Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), enero-febrero 2026,
Volumen 10, Número 1.

https://doi.org/10.37811/cl_rcm.v10i1

MODELO DE MACHINE LEARNING PARA LA IDENTIFICACIÓN DE LA PROBABILIDAD DE RIESGO DE SUPLANTACIÓN DE IDENTIDAD

MACHINE LEARNING MODEL FOR IDENTIFYING OF IDENTITY IMPERSONATION RISKS

Gabriela González-Vázquez
Tecnológico Nacional de México

Luis Alberto León-Bañuelos
Tecnológico Nacional de México

Demetrio Castelan Urquiza
Tecnológico Nacional de México

Araceli Guerrero Alonso
Tecnológico Nacional de México

Felipe de Jesús García López
Tecnológico Nacional de México

DOI: https://doi.org/10.37811/cl_rcm.v10i1.22410

Modelo de Machine Learning para la Identificación de la Probabilidad de Riesgo de Suplantación de Identidad

Gabriela González-Vázquez[1]
gabriela.gv@vbravo.tecnm.mx
https://orcid.org/0000-0003-0780-6392
Tecnológico Nacional de México
TES Valle de Bravo, México

Luis Alberto León-Bañuelos
luis.lb@vbravo.tecnm.mx
https://orcid.org/0000-0003-0332-6228
Tecnológico Nacional de México
TES Valle de Bravo, México

Demetrio Castelan Urquiza
demetrio.cu@vbravo.tecnm.mx
https://orcid.org/0000-0003-0250-7908
Tecnológico Nacional de México
TES Valle de Bravo, México

Araceli Guerrero Alonso
araceli.ga@vbravo.tecnm.mx
https://orcid.org/0009-0006-8868-7442
Tecnológico Nacional de México
TES Valle de Bravo, México

Felipe de Jesús García López
felipefenix05@gmail.com
https://orcid.org/0009-0008-7764-7482
Tecnológico Nacional de México
TES Valle de Bravo, México

RESUMEN

La suplantación de identidad en línea es una amenaza creciente. En México, durante el 2023, ocho de cada diez personas de seis años en adelante fueron usuarios de internet (IFT, 2024). Este aumento ha originado un incremento de los ciberdelitos, afectando principalmente a jóvenes. A pesar de leyes como el Código Penal Federal y la Ley General de Protección de Datos Personales, los delitos cibernéticos siguen siendo un desafío para el sistema judicial (Diputado Monreal Ávila, 2025). Ante esto, surge la necesidad de desarrollar herramientas de prevención más eficaces (UNICEF, 2024), basadas en inteligencia artificial. Donde, los algoritmos de Machine Learning son una solución prometedora para identificar y predecir el riesgo de suplantación de identidad (Rodriguez-Asto et al., 2024). El modelo propuesto se apoya en datos obtenidos mediante encuestas con escala Likert, evaluando el nivel de conocimiento y comportamiento de los usuarios frente al phishing y otras amenazas digitales. La metodología utilizada para el desarrollo de la plataforma se estructura en cuatro fases: recolección de datos, validación, integración y evaluación de resultados. Para la predicción de riesgos, se utilizó un modelo de Naive Bayes (Ige et al., 2024). La plataforma no solo se limita a realizar predicciones, presenta un enfoque educativo, brindando a los usuarios herramientas y recursos para prevenir el phishing y otros tipos de fraudes digitales (Aredo-Vargas et al., 2024).

Palabras clave: suplantación, machine learning, riesgos de internet,algoritmo

[1] Autor principal.
Correspondencia: gabriela.gv@vbravo.tecnm.mx

Machine Learning Model for Identifying of Identity Impersonation Risks

ABSTRACT

Online identity theft is a growing threat. In Mexico, during 2023, eight out of ten people aged six and older were internet users (IFT, 2024). This increase has led to a rise in cybercrime, primarily affecting young people. Despite laws such as the Federal Penal Code and the General Law on the Protection of Personal Data, cybercrimes continue to pose a challenge to the judicial system (Diputado Monreal Ávila, 2025). Given this, there is a need to develop more effective prevention tools (UNICEF, 2024) based on artificial intelligence. Machine learning algorithms are a promising solution for identifying and predicting the risk of identity theft (Rodriguez-Asto et al., 2024). The proposed model is based on data obtained through Likert-scale surveys, assessing users' level of knowledge and behavior regarding phishing and other digital threats. The methodology used to develop the platform is structured in four phases: data collection, validation, integration, and results evaluation. A Naive Bayes model was used for risk prediction (Ige et al., 2024). The platform not only makes predictions but also has an educational focus, providing users with tools and resources to prevent phishing and other types of digital fraud (Aredo-Vargas et al., 2024).

***Keywords*:** identity impersonation, machine learning, internet risks, algorithm

Artículo recibido 09 diciembre 2025
Aceptado para publicación: 12 enero 2026

INTRODUCCIÓN

En el mundo, 62.5% de las personas se conectan a Internet, donde ocho de cada diez utilizan redes sociales (Romero Mireles, 2023), el servicio se ha convertido en una herramienta indispensable en todos los ámbitos (Moreano Guerra et al., 2024), tanto empresarial como educativo, lo cual ha permitido el crecimiento y desarrollo de factores para mejora de variadas actividades. Desafortunadamente este cambio ha provocado ciertas vulnerabilidades en la población. Flores Mayorga et al. (2023) determinaron, a partir de una encuesta aplicada a 215 niños, niñas y adolescentes entre los 10 y 14 años determinaron que 8.76% han sufrido de acoso sexual en línea. Aunado a todo esto, la suplantación de identidad ha ido en incremento, donde los ciberdelincuentes usan estas debilidades para cometer delitos en anonimato (Martínez Galindo, 2024).

En México se ha convertido en un problema significativo en el entorno digital, afectando tanto a individuos como a organizaciones (Alcalá Casillas, 2024). Este delito plantea serias amenazas a la privacidad y la seguridad personal, lo que ha llevado a la sociedad a demandar respuestas más efectivas (Alcalá Casillas y Meléndez Ehrenzweig, 2023). El uso intensivo de la tecnología entre las nuevas generaciones las hace más vulnerables a distintos riesgos digitales, siendo el phishing uno de los más comunes. (García García, 2018), los jóvenes representan un objetivo muy tentador para los atacantes, ya que pueden carecer de la capacidad o el entendimiento necesario para enfrentar estos riesgos (Montemayor Garza y Tapia Cortes, 2022).

La manera más común de suplantación de identidad es utilizando la ingeniería social (López Grande y Salvador Guadrón, 2016)

El Código Penal Federal establece la suplantación de identidad como un delito y sanciona a quienes lo cometen para obtener un beneficio económico o causar daño a una persona (Código Penal, 2025). Por otra parte, la ley General de Protección de Datos Personales en Posesión de los Particulares, establece sanciones para quienes manejen datos de manera indebida (Protección de Datos, 2025). Asimismo la Ley Olimpia, aunque originalmente se enfoca en la violencia digital, incluye disposiciones que abordan la suplantación de identidad y el uso indebido de la imagen de una persona sin su consentimiento (Ley Olimpia, 2025).

Si bien se tienen las leyes y responsables del cumplimiento, los ciberdelitos suelen superar las capacidades para dar seguimiento y por tanto es difícil solucionar estos problemas en un corto tiempo. Es por ello que se han generado diversas estrategias que apoyan en la prevención e identificación temprana (Olivares Romero et al., 2025).

El aumento de casos de suplantación de identidad en el entorno digital ha impactado gravemente a las víctimas (González Véliz y Cuzcano Chavez, 2024), destacando la necesidad urgente de combatir esta amenaza. Se desarrollaron sistemas avanzados de detección basados en inteligencia artificial y campañas de concientización para capacitar a los usuarios sobre la protección de sus datos personales. (Oseda Gago et al., 2024).

Los riesgos informáticos también afectan a grandes organizaciones, que frecuentemente son extorsionadas (Peña Labrini, 2023). Estas entidades deben implementar planes de respuesta inmediata ante amenazas, utilizando el ciclo de Deming (Montesinos González et al., 2020), para diseñar estrategias efectivas y optimizar recursos en el uso de tecnologías de la información.

La Industria 4.0 ha promovido el uso de pagos digitales, lo que mejora la experiencia de consumo y reduce el uso de efectivo. Sin embargo, este avance ha sido explotado por estafadores que utilizan técnicas sofisticadas para engañar a los usuarios. Como respuesta, la industria ha implementado medidas más estrictas para proteger a los consumidores, creando un entorno más seguro. Al mismo tiempo, los usuarios deben adoptar buenas prácticas para evitar fraudes, lo que motiva a las instituciones a seguir mejorando sus sistemas de seguridad (Ramirez-Asisi et al., 2022).

Desarrollar herramientas y estrategias enfocadas en la prevención de delitos en entornos digitales, con un énfasis especial en la protección de datos personales son indispensables en la actualidad, por lo tanto, es necesario complementar las medidas de identificación de vulnerabilidades ante la suplantación de identidad.

Este proyecto tiene como objetivo principal determinar la probabilidad de sufrir suplantación de identidad mediante la implementación de algoritmos de clasificación no supervisada, con la finalidad de realizar análisis precisos y generar predicciones que contribuyan a la toma de decisiones preventivas.

METODOLOGÍA

El proyecto se desarrolló utilizando como base la metodología ágil SCRUM, la cual permitió abordar de manera estructurada y colaborativa cada etapa del trabajo. Este enfoque facilitó la organización del proyecto en ciclos cortos (sprints), promoviendo la entrega de resultados parciales funcionales y adaptándose a las necesidades y cambios durante el desarrollo. Esta metodología permite la comunicación continua y la mejora iterativa, lo que facilita el cumplimiento de los objetivos del proyecto de manera eficiente (Gillespie, 2023). También fomenta una rápida adaptación a los cambios durante el desarrollo, asegurando que los productos finales sean relevantes y alineados con los requisitos del usuario final (Figura 1).

Figura 1. Fases de la investigación

Fases del Proyecto

Recolección de datos: En esta fase se diseñaron y aplicaron encuestas dirigidas a los usuarios para conocer su nivel de conocimiento y su comportamiento frente al phishing. Para ellos, se utilizó un cuestionario estructurado, el cual fue integrado directamente a la plataforma, lo que permitió recopilar información precisa y detallada de cómo interactúan los usuarios ante este tipo de amenazas (Duarte Sánchez y Guerrero Barreto, 2024).

Los códigos QR se utilizan cada vez más para redirigir a los usuarios a sitios fraudulentos a través de mensajes y correos electrónicos (Weinz et al., 2025). Esta práctica se aprovecha de la confianza que los usuarios depositan en los códigos QR al escanearlos desde sus dispositivos móviles.

Así mismo, las tiendas en línea falsas siguen siendo una táctica eficaz durante eventos de ventas como el Black Friday. En estos casos, los ciberdelincuentes replican sitios web legítimos y ofrecer productos a precios bajos con el objetivo de robar información financiera (Maldonado Ruiz, 2025), el 62% de las personas que ingresan en estos sitios proporcionan sus datos, debido a la confianza generada por los certificados SSL fraudulentos que imitan a las páginas legítimas.

El uso de inteligencia artificial en ataques de phishing está en auge, especialmente a través de técnicas como los deepfakes (Tapia Sánchez, 2025). Los ciberdelincuentes emplean Inteligencia Artificial para crear correos electrónicos altamente personalizados y fraudulentos que imitan a empleados o figuras de confianza, lo que hace más difícil detectar el fraude. IBM Security (Kosinski y Carruthers, 2025), indica que más del 43% de los correos maliciosos dirigen a sitios de phishing que simulan páginas de inicio de sesión de empresas legítimas, aumentando la efectividad del ataque.

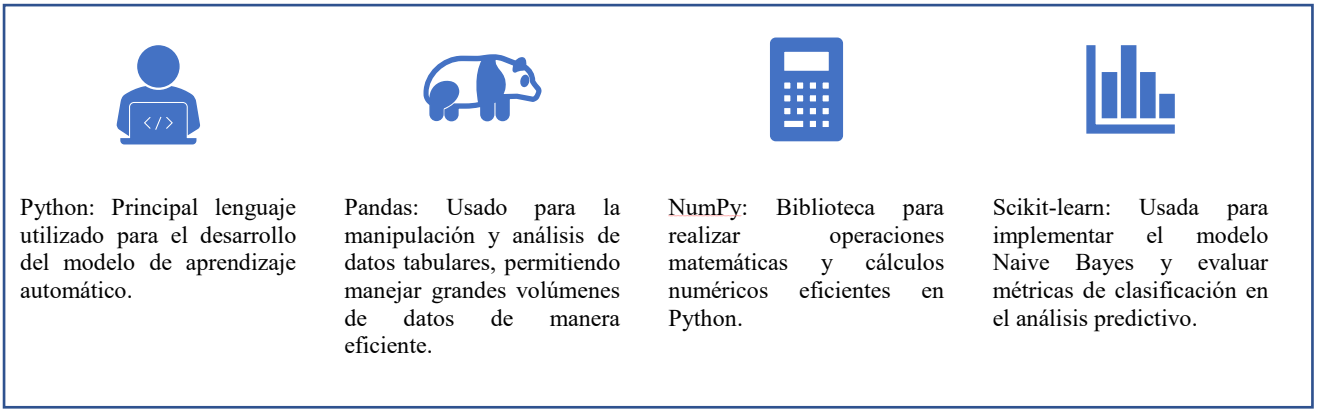
Construcción del modelo predictivo: Después de la recopilación de datos, se realizó el análisis y preprocesamiento de la información para garantizar su calidad. Se utilizaron seis algoritmos de Machine Learning: Regresión Lineal, KNN, Árbol de Decisión, Random Forest, Red Neuronal y Naive Bayes, para predecir la probabilidad de que un usuario sea víctima de phishing. Naive Bayes fue seleccionado como el óptimo debido a su balance entre simplicidad y rendimiento en datasets con distribuciones probabilísticas (Veziroğlu et al., 2024), logrando resultados consistentes en precisión y recall que lo hacen adecuado para este caso de estudio.

Desarrollo de la plataforma web: En esta fase se centró en el diseño y programación de una plataforma web funcional y accesible, utilizando Laravel como framework principal (Avilés Matute et al., 2020). Se integraron componentes visuales con Bootstrap para asegurar una interfaz intuitiva, responsiva y amigable para los usuarios finales, mejorando así la experiencia del usuario (Martínez Ramírez et al., 2024).

Integración del modelo predictivo y pruebas: El modelo de predicción fue integrado en la plataforma como un módulo, que permite analizar los datos de las encuestas y generar predicciones en tiempo real. Se realizaron pruebas exhaustivas para asegurar la precisión y la eficiencia del modelo en un entorno real (Muñoz Torres, 2024).

Herramientas Utilizadas

Figura 2 Análisis y Desarrollo del Modelo Predictivo:



Desarrollo de la Plataforma Web

Laravel: Framework PHP utilizado para la lógica del servidor y la integración del modelo MVC (Modelo-Vista-Controlador), facilitando la interacción con la base de datos y la gestión de la plataforma web.

Bootstrap: Herramienta de diseño web responsivo utilizada para crear interfaces accesibles y atractivas para los usuarios.

Gestión del Proyecto

GitHub: Plataforma para el control de versiones y la colaboración en equipo, que permitió gestionar el código y el progreso del proyecto de manera efectiva.

RESULTADOS Y DISCUSIÓN

Recolección de Información

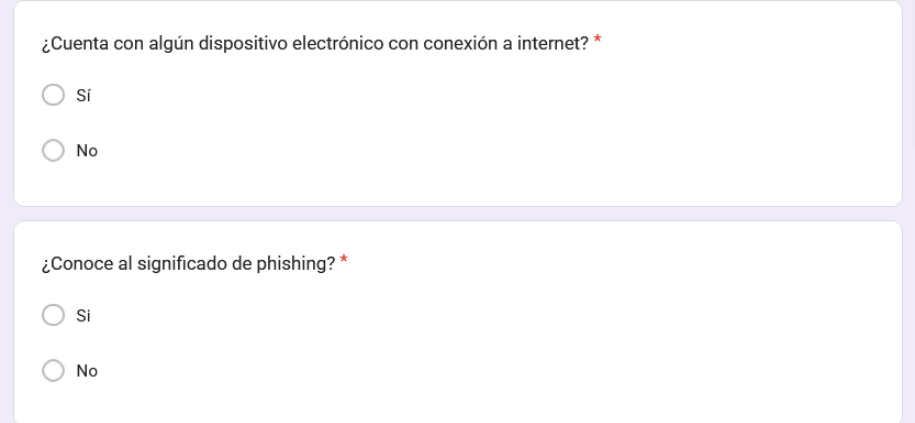
La primera etapa del proyecto se centró en el diseño e implementación de encuestas estructuradas para recolectar datos relacionados con el comportamiento y conocimiento de los usuarios frente al phishing (Figura 2). Estas encuestas tuvieron como propósito generar un conjunto de datos representativos que permitieran entrenar modelos de Machine Learning enfocados en predecir el riesgo de sufrir un ataque de phishing.

El cuestionario aplicado estuvo compuesto por reactivos con temas relacionados a:

- Frecuencia de interacción con correos electrónicos sospechosos.
- Conocimiento sobre técnicas de ingeniería social.

- Hábitos de navegación y uso de contraseñas.

Figura 2. Objeto de recolección de datos



Se utilizó la escala de Likert como formato de respuesta, dado que permite medir la intensidad de las percepciones y actitudes de los usuarios mediante niveles de acuerdo o desacuerdo ante afirmaciones específicas. La plataforma desarrollada ofrece una interfaz sencilla e intuitiva que facilita la asignación y gestión de las respuestas, permitiendo al administrador definirlas de manera rápida y precisa (Figura 3).

Figura 3. Asignación de valores a escala de Likert

La confiabilidad del instrumento fue evaluada mediante el coeficiente Alfa de Cronbach, obteniéndose un valor de 0.883138, el cual indica una alta consistencia interna entre los ítems del cuestionario. De acuerdo con la literatura especializada, valores de alfa comprendidos entre 0.70 y 0.90 son considerados indicativos de una adecuada fiabilidad interna en escalas unidimensionales, lo que confirma que los ítems se encuentran correctamente alineados y son coherentes en la medición del constructo evaluado (Colorado Romero et al., 2024).

El público objetivo para la recolección de datos estuvo conformado por jóvenes, un grupo caracterizado por su uso intensivo de redes sociales y plataformas digitales, lo que implica una mayor exposición a entornos en línea y, en consecuencia, una mayor susceptibilidad a ataques de phishing.

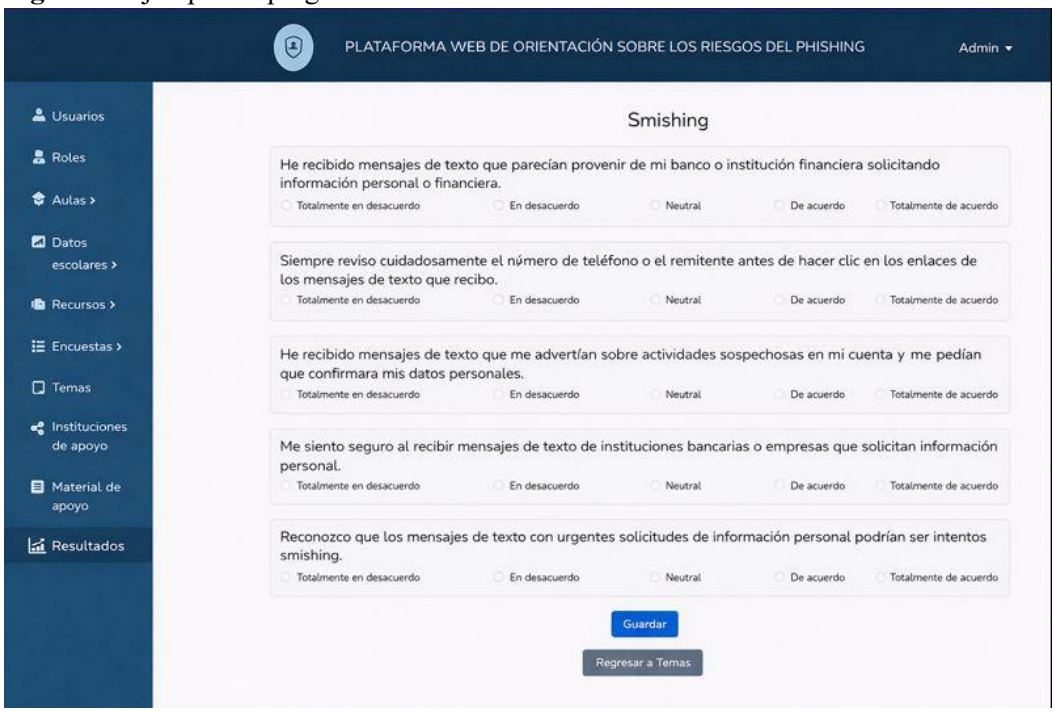
El proposito de la recolección de datos fue evaluar no solo el grado de conocimiento que estos jóvenes tienen sobre el phishing, sino también analizar comportamientos y actitudes que podrían incrementar su vulnerabilidad frente a este tipo de amenazas cibernéticas.

Para lograrlo, las encuestas incluyeron las siguientes áreas clave de evaluación:

1. Experiencias previas con phishing: Preguntas que exploraron si los participantes habían recibido correos electrónicos o mensajes sospechosos y cómo reaccionaron ante ellos.
2. Conocimiento sobre medidas de seguridad: Evaluación de la familiaridad de los jóvenes con prácticas como el uso de contraseñas seguras, autenticación en dos pasos y reconocimiento de señales comunes de phishing.
3. Capacidad para identificar amenazas: Ejercicios prácticos o preguntas diseñadas para medir su habilidad para reconocer elementos sospechosos en correos electrónicos o mensajes, como enlaces falsificados o dominios no confiables.

Esta etapa de recolección de datos permitió construir una base sólida y representativa, que sirvió como insumo principal para las siguientes fases del proyecto (Figura 4). Gracias a la calidad y variedad de la información recopilada, fue posible alimentar los modelos de Machine Learning y optimizar su capacidad predictiva en la identificación de riesgos de phishing.

Figura 4. Ejemplo de preguntas formuladas



Validación del Modelo

En la fase de validación del modelo, el primer paso fue el preprocesamiento de los datos, donde se realizó una limpieza exhaustiva para eliminar respuestas incompletas, inconsistentes o irrelevantes. Este proceso permitió asegurar que los datos fueran de alta calidad y estuvieran listos para el análisis. Además, se transformaron las variables categóricas en formatos adecuados para los modelos de Machine Learning (Figura 5).

Una vez preparados los datos, se procedió a entrenar diversos algoritmos de Machine Learning, incluyendo Naive Bayes, Regresión Lineal, Árboles de Decisión, Bosques Aleatorios, Redes Neuronales, y SVM.

El objetivo fue evaluar cómo cada modelo se ajustaba a los datos y cuál lograba mejores resultados en términos de precisión y capacidad de generalización.

Figura 5. Tabla de resultados

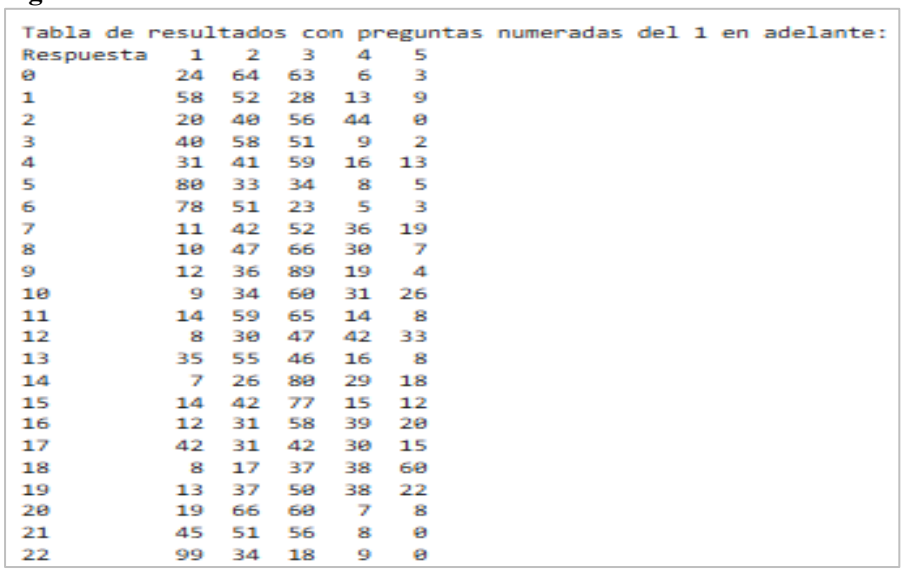


Tabla de resultados con preguntas numeradas del 1 en adelante:

Respuesta	1	2	3	4	5
0	24	64	63	6	3
1	58	52	28	13	9
2	20	40	56	44	0
3	40	58	51	9	2
4	31	41	59	16	13
5	80	33	34	8	5
6	78	51	23	5	3
7	11	42	52	36	19
8	10	47	66	30	7
9	12	36	89	19	4
10	9	34	60	31	26
11	14	59	65	14	8
12	8	30	47	42	33
13	35	55	46	16	8
14	7	26	80	29	18
15	14	42	77	15	12
16	12	31	58	39	20
17	42	31	42	30	15
18	8	17	37	38	60
19	13	37	50	38	22
20	19	66	60	7	8
21	45	51	56	8	0
22	99	34	18	9	0

Los primeros resultados mostraron que la Regresión Lineal era el modelo más robusto y preciso, destacándose en las pruebas con conjuntos de datos medianos a grandes (Tabla 1). Su rendimiento en la clasificación de respuestas fue consistente y confiable. Sin embargo, al proyectarse el uso de grandes volúmenes de datos, se determinó que, aunque es adecuada para datos medianos, no era el modelo óptimo para la implementación final (Gráfica 1).

Tabla 1. Comparación de modelos con los datos obtenidos

Modelo	Precisión	Recall	F1 Score	AUC
Regresión Lineal	84.74	76.92	80.10	87.34
KNN	62.63	58.21	60.90	59.77
Árbol de Decisión	73.12	80.34	76.52	81.32
Random Forest	91.45	88.99	89.21	90.47
Red Neuronal	78.23	65.49	71.92	74.89
Naive Bayes	63.55	70.12	66.88	68.99

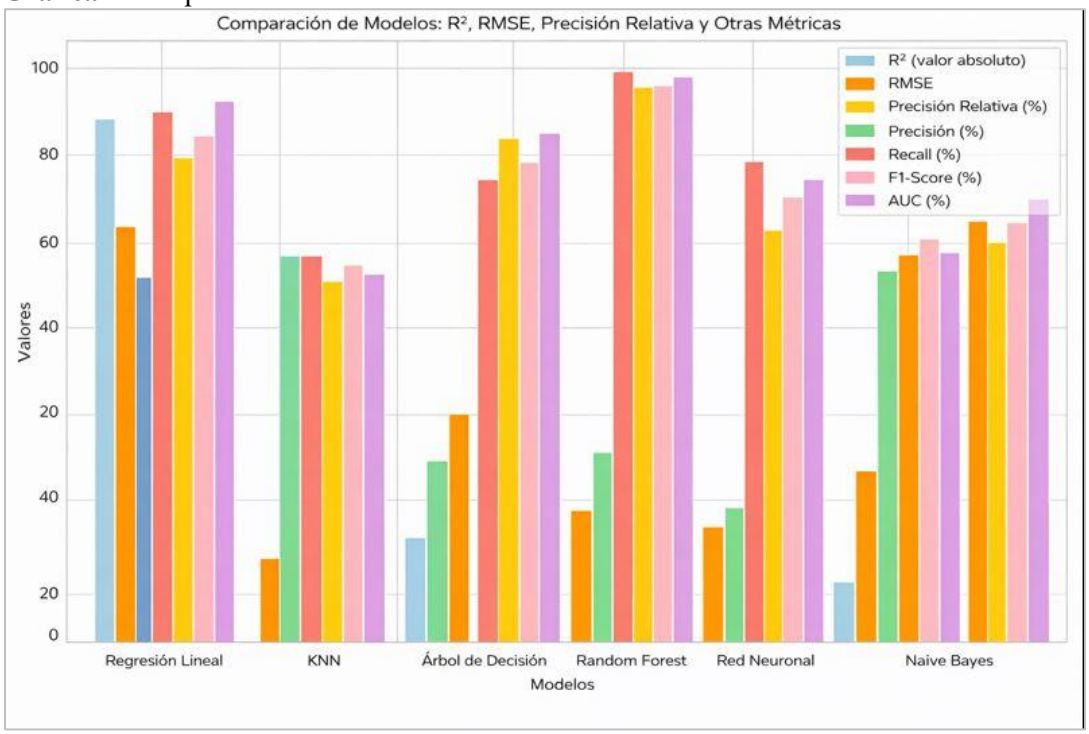
Tabla 2. Comparación de modelos con datos simulados

Modelo	Precisión	Recall	F1 Score	AUC
Regresión Lineal	84.95	84.95	84.95	92.02
KNN	83.62	81.94	82.77	90.63
Árbol de Decisión	65.92	68.56	67.21	66.67
Random Forest	80.33	80.60	80.47	88.63
Red Neuronal	83.51	81.27	82.37	88.67
Naive Bayes	83.50	84.62	84.05	91.95

Para evaluar completamente el rendimiento de los modelos, se llevó a cabo una simulación masiva con grandes volúmenes de datos generados (datagenerate), similares a los datos de un semestre completo (Gráfica 2).

Los resultados mostraron que Naive Bayes se comportó de manera similar a los modelos anteriores, logrando una precisión comparable en escenarios con grandes volúmenes de datos. A pesar de que ambos modelos tuvieron un rendimiento similar, Naive Bayes destacó por su mayor eficiencia en estos escenarios, consolidándose como la opción más adecuada para la implementación final (Tabla 2).

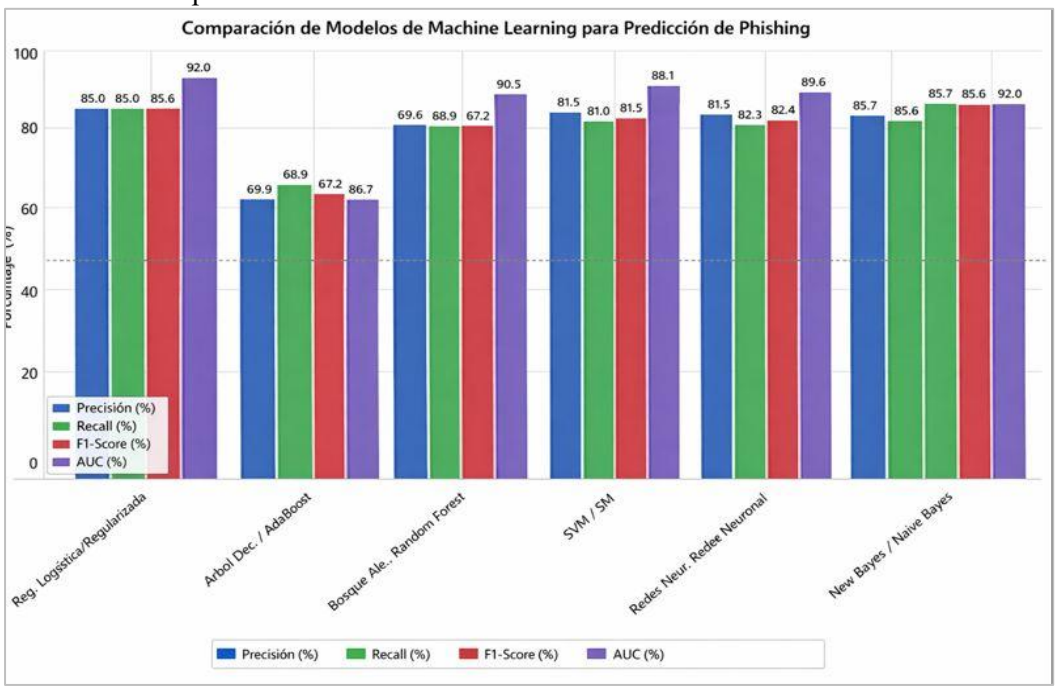
Gráfica 1.Comparación de modelos con los datos obtenidos



Integración

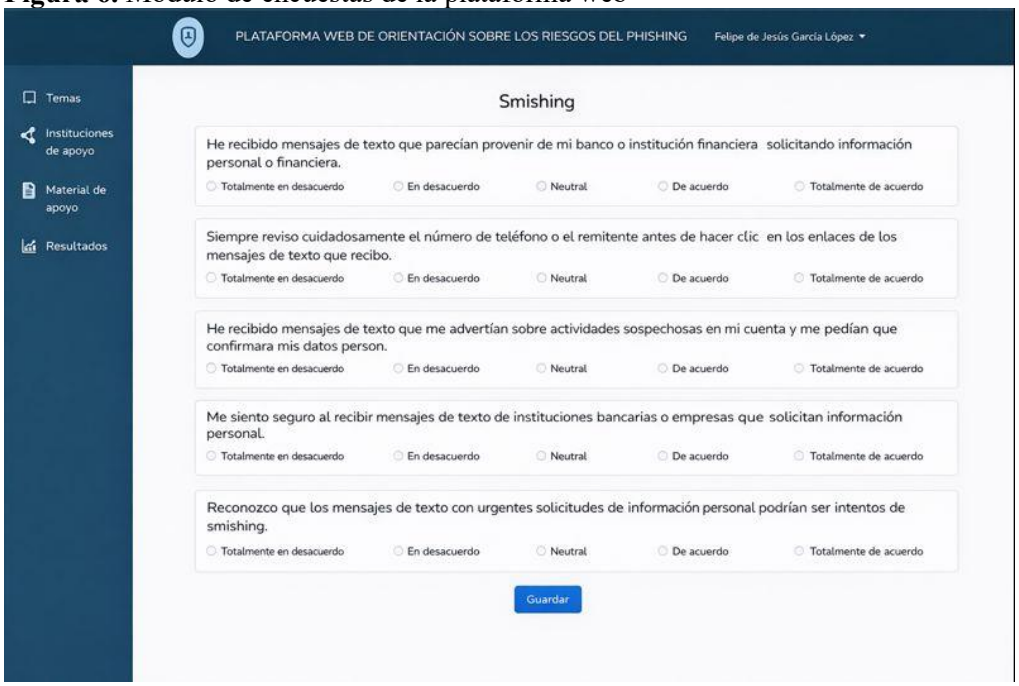
En esta fase, el objetivo fue integrar el modelo de Machine Learning Naive Bayes dentro de la plataforma web, específicamente en los módulos de encuestas y resultados. Este modelo se utilizó para predecir el riesgo de ser víctima de phishing. de los usuarios en función de sus respuestas a las encuestas, y proporcionar recomendaciones personalizadas para fortalecer su seguridad.

Gráfica 2. Comparación de modelos con datos simulados



La plataforma ya contaba con un módulo de encuestas funcional, que permitía a los usuarios completar cuestionarios relacionados con su conocimiento y comportamiento frente al phishing. Para asegurar la compatibilidad de este módulo con el modelo de Naive Bayes, se llevaron a cabo ajustes en el backend de la plataforma web (Figura 6).

Figura 6. Módulo de encuestas de la plataforma web



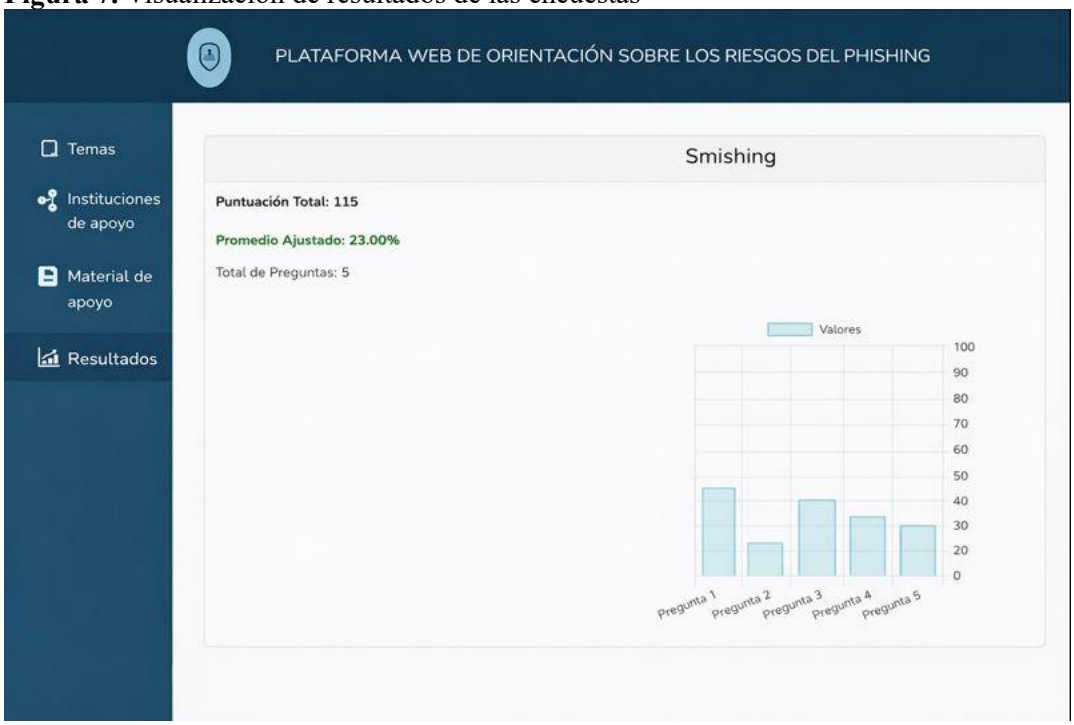
Las respuestas a las encuestas fueron estructuradas de manera que el modelo pudiera procesarlas fácilmente, clasificando las respuestas en categorías relevantes.

Para entrenar el modelo, se utilizó un conjunto de datos histórico recopilado de las respuestas de los usuarios anteriores en la plataforma. Dado que Naive Bayes es ideal para la clasificación de datos categóricos, las respuestas de los usuarios se adaptaron a categorías como “Totalmente en desacuerdo”,” En desacuerdo”, “Neutral”,” De acuerdo”, “Totalmente de acuerdo”, lo que permitió al modelo aprender patrones relacionados con las vulnerabilidades ante el phishing.

El modelo fue entrenado directamente en el servidor, y no fue necesario ningún proceso de integración externa. Una vez finalizado, el modelo estuvo listo para hacer predicciones en tiempo real basadas en las respuestas de nuevas encuestas.

El modelo de Naive Bayes se integró dentro del módulo de resultados de la plataforma, que ya mostraba las puntuaciones de los usuarios después de completar una encuesta. Con la integración del modelo, se añadió una capa adicional para mostrar la predicción del riesgo de phishing en función de las respuestas proporcionadas por el usuario (Figura 7).

Figura 7. Visualización de resultados de las encuestas



Predicción del Riesgo de Phishing: Cuando el usuario finaliza la encuesta, las respuestas son procesadas por el modelo de Naive Bayes directamente en el servidor. El modelo calcula la probabilidad de que el usuario esté en riesgo de ser víctima de un ataque de phishing y genera una predicción.

Ejecución y Análisis

En la fase final, denominada Ejecución y Análisis, se aplicaron las encuestas integradas con el modelo de Machine Learning en la plataforma web, alcanzando una muestra más amplia y variada de usuarios. Este paso fue crucial para probar la eficacia del modelo en condiciones reales, verificando su capacidad para identificar riesgos de phishing y proporcionar recomendaciones precisas y útiles para los usuarios.

Aplicación de Encuestas y Recolección de Datos

Las encuestas diseñadas, que incluían preguntas sobre comportamientos en línea, conocimientos sobre seguridad, y medidas de protección, se implementaron directamente en la plataforma. Al ser completadas por una gran cantidad de usuarios, se recolectaron datos diversos que cubrieron una amplia gama de perfiles y comportamientos. Este proceso permitió observar de manera directa cómo el modelo de Naive Bayes respondía a diferentes tipos de respuestas y la efectividad de sus predicciones en la evaluación del riesgo de phishing.

Análisis de Resultados y Validación del Modelo

Una vez recopiladas las respuestas, se procedió a realizar un análisis detallado utilizando herramientas estadísticas para identificar patrones y correlaciones significativas entre las respuestas de los usuarios y su susceptibilidad a ataques de phishing. Se examinaron diversos factores, tales como:

- Nivel de Conocimiento sobre Seguridad en Línea: Cuánto sabían los usuarios sobre las amenazas de phishing y cómo esto influía en su comportamiento en línea.
- Interacción con Correos y Mensajes Sospechosos: Frecuencia con la que los usuarios recibían y/o interactuaban con mensajes o correos electrónicos sospechosos.
- Medidas de Protección Adoptadas: Cuánto estaban los usuarios protegiendo su información personal con prácticas como la autenticación de dos pasos, el uso de antivirus, entre otros.

Este análisis permitió validar la precisión del modelo de Naive Bayes y explorar posibles mejoras en su rendimiento.

A través de las correlaciones encontradas, se pudo identificar en qué aspectos el modelo era más efectivo, y en qué situaciones necesitaba ajustes adicionales para proporcionar una predicción más precisa.

CONCLUSIONES

El modelo de Machine Learning Naive Bayes demostró ser una herramienta eficaz para predecir el riesgo de sufrir ataques de phishing, al analizar patrones y comportamientos de los usuarios. Este enfoque permitió identificar con precisión a aquellos más vulnerables a los ataques, destacando el potencial del modelo para ser integrado en sistemas de detección de amenazas en tiempo real, lo que ofrece una capa adicional de protección para los usuarios. Sin embargo, la investigación también reveló una falta de comprensión generalizada sobre los riesgos del phishing entre los usuarios, lo que subraya la necesidad de programas educativos más efectivos que complementen las soluciones tecnológicas.

Los resultados sugieren que los usuarios que participaron en las actividades educativas demostraron una atención más enfocada y objetiva sobre los riesgos del phishing, lo que permitió mejorar su conciencia y prácticas de seguridad en línea. Esto resalta la importancia de combinar la prevención tecnológica con la educación continua.

Una estrategia integral que combine la inteligencia artificial con la capacitación constante puede ser clave para mitigar los riesgos. Además, la plataforma desarrollada tiene el potencial de adaptarse y escalar para abordar otras ciberamenazas, ofreciendo una protección más sólida en el entorno digital.

REFERENCIAS BIBLIOGRAFICAS

Alcalá Casillas, M. G. (2024). Desafíos en México sobre la regulación de los ciberdelitos. DERECOM (Revista Internacional de Derecho de la Comunicación y las Nuevas Tecnologías)(35), 1-15. https://dialnet.unirioja.es/servlet/articulo?codigo=9352234

Alcalá Casillas, M., y Meléndez Ehrenzweig, M. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. PAAKAT: revista de tecnología y sociedad(24), 1-37. https://doi.org/https://dx.doi.org/10.32870/Pk.a13n24.759

Aredo-Vargas, G. K., Mlori-Ugarte, C. E., Cieza-Mostacero, S. E., Carbajal-Sanchez, H. A., y Bravo-Huivin, E. K. (2024). Papel de la Educación en Ciudadanía Digital en la Prevención de Ciberdelitos en el Perú. risti (Revista Ibérica de Sistemas e Tecnologías de Informação(E75),

299-313.

Avilés Matute, S., Avila-Pesantez, D., y Avila, L. (2020). Desarrollo de sistema Web basado en los frameworks de Laravel y VueJs, para la gestión por procesos: Un estudio de caso. Revista Peruana de Computación y Sistemas, 3(2), 3-10. https://doi.org/http://dx.doi.org/10.15381/rpcs.v3i2.19256

Código Penal, F. (28 de 11 de 2025). Cámara de Diputados del H. Congreso de la Unión. https://www.diputados.gob.mx/LeyesBiblio/ref/cpf.htm

Colorado Romero, J. R., Romero Montoya, M., Salazar Medina, M., Cabrera Zepeda, G., y Castillo Intriago, V. R. (2024). Análisis comparativo de los coeficientes Alfa de Cronbach, Omega de McDonald y Alfa Ordinal en la validación de cuestionarios. Estudios y Perspectivas Revista Científica y Académica, 4(4), 2738-2755. https://doi.org/https://doi.org/10.61384/r.c.a.v4i4

Diputado Monreal Ávila, R. (05 de 03 de 2025). Sistema de Información Legislativa. Iniciativa que reforma el título vigésimo del Código Penal Federal, en materia de Violencia Digital y los delitos derivados del uso de las Tecnologías de la Comunicación, la Información y los Sistemas de Inteligencia Artificial.: https://sil.gobernacion.gob.mx/Archivos/Documentos/2025/03/asun_4852026_20250311_1741201591.pdf#:~:text=En%20efecto%2C%20el%20C%C3%B3digo%20Penal%20Federal%20vigente,la%20persecuci%C3%B3n%20y%20sanci%C3%B3n%20de%20estos%20delitos.&text=%2D%20Se%20sanciona

Duarte Sánchez, D. D., y Guerrero Barreto, R. (2024). La encuesta como instrumento de recolección de datos, confiabilidad y validez en investigación científica. Revista de Ciencias Empresariales, Tributarias, Comerciales y Administrativa, 3(2). https://educaciontributaria.com.py/revista/index.php/rcetca/issue/view/5

García García, D. E. (2018). El phishing como delito de estafa informática. Comentario a la SAP Devalencia. Revista Boliviana de Derecho(25), 650-659. https://dialnet.unirioja.es/servlet/articulo?codigo=6263417

Gillespie, J. (31 de 05 de 2023). Scrum: Un enfoque de gestión basado en la evidencia. https://www-scrum-org.translate.goog/resources/blog/scrum-evidence-based-management-

approach?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

González Véliz, C., y Cuzcano Chavez, X. (2024). Desafíos y dimensiones de la desinformación en ALAC: deepfakes y la urgencia de proteger los derechos de las mujeres. Revista Digital de la Universidad Autónoma de Chiapas, 13(36), 162-175. https://doi.org/https://doi.org/10.31644/IMASD.36.2024.a19

IFT. (13 de 06 de 2024). Instituto Federal de Telecomunicaciones. Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2023.: https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/encuesta-nacional-sobre-disponibilidad-y-uso-de-tecnologias-de-la-informacion-en-los-hogares-endutih-1#:~:text=Durante%202023%2C%20las%20entidades%20federativas%20con%20los,y%20Chiapas%20(59.

Ige, T., Kiekintveld, C., Piplai, A., Wagler, A., Kolade, O., y Matti, B. H. (2024). An investigation into the performances of the. arXiv preprint arXiv, 1. https://doi.org/https://doi.org/10.48550/arXiv.2411.16751

Kosinski, M., y Carruthers, S. (19 de 05 de 2025). With generative AI, social engineering gets more dangerous—and harder to spot. IBM: https://www.ibm.com/think/insights/generative-ai-social-engineering

Ley Olimpia. (2025). Orden Jurídico Nacional. https://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf

López Grande, C. E., y Salvador Guadrón, R. (2016). Ingeniería Social: El ataque silencioso. Revista Tecnológica(8), 38-45.

Maldonado Ruiz, L. M. (2025). Elementos criminógenos de las tecnologías de la información y proliferación de la delincuencia informática. Ivestigación, Tecnología e Innovación, 17(23), 41-51. https://doi.org/https://doi.org/10.53591/iti.v17i23.1945

Martínez Galindo, G. (2024). Suplantación de identidad digital: hacia una necesaria tutela penal. Revista de Derecho Público, 72(1), 199-228. https://doi.org/https://doi.org/10.18543/ed7212024

Martínez Ramírez, V., Luciano Machorro, T., Martínez Rabanles, S., Osorio Ramírez, E. A., y Reyes Ramos, J. J. (2024). Optimización web móvil: El poder de bootstrap en el desarrollo adaptativo. 7(2), 284-294. https://doi.org/https://doi.org/10.61117/ipsumtec.v7i2.337

Montemayor Garza, M., y Tapia Cortes, C. (2022). Impacto y modos de uso de las redes sociales: Una revisión sistemática de literatura 2017-2021. New Trends in Qualitative Research, 12, 1-13. https://doi.org/https://doi.org/10.36367/ntqr.12.2022.e660

Montesinos González, S., Vázquez Cid de León, C., Maya Espinoza, I., y Gracida Gracida, E. B. (2020). Mejora Continua en una empresa en México: estudio desde el ciclo Deming. Revista Venezolana de Gerencia, 25(92), 1863-1883. https://www.redalyc.org/journal/290/29065286036/html/

Moreano Guerra, C. B., Escobar Erazo, T. E., Haro Haro, E. R., y Villagomez Valencia, P. A. (2024). Redes Sociales y su Impacto en el Entorno Digital de las Empresas. Ciencia Latina, Revista Multidisciplinar, 8(2), 831-857. https://doi.org/https://doi.org/10.37811/cl_rcm.v8i2.10531

Muñoz Torres, P. S. (2024). Modelo predictivo basado en algoritmos de machine learning para la estimación del peso de racimos de banano en una hacienda. Revista Latinoamericana de Ciencias Sociales y humanidades, 5(6), 986-1015. https://doi.org/https://doi.org/10.56712/latam.v5i6.3061

Olivares Romero, S., Rangel León, M. R., Chino Francisco, B., y Corte Cortés, M. (2025). El uso responsable de las redes sociales como herramienta de aprendizaje en la Educación Media Superior. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 6(2), 3309-3323. https://doi.org/https://doi.org/10.56712/latam.v6i2.3907

Oseda Gago, D., Durán Carhuamaca, A., Larico Uchamaco, G. R., Ramos Toledo, M. C., Palomino Quispe, H. A., Huarancca Contreras, P. P., y Medina Aliaga, J. L. (2024). Importancia de la ciberseguridad en la era digital. En J. A. Romero Palmera, y V. M. Calzolaio Cristofano, Ciberseguridad: Un enfoque interdisciplinario para la protección del mundo digital (pp. 3-8). Sello Editorial CITSA.

Peña Labrini, D. E. (2023). Ciberdelitos y criminalidad informática. Rol de la prevención en la expansión de la ciberdelincuencia. Informática y Derecho: Revista Iberoamericana de Derecho

Informático (segunda época)(13), 57-72. https://dialnet.unirioja.es/servlet/articulo?codigo=9265276

Protección de Datos, P. e. (14 de 11 de 2025). Cámara de Diputados del H. Congreso de la Unión. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ramirez-Asisi, E. H., Norabuena-Figueroa, R. P., Toledo-Quiñones, R. E., y Henostroza-Márquez-Mázmela, P. (2022). Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de Perú. Revista Científica General José María Córdova, 20(37), 209-224. https://doi.org/https://dx.doi.org/10.21830/19006586.791

Romero Mireles, L. L. (07 de 12 de 2023). Gaceta UNAM. Los mexicanos usan más internet que el promedio mundial: https://www.gaceta.unam.mx/uso-patologico-de-las-redes-sociales-es-un-fenomeno-en-crecimiento/

Tapia Sánchez, L. S. (2025). Cibercrimen:Un breve análisis doctrinal de los ciberdelitos y su relación con la inteligencia artificial. Revista Internacional de Desarrollo Humano y Sostenibilidad, 2(2), 183-208. https://doi.org/https://doi.org/10.51660/ridhs22316

UNICEF. (17 de 04 de 2024). UNICEF Comité Español. Ciberacoso: qué es, impacto y cómo detenerlo.: https://www.unicef.es/blog/educacion/ciberacoso-que-es-impacto-y-como-detenerlo

Veziroğlu, M., Eziroğlu, E., y Bucak, İ. Ö. (2024). Performance Comparison between Naive Bayes and Machine Learning Algorithms for News Classification. En İ. Ö. Bucak, Bayesian Inference - Recent Trends. IntechOpen. https://doi.org/10.5772/intechopen.1002778

Weinz, M., Zannone, N., Allodi, L., y Apruzzese, G. (2025). The Impact of Emerging Phishing Threats: Assessing Quishing and LLM-generated Phishing Emails against Organizations. ASIA CCS '25: Proceedings of the 20th ACM Asia Conference on Computer and Communications Security, 1550-1566. https://doi.org/https://doi.org/10.1145/3708821.373619