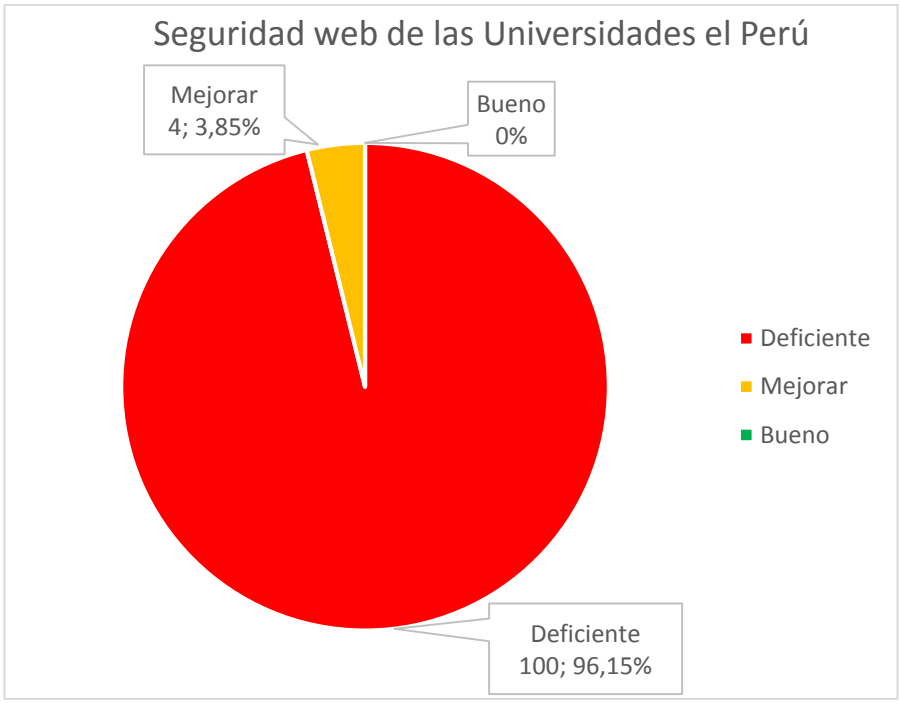
Indicador	Sugerencias	Nivel de seguridad		
		Deficiente	Mejorar	Bueno
1. disown-opener	95 9,13%			
2. https-only	57 5,48%			
3. no-disallowed-headers	102 9,81%	100	4	0
4. no-protocol-relative-urls	75 7,21%			
5. sri	93 8,94%			
6. strict-transport-security	99			

	9,52%			
7. validate-set-cookie-header	64 6,15%			
8. x-content-type-options	103 9,90%			
9. no-vulnerable-javascript-libraries	96 9,23%			
10. ssllabs	98 9,42%			
Total/10	88 84,81% 16 15,19%	100 (96,15%)	4 (3,85%)	0 (0,0%)

En la tabla 7, se observan los resultados de la variable de investigación seguridad de sitios web de las Universidades del Perú, para los indicadores, disown-opener 9,13%, https-only 5,48%, no-disallowed-headers 9,81%, no-protocol-relative-urls 7,21%, sri 8,94%, strict-transport-security 9,52%, validate-set-cookie-header 6,15%, x-content-type-options 9,90%, no-vulnerable-javascript-librar 9,23% y ssllabs 9,42%.

Ilustración 7.

Seguridad web en las Universidades Peruanas según categorías.



En la ilustración 5 y tabla 7, se observa el nivel de seguridad web que presentan, cuando se evaluaron los diez indicadores, 88 Universidades Peruanas que representa al 84,81% no pasan seguridad y solamente 16 Universidades que representa al 15,19% pasan la seguridad web. Cuando los datos de categorizaron por niveles, el 96,15% que representa a 100 Universidades, están en la categoría deficiente. Asimismo, solamente el 3,85% que representa a 4 Universidades están en la categoría necesita mejorar y ninguno en la categoría bueno.

Tabla 8
Universidades Peruanas, seguridad cero

Asociativa	Societaria	Pública	Seguridad = 0	Seguridad > 0	Total
8	7	12	27	77	104
7,69%	6,73%	11,54%	25,96%	74,04 %	100,00%

En la tabla 8, se observa a 27 Universidades que representa al 25,96% tienen cero en los indicadores de seguridad y 77 Universidades que representa a 74,04%, por lo menos pasa un indicador de seguridad.

4.1.3 Modelo predictivo machine learning

Los algoritmos de machine learning, fueron evaluados después de haberse realizado entrenamiento al grupo experimental (G1), la evaluación consistió comparar métricas de cada uno de los algoritmos de aprendizaje automático como son MAE, RMSE, RAE, RSE y R^2 para las Universidades Asociativas, Societarias, Públicas y del Perú, para más detalle de los resultados de entrenamiento ver modelo predictivo machine learning en el anexo 04.

Los algoritmos de machine learning entrenados fueron Bayesian linear, Regression, Decision Forest Regression, Linear regression, Neural Network

Regression y Boosted Decision Tree Regression. El mejor algoritmo más eficiente de los cinco entrenados fue Linear regression con una concordancia de índice Kappa muy buena.

Ilustración 8:

Modelo predictivo machine learning entrenado

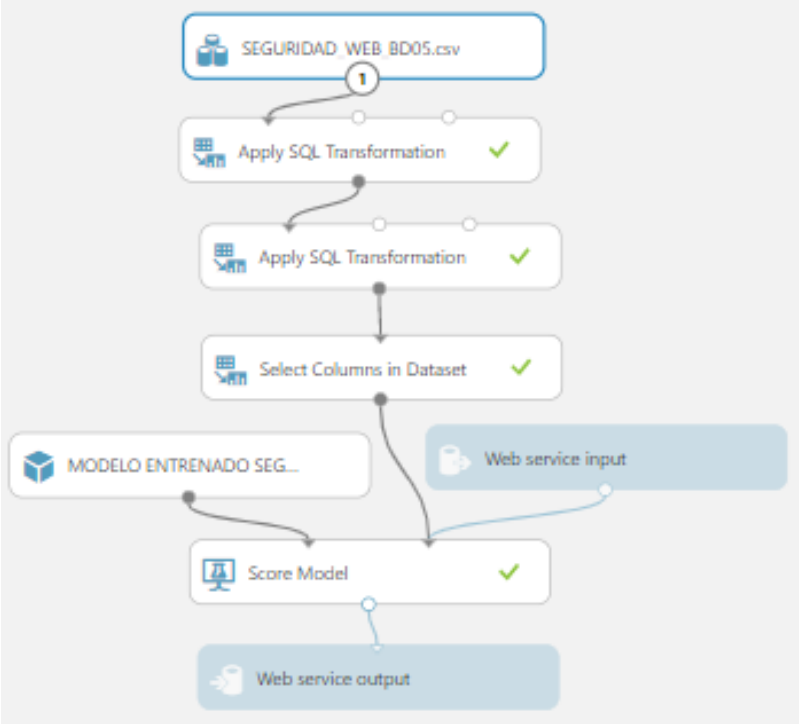


Tabla 9

Algoritmo Linear regression y sus métricas por tipo de Universidad e índice Kappa

Algoritmo	Métricas	Asociativas	Societarias	Públicas	Univ, Perú	Índice Kappa
Linear regression	MAE	0,0153	0,0042	0,0141	0,0013	Muy buena
	RMSE	0,0204	0,0052	0,0192	0,0018	
	RAE	0,0172	0,0046	0,0086	0,0013	
	RSE	0,0004	0,0000	0,0001	0,0000	
	R^2	0,9996	1,00	0,9999	1,00	

En la tabla 9, se muestran los resultados de entrenar al algoritmo Linear regression y sus métricas de machine learning. El coeficiente de determinación múltiple del modelo predictivo fueron 99,96%, 100%, 99,99% y 100% de la proporción de varianza total de la variable que explica la regresión múltiple, para las Universidades Societarias, Asociativas, Públicas y del Perú con una concordancia de índice Kappa en la categoría muy buena.

A continuación, la tabla 10 muestra resultados de dos tratamientos X y Y del grupo experimental de las Universidades Asociativas, Societarias y Públicas, variable de investigación de seguridad de sitios web.

Tabla 10

Tratamiento basado en dos tratamientos X y Y por tipo de Universidad

Asociativa: n = 30		Societaria: n = 38		Pública: n = 36	
X	*Y*	*X*	*Y*	*X*	*Y*
2	1,97	3	2,96	0	0,00
1	0,99	1	1,01	2	2,00
3	3,00	1	1,00	1	1,00
1	0,99	1	0,99	2	2,00
4	3,98	2	2,01	0	0,01
1	0,99	3	3,00	1	1,00
2	2,00	0	0,02	1	1,01
0	0,01	0	0,02	4	3,99
2	1,97	1	0,99	2	2,00
1	0,99	3	3,00	2	2,00
1	1,00	1	0,99	3	2,99
3	2,97	3	2,99	4	4,00
2	1,97	2	1,99	5	5,00
4	3,99	1	0,96	2	2,00
0	0,01	3	2,99	0	0,00
		6	5,97	0	0,00
		2	2,00	2	2,00
		3	2,98	7	6,98
		2	2,00		

Según la 10, los resultados de seguridad web basados en la ilustración 6 para Universidad asociativa, donde, el primer tratamiento X = 2 y con tratamiento Y = 1,97 y así sucesivamente. La Universidad Societaria presenta con el primer tratamiento X = 3 con tratamiento Y = 2,96, así sucesivamente. La Universidad Pública con el primer tratamiento X = 0 y con el tratamiento Y = 0,00 entonces los resultados de dos tratamientos las diferencias son mínimas, lo que significa que el modelo predictivo machine learning Y es casi igual al valor del tratamiento con X.

Tabla 11

Resultado de métricas después del entrenamiento de los algoritmos de machine learning

Algoritmo	MAE	RMSE	RAE	RSE	R^2
1. Bayesian linear regression	0,599083	0,814379	0,600416	0,499952	0,500048
2. Decision Forest Regression	0,001202	0,008667	0,001205	0,000057	0,999943
3. Linear Regression	0,001340	0,001822	0,001343	0,000003	0,999997
4. Neural Network Regression	0,260899	0,341420	0,261479	0,087872	0,912128
5. Boosted Decision Tree Regression	0,343852	0,465382	0,344616	0,163265	0,836735

En la tabla 11, se observa, el resultado de las métricas MAE, RMSE, RAE, RSE y R^2 para cada uno de los algoritmos de machine learning, al evaluar los cinco algoritmos, los algoritmos más eficientes fueron Decision Forest Regression y Linear Regression con coeficientes de determinación de 0,999943 y 0,999997 respectivamente, pero, evaluando las métricas de machine learning, el algoritmo más eficiente fue Linear Regression.

Tabla 12

Tratamiento basado en indicadores (X) y machine learning (Y), Universidades del Perú.

Dato	X	Y	Dato	X	Y	Dato	X	Y	Dato	X	Y
1	1	1,0008	14	1	1,0003	27	1	1,0003	40	2	2,0010
2	1	1,0008	15	1	1,0002	28	3	2,9991	41	2	2,0025
3	1	1,0012	16	0	0,0054	29	2	1,9948	42	1	0,9979
4	0	0,0013	17	3	3,0009	30	1	0,9984	43	3	2,9989
5	2	2,0001	18	2	2,0010	31	3	2,9945	44	1	0,9984
6	0	0,0007	19	3	3,0001	32	2	1,9972	45	3	3,0011
7	1	0,9988	20	4	3,9991	33	1	0,9985	46	0	0,0007
8	1	1,0005	21	0	0,0036	34	4	3,9999	47	1	1,0015
9	2	2,0005	22	0	0,0019	35	0	0,0008	48	0	0,0010
10	2	2,0025	23	3	2,9990	36	1	0,9997	49	3	3,0010
11	2	2,0003	24	3	3,0010	37	1	1,0006	50	0	0,0027
12	0	0,0008	25	1	0,9992	38	2	1,9983	51	3	3,0009
13	0	0,0007	26	1	1,0009	39	2	1,9993	52	0	0,0011

Tabla 13

Pesos (W_i) de los interceptores y regresores del modelo predictivo machine learning de las Universidades Peruanas

Univer_sidad	Interceptor	Regresores W_i					R^2
	W_0	W_1	W_2	W_3	W_4	W_5	
Asociativa	36,231	0,0370	0,0016	0,0066	0,0177	0,5051	0,9999
Societaria	47,551	0,0157	0,0017	0,0080	0,0104	- 0,5151	0,9998
Pública	120,492	0,0008	- 0,0021	-0,0237	-0,0393	-0,6219	0,9999
Perú	74,637	0,0133	-0,0041	0,0115	0,0028	- 0,8002	1,0000

En la tabla 12, se observa, el modelo predictivo machine learning para la Universidad Asociativa, tiene un coeficiente de determinación de 99,99. Societaria 99,98%. Pública

99,99% y las Universidades del Perú 100% que explican las varianzas totales de la variable de investigación dependiente del modelo predictivo $\hat{Y}$:

$$\hat{Y} = 3{,}6231 + 0{,}0370x_1 + 0{,}0016x_2 + 0{,}0066x_3 + 0{,}0177x_4 + 0{,}5051x_5 \quad (5)$$

$$\hat{Y} = 3{,}6231 + 0{,}0370x_1 + 0{,}0016x_2 + 0{,}0066x_3 + 0{,}0177x_4 + 0{,}5051x_5 \quad (6)$$

$$\hat{Y} = 3{,}6231 + 0{,}0370x_1 + 0{,}0016x_2 + 0{,}0066x_3 + 0{,}0177x_4 + 0{,}5051x_5 \quad (7)$$

$$\hat{Y} = 3{,}6231 + 0{,}0370x_1 + 0{,}0016x_2 + 0{,}0066x_3 + 0{,}0177x_4 + 0{,}5051x_5 \quad (8)$$

Las ecuaciones 5, 6, 7 y 8, corresponden a los modelos predictivos de las Universidades Asociativas, Societarias, Públicas y Universidades del Perú.

4.2 Contrastación de hipótesis

4.2.1 Primera hipótesis derivada

a) Planteamiento de hipótesis

H_0: No Existe una diferencia de medias del mejor algoritmo predictivo de machine learning entrenado más eficiente basados en las métricas entre la calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

$H_0: \mu_X = \mu_Y = 0$

H_1: Existe una diferencia de medias del mejor algoritmo predictivo de machine learning entrenado más eficiente basados en las métricas entre la calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

$H_1: \mu_X \neq \mu_Y$

b) Nivel de confianza

$\alpha = 0{,}05$

c) Estadístico para prueba de hipótesis

T-Student de dos muestras

Universidad	Intervalo de confianza Diferencia de Medias (μ)	Valor T	Valor p	R^2
Asociativa	0,0035 - 0,0191	3,12	0,008	0,9999
Societaria	-0,0014 - 0,0150	1,75	0,097	0,9998
Pública	0,0023 - 0,0045	0,70	0,495	0,9999

d) Regla de decisión

Universidad	Decisión	
Asociativa	$Aceptar\ H_0: Si,$	$Valor\ p = 0{,}008 > \ \alpha = 0{,}05$
	$Aceptar\ H_1: Si,$	$Valor\ p = 0{,}008 < \ \alpha = 0{,}05$
Societaria	$Aceptar\ H_0: Si,$	$Valor\ p = 0{,}097 > \ \alpha = 0{,}05$
	$Aceptar\ H_1: Si,$	$Valor\ p = 0{,}097 < \ \alpha = 0{,}05$
Pública	$Aceptar\ H_0: Si,$	$Valor\ p = 0{,}495 > \ \alpha = 0{,}05$
	$Aceptar\ H_1: Si,$	$Valor\ p = 0{,}495 < \ \alpha = 0{,}05$

e) Toma de decisión

Para la Universidad Asociativa, rechazar la hipótesis nula y aceptar la hipótesis alterna porque se haya evidencia estadística suficiente de que las medias difieren por ser mayor a cero, en el nivel de significancia de 0,05 y existe una relación de 99,99% del algoritmo predictivo Linear Regression de machine learning más eficiente entre calidad de aplicaciones y seguridad web de las Universidades Asociativas. En la tabla 9, se observa que las diferencias son mínimas, pero la predicción post test es similar al resultado a valor observado en pretest.

Para las Universidades Societarias y Públicas, se rechazan las hipótesis alternas y se aceptan las hipótesis alternas porque existe suficiente evidencia

estadística de que las medias no difieren porque son iguales, en el nivel de significancia de 0,05 y existe una relación de 99,98% y 99,99% del algoritmo predictivo Linear regression de machine learning más eficiente entre calidad de aplicaciones y seguridad web de las Universidades Societarias y Públicas. En la tabla 9, se observa que las diferencias entre los resultados de pre test y post test es muy similar, por tanto, la predicción es muy buena.

4.2.2 Segunda hipótesis derivada

a) Planteamiento de hipótesis

H_0: No existe diferencia de pesos pronosticados ($\widehat{W}_i$) de aprendizaje para una regresión significativa para el modelo predictivo de machine learning entre calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

H_0: $\widehat{W}_1 = \widehat{W}_2 = \widehat{W}_3 = \widehat{W}_4 = \widehat{W}_5 = 0$

H_1: Existe diferencia de pesos pronosticados ($\widehat{W}_i$) de aprendizaje para una regresión significativa para el modelo predictivo de machine learning entre calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

H_1: $\widehat{W}_1 \neq \widehat{W}_2 \neq \widehat{W}_3 \neq \widehat{W}_4 \neq \widehat{W}_5$

b) Nivel de confianza

$\alpha = 0{,}05$

c) Estadístico para prueba de hipótesis

Análisis de varianza F

Fuente de Variación	Grados de libertad	Suma de cuadrados	Promedio de los cuadrados	F	Valor crítico de F_0	Universidad
Regresión	5	173,387	34,677	61,664	0,0094	Asociativa
Residuos	9	50,613	0,5624			
Total	14	224,000				
Regresión	5	29,1044	5,8209	10,9738	0,0003	Societaria
Residuos	13	6,8956	0,5304			
Total	18	36				
Regresión	5	54,2837	10,8567	17,3844	0,0000	Pública
Residuos	12	7,4941	0,6245			
Total	17	61,7778				

d) Regla de decisión

Universidad	Decisión	
Asociativa	$Aceptar\ H_0: Si,$	$Valor\ crítico\ F_0 = 0{,}0094 >\ \alpha = 0{,}05$
	$Aceptar\ H_1: Si,$	$Valor\ crítico\ F_0 = 0{,}0094 <\ \alpha = 0{,}05$
Societaria	$Aceptar\ H_0: Si,$	$Valor\ crítico\ F_0 = 0{,}0003 >\ \alpha = 0{,}05$
	$Aceptar\ H_1: Si,$	$Valor\ crítico\ F_0 = 0{,}0003 <\ \alpha = 0{,}05$
Pública	$Aceptar\ H_0: Si,$	$Valor\ crítico\ F_0 = 0{,}0000 >\ \alpha = 0{,}05$
	$Aceptar\ H_1: Si,$	$Valor\ crítico\ F_0 = 0{,}0000 <\ \alpha = 0{,}05$

e) Toma de decisión

Para los parámetros de aprendizaje, peso de interceptores (W_0) y peso de regresores ($W_{1,2,3,4,5}$) de las ecuaciones (1), (2) y (3) de las Universidades Asociativas, Societarias y Públicas, se rechazan las hipótesis nulas y se aceptan las hipótesis alternas porque existe suficiente evidencia estadística de que las medias de los parámetros aprendizaje peso (W) difieren porque no son iguales, en el nivel de significancia de 0,05 y existe una relación de 99,99%, 99,98% y 99,99% del algoritmo predictivo Linear regression de machine learning más eficiente entre

calidad de aplicaciones y seguridad web de las Universidades Societarias y Públicas.

4.2.3 Hipótesis general

a) Planteamiento de hipótesis

H_0: No Existe una diferencia de medias de dos tratamientos del modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las universidades del Perú, año 2020.

$H_0: \mu_X = \mu_Y = 0$

H_1: Existe una diferencia de medias de dos tratamientos del modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las universidades del Perú, año 2020.

$H_1: \mu_X \neq \mu_Y$

b) Nivel de confianza

$\alpha = 0{,}05$

c) Estadístico para prueba de hipótesis

- T-Student

  Universidades del Perú : 104 (G1 = 52, G2 = 52)

  gl = *n* - 2 = 104 - 2 = 102

  Valor T : - 0,00

  Valor p : 0,999

  R^2 : 1,00

- Análisis de varianza para Aprendizaje basado en pesos (W_i)

  k = columnas = 5

  Grados de libertad numerador, *gl = k* = 5

  Grados de libertad denominador, *gl = (n-k-1)* = (52-5-1) = 46

Fuente de variación	Suma de cuadrados	Grados de libertad	Promedio de los cuadrados	F	Valor-p	R^2
Regresión	67,5990	5	13,5198	450,07	0,000	0,9800
Residuos	1,3818	46	0,0300			
Total	68,9808	51	51			

d) Regla de decisión

$$Aceptar\ machine\ learning = \begin{cases} H_0: Si, & Valor - p = 0{,}999 > \alpha = 0{,}05 \\ H_1: Si, & Valor - p = 0{,}999 < \alpha = 0{,}05 \end{cases}$$

$$Aceptar\ W_i\ aprendizaje = \begin{cases} H_0: Si, & Valor - p = 0{,}000 > \alpha = 0{,}05 \\ H_1: Si, & Valor - p = 0{,}000 < \alpha = 0{,}05 \end{cases}$$

e) Toma de decisión

Para la población muestral de 104 Universidades del Perú, el grupo experimental y control de 52 cada uno, con 102 grados de libertad, el nivel de significancia observado (valor-p) fue de 0,999 que es mayor al α = 0,05 entonces se decide rechazar la hipótesis alterna y aceptar la hipótesis nula porque existe suficiente evidencia estadística de que las medias de dos tratamientos no difieren, por lo que se concluye que el modelo predictivo machine learning con tratamiento X y Y, reportan en promedio, que son iguales entre la calidad de aplicaciones y seguridad web de las Universidades del Perú.

Para los parámetros aprendizaje peso (W_i) interceptor y regresores del modelo $Y = 9{,}526 - 0{,}0016x_1 - 0{,}0039x_2 + 0{,}0033x_3 + 0{,}0060x_4 - 0{,}9328x_5$, se rechaza la hipótesis nula y se acepta la hipótesis alterna porque Fo es menor a alfa, que significa que la media de los regresores es diferente de

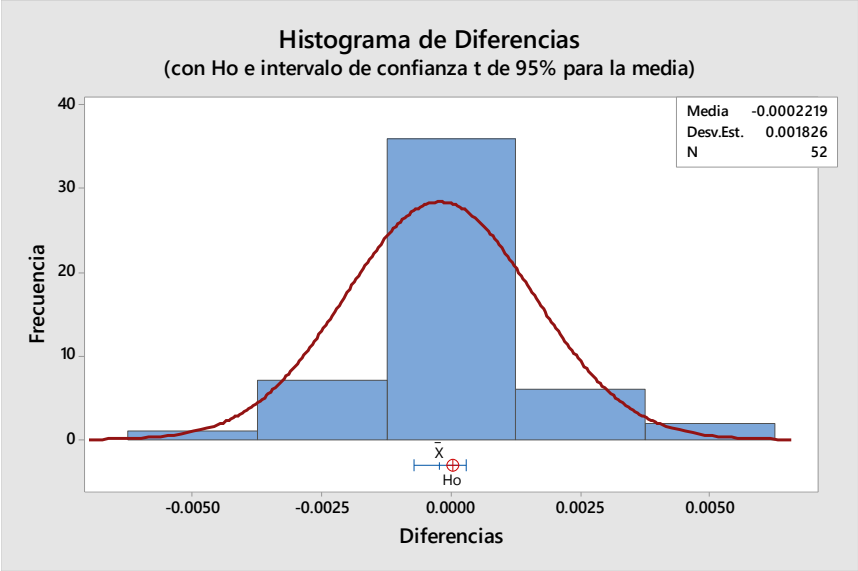
cero por lo que el modelo tiene una eficiencia de 98,00% de predicción en post test con respecto a pre test.

4.3 Discusión de los resultados

Los resultados para modelo predictivo ML de calidad de aplicaciones y seguridad web de universidades del Perú, año 2020, indican un coeficiente de determinación 0,99 y una diferencia de media cero y una desviación estándar de 0,001826 con los datos expuestos, como muestra en la ilustración 5.

Ilustración 5:

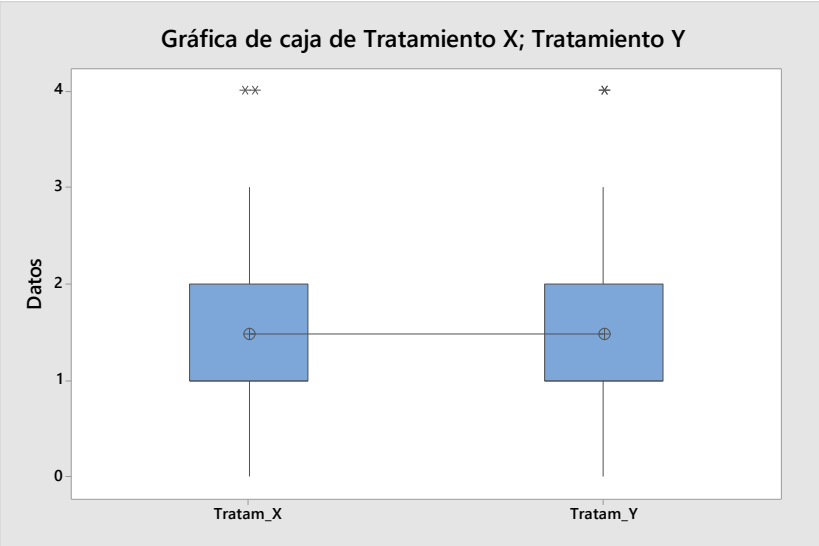
Diferencia de medias del pretest y post test predictivo de las Universidades del Perú.



En la diferencia de dos medias poblacionales, se tienen dos muestras u observaciones antes y después (Karasan 2022) , es decir, las Universidades del Perú fueron evaluados aleatoriamente con tratamiento X y Y, pero con resultados iguales, ilustración 6.

Ilustración 9:

Resultado con tratamiento X y Y



Después de entrenar cinco algoritmos de machine learning, se evaluó las métricas de los algoritmos comparando principalmente los coeficientes de determinación, la predicción de la variable de investigación seguridad web de universidades del Perú, se explican al predecir el resultado de un evento con el modelo predictivo machine learning. En otras palabras, este coeficiente, que se conoce más comúnmente como R cuadrado (R^2), evalúa qué tan fuerte es la relación lineal entre dos variables de investigación para la predicción del modelo (Hurst et al., 2022)

Aplicando la inferencia lógica Modus Ponens de (González, Albert, & Artalejo, 2019), a los resultados de la investigación, los predicados P = Modelo predictivo machinen learning de calidad de aplicaciones web y Q = Seguridad web de universidades del Perú, año 2020, cumplen con ser verdaderos las implicancias, siempre que las premisas sean verdaderas o falsos, entonces las conclusiones son

verdaderos según las reglas 1, 3 y 4. No cumple la regla 2, siendo la premisa verdadera no se puede concluir como falso.

Regla (R)	P	Q	$P \longrightarrow Q$
R1	V	V	V
R2	V	F	F
R3	F	V	V
R4	F	F	V

Taboada (2021), en su tesis de maestría, utilizó aprendizaje por refuerzo o machine learning, donde, los mejores decisiones del agente para asegurar la seguridad web, su comportamiento más eficientemente a la respuesta adaptiva, llegó a bloquear o predecir el 95,5% de problemas de seguridad y comparando los resultados de predicción sobre sobre seguridad web de las universidad peruanas fue 99,99% utilizando el algoritmo de aprendizaje automático por refuerzo Linear Regression mejorando en 4,1% a la investigación arriba citada.

Existen universidades con seguridad cero, porque no cumplen ninguno de los 10 indicadores de seguridad como disown-opener, https-only, no-disallowed-headers, no-protocol-relative-urls, sri, strict-transport-security, validate-set-cookie-header, x-content-type-options, no-vulnerable-javascript-librar y ssllabs. Las universidades que incumplen el 100% de seguridad web son: Universidad Peruana Cayetano Heredia, Universidad del Pacífico, Universidad de Piura, Universidad Ricardo Palma, Universidad Peruana Unión, Universidad Particular de Chiclayo, Universidad Científica del Perú, Universidad Católica Los Ángeles de Chimbote, Universidad Señor de Sipán, Universidad Peruana de Ciencias e Informática, Universidad Sergio Bernales S.A., Universidad Privada Juan Mejía Baca,

Universidad de Ciencias y Artes de América Latina S.A.C., Universidad Peruana de Investigación y Negocios S.A.C., Universidad Autónoma San Francisco, Universidad Nacional de San Cristóbal de Huamanga, Universidad Nacional de San Antonio Abad del Cusco, Universidad Nacional de Ingeniería, Universidad Nacional de Educación Enrique Guzmán y Valle, Universidad Nacional Daniel Alcides Carrión, Universidad Nacional José Faustino Sánchez Carrión, Universidad Nacional de San Martín, Universidad Nacional de Tumbes, Universidad Nacional Intercultural de la Amazonía, Universidad Nacional Tecnológica de Lima Sur, Universidad Nacional de Moquegua y Universidad Nacional José María Arguedas.

En su investigación Alani & Tawfik (2022), concluye que la calidad de sitios web es baja con 72,10%, pero, las universidades peruanas están mejor en cuanto a la calidad de sitios web con 66,11% en la categoría mejorar, tabla 7.

La métrica de machine learning, coeficiente de determinación fue de 1,00 en la categoría muy alta. Al realizar la contrastación de hipótesis sobre la diferencia de medias con t-student pareado, el p-valor fue 0,385 por tanto se procedió a aceptar la hipótesis nula, porque, los resultados de la media de seguridad web del pre test y post test fueron iguales, porque, el intervalo de confianza entre -0,000730 a 0,000287, significó que estadísticamente eran iguales las muestras para el modelo predictivo machine learning entre la calidad de aplicaciones y seguridad web de las Universidades del Perú, año 2020.

En la contrastación de hipótesis, los parámetros de aprendizaje peso (W) del modelo predictivo el peso de aprendizaje interceptor y los regresores fueron $W_0 = 9{,}526$; $W_1 = -0{,}0016$; $W_2 = -0{,}0039$; $W_3 = 0{,}0033$; $W_4 = 0{,}0060$; $W_5 = -0{,}9328$. Los resultados, fueron analizados con el estadístico análisis de varianza

y se rechazó hipótesis nula y se aceptó la hipótesis alterna, porque, el valor crítico F_0 fue 0,00 menor al alfa 0,05 con 51 grados de libertad, correlación múltiple de 0,98 y que el modelo predictivo, predice lo más cercano a la realidad por tener un aprendizaje de 1,00.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Primera.

Se determinó, que el coeficiente de determinación fue 1,00 y diferencia de medias fueron iguales para el modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las universidades del Perú, año 2020.

Segunda.

Se evaluó, los resultados de la predicción post test y pretest como la diferencia de medias del algoritmo predictivo linear regression de machine learning entrenado más eficiente basados en las métricas para el modelo predictivo de la calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

Tercera.

Se determinó, los parámetros aprendizaje peso (W) $\hat{Y} = 9{,}526 - 0{,}0016x_1 - 0{,}0039x_2 + 0{,}0033x_3 + 0{,}0060x_4 - 0{,}9328x_5$ para el modelo predictivo de machine learning entre los indicadores de calidad de aplicaciones y seguridad web de las Universidades Asociativas, Societarias y Públicas.

5.2 Recomendaciones

Primera.

Profundizar la investigación con más variables y comparar con las universidades latinoamericanos, el modelo predictivo machine learning entrenado entre la calidad de aplicaciones y seguridad web de las universidades del Perú.

Segunda.

Profundizar la investigación, sobre el algoritmo predictivo Redes neuronales artificiales para el modelo predictivo machine learning de la calidad de aplicaciones y seguridad web de las universidades peruanas.

Tercera.

Realizar investigación, en el campo de clúster para el modelo predictivo de machine learning de calidad de aplicaciones y seguridad web de las universidades de Perú.

BIBLIOGRAFÍA

Altman, D. G. J. L., & York, N. (1991). Practical statistics for medical research Chapman and Hall.

Álvarez, A. C. (2019). *Programar con Python 3*: Lulu.com.

Anderson, D. R., Sweeney, D. J., & Williams, T. A. (2008). *Estadística Para Administración Y Economía*: Cengage Learning Latin America.

Alani, M. M., & Tawfik, H. (2022). PhishNot: A Cloud-Based Machine-Learning Approach to Phishing URL Detection. *Computer Networks, 218*, 109407. https://doi.org/10.1016/j.comnet.2022.109407

Ashtari, A., shabani, ahmad, & Alizadeh, B. (2022). A comparative study of machine learning classifiers for secure RF-PUF-based authentication in internet of things. *Microprocessors and Microsystems*, *93*, 104600. https://doi.org/10.1016/j.micpro.2022.104600

Berghout, T., Benbouzid, M., & Muyeen, S. M. (2022). Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. *International Journal of Critical*

Bancila, M., Rialdi, R., Sharma, A., & Esposito, D. (2020). *Learn C# Programming: A guide to building a solid foundation in C# language for writing efficient programs*: Packt Publishing.

Barnes, J. (2015). *Microsoft Azure Essentials Azure Machine Learning*: Pearson Education.

Bloch, J. (2018). *Effective Java*: Addison-Wesley.

Butler, T., & Yank, K. (2017). *PHP & MySQL: Novice to Ninja: Get Up to Speed With PHP the Easy Way*: SitePoint.

Candel, J. M. O. (2019). *Seguridad en aplicaciones Web Java*: Ediciones de la U Ltda.

Chafloque Farroñay, E. E. (2016). *Evaluación de la usabilidad en las interfaces de usuario de las aplicaciones web mediante normas de calidad.* Retrieved from http://repositorio.uss.edu.pe/handle/uss/4258

Chopra, R. (2016). *WEB ENGINEERING*: Prentice Hall India Pvt., Limited.

Conesa, M. (2010). *Evaluación de la calidad de los sitios web con información sanitaria en castellano.* Tesis Doctoral. Murcia: Universidad de Murcia,

Dowden, M., & Dowden, M. (2020). *Architecting CSS: The Programmer's Guide to Effective Style Sheets*: Apress.

El Naqa, I., Li, R., & Murphy, M. J. (2015). *Machine learning in radiation oncology: theory and applications*: Springer.

Elbaz, K. (2022). A new model view controller implementation to maximise maintainability of web-based applications. *International Journal of System of Systems Engineering*, *12*(3), 271. https://doi.org/10.1504/IJSSE.2022.125948

Erinle, B. (2017). *Performance Testing with JMeter 3*: Packt Publishing.

Fred, A. M., Perepa, B., Patrocinio, E. A., Gorski, H., Gupta, M., Ryan, P. M., . . . Redbooks, I. (2015). *IBM Bluemix Architecture Series: Web Application Hosting on IBM Containers*: IBM Redbooks.

Gallagher, M., Pitropakis, N., Chrysoulas, C., Papadopoulos, P., Mylonas, A., & Katsikas, S. (2022). Investigating machine learning attacks on financial time series models. *Computers & Security*, *123*, 102933. https://doi.org/10.1016/j.cose.2022.102933

González, M. T. H., Albert, J. L., & Artalejo, M. R. (2019). *Matemática discreta y lógica matemática*: Garceta Grupo Editorial.

Goolge. (2020). Web Fundamentals. *Tutorials, guides, and best practices for building the next generation of web experiences.* Retrieved from https://developers.google.com/

Grid, A. (2020). *C++ Programming: A Step-By-step Beginner's Guide to Learn the Fundamentals of a Multi-paradigm Programming Language and BEGIN to Manage Data Including How to Work on Your First Program*: Independently Published.

Gutiérrez del Moral, L. J. S. P. R. L. (2014). Curso de ciberseguridad y hacking ético 2013. Ahammad, S. H., Kale, S. D., Upadhye, G. D., Pande, S. D., Babu, E. V., Dhumane, A. V., & Bahadur, Mr. D. K. J. (2022). Phishing URL detection using machine learning methods. *Advances in Engineering Software*, *173*, 103288. https://doi.org/10.1016/j.advengsoft.2022.103288

Gallagher, M., Pitropakis, N., Chrysoulas, C., Papadopoulos, P., Mylonas, A., & Katsikas, S. (2022). Investigating machine learning attacks on financial time series models. *Computers & Security*, *123*, 102933. https://doi.org/10.1016/j.cose.2022.102933

Huerta Agurto, C. (2020). *Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019* [Tesis de Maestría]. Universidad Cesar Vallejo.

Hurst, W., Tekinerdogan, B., Alskaif, T., Boddy, A., & Shone, N. (2022). Securing electronic health records against insider-threats: A supervised machine learning approach. *Smart Health*, *26*, 100354. https://doi.org/10.1016/j.smhl.2022.100354

Hurwitz, J., & Kirsh, D. (2018). *Machine Learning For Dummies®, IBM Limited Edition*. 75.

Jimenez, F. V. J., Jimenez, F. O. J., Jimenez, F. J. C., & Jimenez, C. J. U. (2020). Performance Comparison of Natural Language Understanding Engines in the Educational Domain. *International Journal of Advanced Computer Science and Applications, 11*(8). doi:10.14569/IJACSA.2020.0110892

Karasan, A. (2022). *Machine learning for financial risk management with Python: Algorithms for modeling risk.* O'Reilly.

Körner, C., & Waaijer, K. (2020). *Mastering Azure Machine Learning: Perform Large-scale End-to-end Advanced Machine Learning on the Cloud with Microsoft Azure ML*: Packt Publishing.

Lind, D. A., Mason, R. D., & Marchal, W. G. (2004). *Estadística para administración y economía*: Alfaomega.

Lopez, F. (2018). *PREDICCIÓN DEL TIPO Y CANTIDAD DE ACTIVIDADES DE INSTALACIÓN Y MANTENIMIENTO GESTIONADOS POR EL PERSONAL TÉCNICO DE LA EMPRESA COLVATEL S.A., USANDO REDES NEURONALES.* [Tesis de Maestría]. Universidad Piloto de Colombia.

Manrique, V. (2022). *Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico Público, Lima-2021* [Tesis de Maestría]. Universidad Cesar Vallejo.

Meiert, J. O. (2016). *The Little Book of Website Quality Control*: O'Reilly Media.

Microsoft. (2020). Tools. *Check and debug your site with these cross-platform tools.* Retrieved from https://developer.microsoft.com/es-es/microsoft-edge/tools/

Muzaffar, A., Ragab Hassen, H., Lones, M. A., & Zantout, H. (2022). An in-depth review of machine learning based Android malware detection. *Computers & Security, 121*, 102833. https://doi.org/10.1016/j.cose.2022.102833

Narro, S. (2021). *El Sistema de Gestión de seguridad de la Información y la Gestión de Riesgos en el Área Informatica de una Universidad Pública, Región Cajamarca 2020.* [Tesis de Maestría]. Universidad Privada del Norte.

Offutt, J. (2002). Quality attributes of Web software applications. *Software, IEEE, 19*, 25-32. doi:10.1109/52.991329

Olsina, L., Lew, P., Dieser, A., & Rivera, B. J. J. o. W. E. (2012). Updating quality models for evaluating new generation web applications. *11*(3), 209.

Ortega Santamaría, S., & Yusef, H.-M. (2013). Análisis y evaluación de sitios web universitarios españoles a partir del proceso de Bolonia. *Perspectivas em Ciencia da Informacao, 18*, 70-92. doi:10.1590/S1413-99362013000400006

Parnas, D. L., Van Schouwen, A. J., & Kwan, S. P. J. C. o. t. A. (1990). Evaluation of safety-critical software. *33*(6), 636-648.

Pressman, R. S. (2010). *Ingeniería de Software. Un enfoque práctico Séptima Edición*: McGraw Hill Educación.

Pulido, H. G., de la Vara Salazar, R., & Castellanos, M. Á. T. (2012). *Análisis y diseño de experimentos*: McGraw-Hill.

Romero, J., Dafonte, C., Gómez, Á., & Penousal, F. (2007). *Inteligencia artificial y computación avanzada*.

Rueda Liberato, E. E. (2019). *Cifrado con el protocolo ssl/tls y el rendimiento de sitios web. caso: empresa web-out, 2018 – 2019.* Retrieved from http://repositorio.unas.edu.pe/handle/UNAS/1535

Sampieri, R. H. (2018). *METODOLOGÍA DE LA INVESTIGACIÓN: LAS RUTAS CUANTITATIVA, CUALITATIVA Y MIXTA*: McGraw-Hill Interamericana.

Sun, Y., Jing, S., Gao, R., Dong, B., Chen, W., & Xu, X. (2021). Research on the Detection and Analysis Technology in Web Application Attacks Logs.

2021 2nd International Symposium on Computer Engineering and Intelligent Communications (ISCEIC), 132–135. https://doi.org/10.1109/ISCEIC53685.2021.00034

Taboada, L. (2021). *Modelo de seguridad de la información para contribuir en la mejora de la seguridad de los activos de información financiera de las unidades de gestión educativa local de Lambayeque-2021* [Tesis de Maestría]. UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO.

Valverde Chávez, J. (2018). *Los riesgos de seguridad de websites y sus efectos en la gestión de información de medianas empresas de Lima Metropolitana* [Tesis de Maestría, Universidad Nacional Mayor de San Marcos]. http://revistas.urp.edu.pe/index.php/Perfiles_Ingenieria/article/view/1469

Tent, T. P. (2020). *Programming Language; The Beginner 's Guide: The Hyper Text Markup Language Five (HTML5)*: Independently Published.

Valverde Chávez, J. (2018). *Los riesgos de seguridad de websites y sus efectos en la gestión de información de medianas empresas de Lima Metropolitana* [Tesis de Maestría, Universidad Nacional Mayor de San Marcos]. http://revistas.urp.edu.pe/index.php/Perfiles_Ingenieria/article/view/1469

Web.dev. (s/f). Recuperado el 22 de enero de 2021, de https://web.dev

Yépez Cabanillas, D. G. (2018). *Impacto del modelo de calidad Furps en la aplicación web de gestión de historias infantiles del C.A.R Niña Belén (Tesis Parcial).* Retrieved from http://hdl.handle.net/11537/13332

Yu, C. T., & Tomorrowskills, H. (2020). *R for Ruby: Learn the Basic Vocabs of the Ruby Programming Language*: Amazon Digital Services LLC - KDP Print US.