### 

### 

### **📄 Estructura del Documento en Word**

#### **📘 Portada**

* **Título del proyecto**
* Nombre del autor o equipo
* Profesores
* Fecha
* Logo institucional

### **1. Introducción**

* Breve descripción del problema
* Objetivo general y específicos
* Alcance del proyecto

### **2. Metodología: CRISP-DM**

#### **2.1. Comprensión del Negocio**

* Descripción del problema desde el punto de vista del negocio
* Objetivos del negocio
* Criterios de éxito

#### **2.2. Comprensión de los Datos**

* Descripción de la(s) fuente(s) de datos
* Estructura de los datos (variables, formatos, etc.)
* Problemas detectados (datos faltantes, errores, duplicados)

#### **2.3. Preparación de los Datos**

* Limpieza de datos
* Transformaciones realizadas (normalización, codificación, etc.): **homologacion**
* Selección de variables

#### **2.4. Modelado**

* Algoritmos seleccionados y justificación
* Proceso de entrenamiento y validación
* Métricas de evaluación
* Comparación entre modelos

#### **2.5. Evaluación**

* Análisis de resultados
* Validación con expertos o stakeholders
* Lecciones aprendidas
* Limitaciones

#### **2.6. Implementación**

* Plan de despliegue
* Herramientas utilizadas (ej. Streamlit, Power BI, API, etc.)
* Consideraciones para mantenimiento

### **3. Presupuesto**

| **Concepto** | **Cantidad** | **Costo Unitario** | **Total** |
| --- | --- | --- | --- |
| Licencias de software (ej. Anaconda, Power BI Pro) | 2 | $50.000 | $100.000 |
| Sueldos/Data Scientist (mes) | 1 | $4.000.000 | $4.000.000 |
| Infraestructura en la nube (ej. Azure, AWS) | 1 mes | $300.000 | $300.000 |
| Visualizaciones/Reportes | 1 | $200.000 | $200.000 |
| Otros gastos operativos | - | - | $150.000 |
| **Total estimado** |  |  | **$4.750.000** |

Puedes usar un formato de tabla en Word para hacer esto más claro. Si estás haciendo un trabajo académico, puedes justificar cada ítem.

### **4. Manejo del Contenido Relacionado (Apéndices / Anexos)**

* **Anexo A**: Diccionario de datos
* **Anexo B**: Código fuente (puedes incluir fragmentos o referencias a GitHub)
* **Anexo C**: Visualizaciones principales
* **Anexo D**: Detalles técnicos del modelo (hiperparámetros, curvas ROC, etc.)
* **Anexo E**: Plan de implementación técnica o de escalabilidad

### **5. Conclusiones y Recomendaciones**

* Conclusiones claves del análisis
* Recomendaciones para el negocio o para futuras investigaciones
* Consideraciones éticas

PhishEye

Luis Miguel Pedrozo

Jacobo Giraldo Rivera

Paolo Andrés Patiño Duque

Natalia Ramírez López

Jose Antonio Cely

Frank Yesid Zapata

Natalia Betancur

Andrés Felipe Sanchez

19/05/2025

Actualización de base de datos 27/09/2020



***Introducción***

## ***Escogimos el problema del phishing para nuestro modelo de machine learning debido a la creciente amenaza que representa en el ámbito de la ciberseguridad. El phishing es una técnica de ciberdelito que consiste en engañar a las personas para que revelen información confidencial, como contraseñas, datos bancarios o información personal, haciéndose pasar por entidades o personas de confianza mediante correos electrónicos, mensajes o sitios web fraudulentos. Esta amenaza es especialmente relevante porque explota la vulnerabilidad humana más que las tecnológicas, manipulando a las víctimas para que realicen acciones que comprometen su seguridad o la de sus organizaciones***

## ***Objetivo General***

El objetivo general de este proyecto es diseñar, desarrollar y evaluar un modelo de machine learning capaz de detectar de manera automática y precisa ataques de phishing, específicamente en sitios web y correos electrónicos, con el fin de mejorar la seguridad informática y proteger a los usuarios contra fraudes digitales. Este modelo buscará identificar patrones y características distintivas de sitios web o mensajes fraudulentos mediante técnicas avanzadas de aprendizaje supervisado, integrando procesos como la recolección y preparación de datos, selección de algoritmos, entrenamiento y evaluación del rendimiento del sistema.

En resumen, este objetivo general busca aprovechar el potencial del machine learning para crear un sistema integral y robusto de detección de phishing, que pueda ser utilizado como una herramienta preventiva y de apoyo en la defensa contra amenazas cibernéticas, aumentando la seguridad y confianza en el entorno digital

## 

## 

## ***Objetivos Específicos***

## Recopilar y analizar datos relevantes sobre ataques de phishing, incluyendo correos electrónicos, URLs y características comunes de estos ataques.

## Preprocesar y limpiar los datos para mejorar la calidad del entrenamiento del modelo, aplicando técnicas de extracción de características y selección de variables.

## Desarrollar y entrenar diferentes algoritmos de machine learning para comparar su efectividad en la detección de phishing.

## 

***Alcance del proyecto***

El proyecto abarcará la creación de un prototipo funcional capaz de clasificar de manera efectiva entre contenido legítimo y fraudulento, con especial atención en minimizar falsos positivos y adaptarse a nuevas variantes de phishing mediante la actualización continua del modelo. Aunque no se contempla el despliegue en un entorno productivo, el desarrollo se enfocará en validar la viabilidad y eficacia del sistema mediante pruebas con conjuntos de datos reales y representativos.

En resumen, el proyecto pretende sentar las bases para una herramienta automatizada que contribuya a la mejora de la ciberseguridad, facilitando la detección temprana y precisa de ataques de phishing y apoyando la protección de usuarios y organizaciones frente a esta creciente amenaza digital

***Descripción del problema desde el punto de vista del negocio***

Desde el punto de vista de negocio, el problema del phishing representa una amenaza crítica que genera pérdidas financieras directas e indirectas significativas para las empresas. Los ataques de phishing pueden provocar transferencias bancarias no autorizadas, robo de información sensible de empleados y clientes, y comprometer la propiedad intelectual, lo que conlleva costos elevados en servicios legales, recuperación de datos y mejoras en la seguridad. Además, estos ataques causan interrupciones operativas que afectan la productividad y la continuidad del negocio, generando pérdidas adicionales por tiempo de inactividad.

El impacto reputacional es otro aspecto clave, ya que un ataque exitoso puede erosionar la confianza de clientes, socios y el público, dificultando la retención y captación de clientes y afectando negativamente la imagen corporativa a largo plazo. En términos económicos, el phishing ha incrementado los costos de ciberseguridad y respuesta ante incidentes, con pérdidas que pueden alcanzar millones de dólares anuales en grandes organizaciones, incluyendo gastos en mitigación, formación y prevención.

***Objetivos de negocio***

* Reducir pérdidas financieras causadas por fraudes y ataques de phishing, minimizando el impacto económico directo e indirecto en la empresa.
* Mejorar la eficiencia operativa al automatizar la detección de ataques, disminuyendo el tiempo y recursos dedicados a la revisión manual de posibles fraudes.
* Incrementar la precisión en la identificación de amenazas, reduciendo falsos positivos y negativos para optimizar la respuesta y evitar interrupciones innecesarias en procesos legítimos.
* Proteger la reputación y confianza de la empresa frente a clientes y socios, evitando daños reputacionales derivados de brechas de seguridad o ataques exitosos.

***Criterios de éxito***

* Alta precisión en la detección, logrando una tasa de acierto superior al 90-95% para identificar correctamente sitios web y correos electrónicos de phishing, minimizando falsos positivos y falsos negativos.
* Capacidad de generalización y adaptación, donde el modelo pueda detectar nuevas variantes de phishing basándose en patrones aprendidos, incluso con datos no vistos previamente.
* Uso eficiente de características relevantes, como análisis de URLs, edad y certificación del dominio, contenido textual y metadatos, que permitan mejorar la exactitud del modelo sin requerir procesos computacionales excesivos.
* Implementación de un prototipo funcional, por ejemplo, una extensión para navegador o herramienta que evalúe en tiempo real la probabilidad de phishing de una página o mensaje, demostrando aplicabilidad práctica.

***Comprensión de los datos***

<https://www.kaggle.com/datasets/shashwatwork/web-page-phishing-detection-dataset>

Formato: CCV

Cantidad de columnas:90

Cantidad de fila: 11.160

Datos faltantes: 0

Errores: 0

Duplicados: 0

El conjunto de datos proporcionado incluye 11 430 URL con 87 características extraídas. Está diseñado para usarse como referencia para sistemas de detección de phishing basados ​​en aprendizaje automático. Las características provienen de tres clases diferentes: 56 extraídas de la estructura y sintaxis de las URL, 24 del contenido de sus páginas correspondientes y 7 extraídas mediante consultas a servicios externos. El conjunto de datos está equilibrado y contiene exactamente un 50 % de URLs de phishing y un 50 % de URLs legítimas.

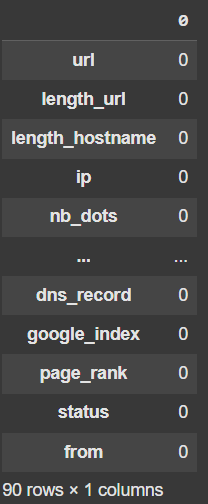
Variables:

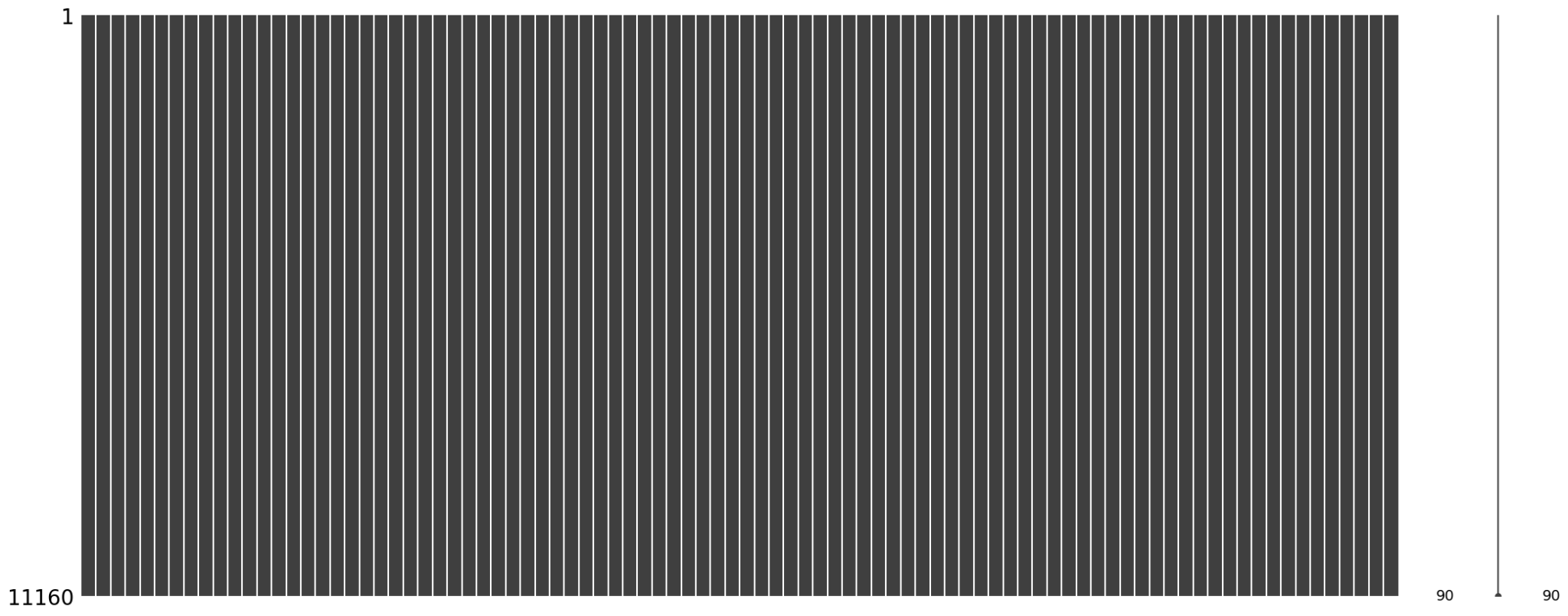
| • url | Dirección web que se está analizando. |
| --- | --- |
| • length\_url | Longitud total de la URL. |
| • length\_hostname | Longitud del nombre del host en la URL. |
| • ip | Indica si la URL contiene una dirección IP en lugar de un dominio. |
| • nb\_dots | Número de puntos en la URL. |
| • nb\_hyphens | Número de guiones en la URL. |
| • nb\_at | Número de caracteres "@" en la URL. |
| • nb\_qm | Número de signos de interrogación en la URL. |
| • nb\_and | Número de caracteres "&" en la URL. |
| • nb\_or | Número de caracteres "OR" en la URL. |
| • nb\_eq | Número de signos "=" en la URL. |
| • nb\_underscore | Número de guiones bajos en la URL. |
| • nb\_tilde | Número de caracteres "~" en la URL. |
| • nb\_percent | Número de caracteres "%" en la URL. |
| • nb\_slash | Número de barras "/" en la URL. |
| • nb\_star | Número de caracteres "\*" en la URL. |
| • nb\_colon | Número de caracteres " en la URL. |
| • nb\_comma | Número de comas en la URL. |
| • nb\_semicolumn | Número de puntos y comas en la URL. |
| • nb\_dollar | Número de caracteres "$" en la URL. |
| • nb\_space | Número de espacios en la URL. |
| • nb\_www | Número de veces que aparece "www" en la URL. |
| • nb\_com | Número de veces que aparece ".com" en la URL. |
| • nb\_dslash | Número de dobles barras "//" en la URL. |
| • http\_in\_path | Indica si "http" aparece en la ruta de la URL. |
| • https\_token | Indica si "https" aparece en la URL. |
| • ratio\_digits\_url | Proporción de dígitos en la URL. |
| • ratio\_digits\_host | Proporción de dígitos en el nombre del host. |
| • punycode | Indica si la URL usa codificación Punycode. |
| • port | Número de puerto utilizado en la URL. |
| • tld\_in\_path | Indica si el dominio de nivel superior (TLD) aparece en la ruta. |
| • tld\_in\_subdomain | Indica si el TLD aparece en el subdominio. |
| • abnormal\_subdomain | Evalúa si hay subdominios inusuales. |
| • nb\_subdomains | Número de subdominios en la URL. |
| • prefix\_suffix | Indica si hay prefijos o sufijos sospechosos en el dominio. |
| • random\_domain | Evalúa si el dominio parece aleatorio. |
| • shortening\_service | Indica si la URL proviene de un servicio de acortamiento. |
| • path\_extension | Indica si la URL tiene una extensión de archivo en la ruta. |
| • nb\_redirection | Número de redirecciones internas. |
| • nb\_external\_redirection | Número de redirecciones externas. |
| • length\_words\_raw | Longitud total de las palabras en la URL. |
| • char\_repeat | Indica si hay caracteres repetidos en la URL. |
| • shortest\_words\_raw | Longitud de la palabra más corta en la URL. |
| • shortest\_word\_host | Longitud de la palabra más corta en el host. |
| • shortest\_word\_path | Longitud de la palabra más corta en la ruta. |
| • longest\_words\_raw | Longitud de la palabra más larga en la URL. |
| • longest\_word\_host | Longitud de la palabra más larga en el host. |
| • longest\_word\_path | Longitud de la palabra más larga en la ruta. |
| • avg\_words\_raw | Promedio de longitud de palabras en la URL. |
| • avg\_word\_host | Promedio de longitud de palabras en el host. |
| • avg\_word\_path | Promedio de longitud de palabras en la ruta. |
| • phish\_hints | Indicadores de posible phishing. |
| • domain\_in\_brand | Indica si el dominio contiene nombres de marcas conocidas. |
| • brand\_in\_subdomain | Indica si la marca aparece en el subdominio. |
| • brand\_in\_path | Indica si la marca aparece en la ruta. |
| • suspecious\_tld | Evalúa si el TLD es sospechoso. |
| • statistical\_report | Información estadística sobre la URL. |
| • nb\_hyperlinks | Número total de hipervínculos en la página. |
| • ratio\_intHyperlinks | Proporción de enlaces internos. |
| • ratio\_extHyperlinks | Proporción de enlaces externos. |
| • ratio\_nullHyperlinks | Proporción de enlaces vacíos o nulos. |
| • nb\_extCSS | Número de hojas de estilo externas. |
| • ratio\_intRedirection | Proporción de redirecciones internas. |
| • ratio\_extRedirection | Proporción de redirecciones externas. |
| • ratio\_intErrors | Proporción de errores internos en la página. |
| • ratio\_extErrors | Proporción de errores externos en la página. |
| • login\_form | Indica si la página tiene un formulario de inicio de sesión. |
| • external\_favicon | Indica si el favicon proviene de un dominio externo. |
| • links\_in\_tags | Número de enlaces dentro de etiquetas HTML. |
| • submit\_email | Indica si la página permite enviar correos electrónicos. |
| • ratio\_intMedia | Proporción de contenido multimedia interno. |
| • ratio\_extMedia | Proporción de contenido multimedia externo. |
| • sfh | Evalúa si los formularios son seguros. |
| • iframe | Indica si la página usa iframes. |
| • popup\_window | Indica si la página tiene ventanas emergentes. |
| • safe\_anchor | Evalúa si los enlaces son seguros. |
| • onmouseover | Indica si hay eventos "onmouseover" en la página. |
| • right\_clic | Indica si el clic derecho está bloqueado. |
| • empty\_title | Indica si el título de la página está vacío. |
| • domain\_in\_title | Indica si el dominio aparece en el título. |
| • domain\_with\_copyright | Indica si el dominio aparece en el aviso de derechos de autor. |
| • whois\_registered\_domain | Información sobre el registro del dominio. |
| • domain\_registration\_length | Duración del registro del dominio. |
| • domain\_age | Antigüedad del dominio. |
| • web\_traffic | Métricas de tráfico web. |
| • dns\_record | Información sobre los registros DNS del dominio. |
| • google\_index | Indica si la página está indexada en Google. |
| • page\_rank | Clasificación de la página en buscadores. |
| • status | Estado de la URL (puede indicar si es legítima o sospechosa). |
| • from | Fuente de la URL. |

***Preparación de los datos***

* Limpieza de datos:

Al momento de descargar la BBDD no tuvimos que hacer ninguna limpieza, ya que en las columnas no venia ningun dato vacío como lo podemos ver a continuación:





* Transformaciones realizadas:

Lo que se hizo en la BBDD fue una homologación - añadir el país de origen de donde probablemente puede ser la URL.

* ***Selección de variables:***

En la primer columna que es donde se encuentran las URL que se están verificando es de allí de donde se están sacando las características y son los datos que nos encontramos en el resto de columnas, la columna de **“status”** es nuestra etiqueta y no tuvimos que modificar nada en esta columna.

#### **2.4. Modelado**

***Algoritmos seleccionados y justificación***

Para elegir el mejor modelo, seguimos un proceso ordenado y basado en pruebas con nuestra base de datos.

Primero, preparamos y limpiamos los datos que contienen ejemplos de URLs o correos etiquetados como phishing o legítimos. Luego, probamos varios modelos populares de clasificación, como Random Forest, SVM y LGBMClassifier, para ver cuál funcionaba mejor con nuestros datos.

Para comparar los modelos, usamos métricas como la precisión (qué tan bien identifica correctamente los casos) y también tomamos en cuenta el tiempo que tardaba cada modelo en entrenarse. Después de evaluar todos, vimos que el modelo LGBMClassifier obtuvo un 97% de precisión, que fue el mejor resultado, además de ser rápido y eficiente.

Por eso, decidimos en equipo elegir LGBMClassifier para nuestro proyecto. Este modelo no solo tiene un alto porcentaje de aciertos, sino que también es capaz de manejar bien los datos y adaptarse a diferentes patrones que pueden indicar phishing.

Esta elección está respaldada por estudios y casos similares en los que LGBMClassifier ha demostrado ser efectivo para detectar fraudes y ataques cibernéticos. En resumen, seleccionamos este modelo porque nos ofrece un buen equilibrio entre precisión y rapidez, lo que es muy importante para un sistema que debe detectar ataques de forma confiable y rápida.

***Proceso de entrenamiento y validación***

Durante el entrenamiento de nuestro modelo LGBMClassifier, observamos varios detalles importantes que nos ayudan a entender cómo funciona y cómo se ajustó a nuestros datos.

Primero, el conjunto de entrenamiento estaba compuesto por 8,928 muestras, de las cuales 4,361 eran positivas y 4,567 negativas. Esto significa que las clases están bastante equilibradas, aunque hay un ligero predominio de las negativas. Para manejar este pequeño desbalance, LightGBM puede ajustar internamente el peso de las clases, pero en nuestro caso, dado que la diferencia no es tan grande, no fue necesario hacer un ajuste manual significativo.

El modelo utiliza una técnica llamada "multi-threading" para acelerar el proceso de entrenamiento, específicamente el modo "row-wise", que significa que el procesamiento se hace por filas de datos. Esto es eficiente para conjuntos de datos como el nuestro, con casi 9,000 muestras y 72 características. Además, LightGBM convierte las características continuas en una cantidad limitada de "bins" o intervalos discretos — en nuestro caso, un total de 5,054 bins — lo que ayuda a que el entrenamiento sea más rápido y a evitar el sobreajuste.

Antes de comenzar el entrenamiento, el modelo calcula una puntuación inicial basada en la proporción de clases positivas y negativas. En nuestro caso, esta puntuación fue aproximadamente -0.046, lo que indica que el modelo parte de un punto cercano a un balance entre ambas clases y luego mejora mediante iteraciones sucesivas.

En resumen, el proceso de entrenamiento con LightGBM fue eficiente y adecuado para nuestro problema, gracias a su capacidad para manejar grandes cantidades de datos y características, así como a su forma inteligente de discretizar los datos y paralelizar el cálculo. Para futuras mejoras, podríamos experimentar con parámetros como el número de bins o ajustar el peso de las clases si detectamos un desbalance más fuerte.

***Métricas de evaluación***

Estas métricas reflejan que nuestro modelo LGBMClassifier tiene un desempeño muy bueno para distinguir entre sitios legítimos y phishing, con una alta precisión y sensibilidad en ambas clases. Esto es especialmente importante en problemas de seguridad, donde tanto evitar falsos positivos como falsos negativos es crítico.

Además, el valor equilibrado del F1-score confirma que el modelo no está sesgado hacia ninguna clase, lo que es coherente con el balance de clases en nuestros datos.

Para futuras mejoras, podríamos analizar otras métricas complementarias como la curva ROC-AUC o el estadístico KS, que miden la capacidad discriminativa del modelo en diferentes umbrales, pero con estas métricas ya tenemos una base sólida para validar la efectividad del modelo.

***Comparación entre modelos***

Comparando varios modelos, elegimos LGBMClassifier porque logró un excelente desempeño con un accuracy y F1-score de 0.97, igualando a otros modelos como RandomForest, pero con un tiempo de entrenamiento mucho menor (0.65 segundos frente a más de 1 segundo en otros casos).

Además, LGBMClassifier es eficiente, rápido y flexible para ajustar hiperparámetros, lo que lo hace ideal para nuestro problema. Por estas razones, consideramos que es la mejor opción para nuestro proyecto, ya que combina precisión y velocidad de manera óptima.

#### **2.5. Evaluación**

***Análisis de resultados***

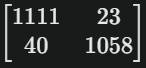
Después de entrenar y evaluar nuestro modelo LGBMClassifier, obtuvimos una precisión global de aproximadamente 0.97, lo que indica que el 97% de las predicciones fueron correctas en el conjunto de prueba. Este valor de precisión refleja la capacidad general del modelo para clasificar correctamente tanto sitios legítimos como phishing.

El reporte de clasificación nos muestra métricas específicas para cada clase:

* Precisión (precision): Para la clase "legitimate" es 0.97 y para "phishing" es 0.98. Esto significa que cuando el modelo predice una clase, lo hace correctamente en el 97-98% de los casos, lo que reduce los falsos positivos.
* Recall (sensibilidad): Es 0.98 para "legitimate" y 0.96 para "phishing". Esto indica que el modelo detecta correctamente el 96-98% de los casos reales de cada clase, minimizando los falsos negativos.
* F1-score: Con valores de 0.97 para ambas clases, esta métrica combina precisión y recall, mostrando un buen equilibrio entre ambas.

El soporte (support) indica que se evaluaron 1,134 muestras legítimas y 1,098 phishing, lo que confirma un conjunto de prueba balanceado.

La matriz de confusión complementa esta información:



* 1111 legítimos fueron correctamente clasificados (verdaderos positivos para "legitimate").
* 23 legítimos fueron clasificados erróneamente como phishing (falsos negativos para "legitimate").
* 40 phishing fueron clasificados erróneamente como legítimos (falsos negativos para "phishing").
* 1058 phishing fueron correctamente clasificados (verdaderos positivos para "phishing").

Esta matriz muestra que el modelo tiene un bajo número de errores en ambas clases, lo que confirma su alta efectividad.

En resumen, el modelo LGBMClassifier presenta un desempeño sólido, con alta precisión, recall y F1-score, lo que indica que es capaz de identificar correctamente tanto sitios legítimos como phishing con muy pocos errores. La matriz de confusión refuerza esta conclusión al mostrar que los falsos positivos y falsos negativos son mínimos, lo cual es crucial en aplicaciones de seguridad para evitar tanto alarmas falsas como omisiones peligrosas.

***Validación con expertos o stakeholders***

Al explicar estas métricas a los stakeholders, destacamos que el modelo no solo es técnicamente sólido, sino que también cumple con los requisitos de seguridad y confiabilidad necesarios para proteger a los usuarios contra ataques de phishing. La alta precisión y recall aseguran que se minimizan tanto las falsas alarmas como las omisiones, lo que protege la experiencia del usuario y reduce riesgos para la organización.

Además, al presentar estos resultados con claridad, facilitamos la toma de decisiones informadas sobre la implementación y posibles mejoras del sistema, alineando expectativas técnicas con objetivos de negocio y seguridad.

***Lecciones aprendidas***

Las lecciones aprendidas representan el conocimiento valioso que se obtiene a partir de la reflexión crítica sobre la experiencia durante el desarrollo del proyecto, y su correcta gestión contribuye a mejorar futuros trabajos. En el contexto de nuestro proyecto de machine learning con LGBMClassifier, estas lecciones se fundamentan en aspectos técnicos y de gestión que impactaron directamente en el éxito del modelo y la calidad del proceso.

1. Importancia del preprocesamiento y balanceo de datos  
   La fase de preparación de datos es clave para el desempeño del modelo, tal como indican los ciclos de vida de machine learning que enfatizan la necesidad de un análisis profundo y limpieza de datos antes del entrenamiento. En nuestro caso, identificar y manejar el balance entre clases permitió evitar sesgos y mejorar la precisión general.
2. Elección del modelo adecuado según recursos y problema  
   La comparación entre modelos mostró que no siempre el más complejo es el mejor, sino el que equilibra precisión y eficiencia. Esto coincide con prácticas recomendadas en ingeniería de modelos, donde se prioriza la escalabilidad y rapidez sin sacrificar la calidad. LGBMClassifier destacó por su rapidez y buen desempeño, lo que fue fundamental para nuestro proyecto.
3. Comunicación efectiva de resultados con expertos y stakeholders  
   Validar métricas y resultados con expertos facilitó la interpretación y aceptación del modelo, alineando aspectos técnicos con objetivos de negocio y seguridad. La literatura sobre gestión de proyectos resalta que compartir aprendizajes y resultados claros es esencial para la toma de decisiones informadas y para asegurar el apoyo de todas las partes involucradas.
4. Uso de la matriz de confusión para comprender errores  
   Más allá de las métricas globales, la matriz de confusión permitió identificar el tipo y cantidad de errores cometidos, lo que es crucial para evaluar riesgos en aplicaciones sensibles como la detección de phishing. Este enfoque detallado es una práctica estándar para mejorar la robustez del modelo.
5. Proceso iterativo de ajuste y optimización  
   El ajuste de hiperparámetros y la experimentación constante reflejan el ciclo iterativo del machine learning, donde se monitorea y mejora el modelo en función de métricas y resultados. Esta experiencia reafirma que la optimización es un proceso continuo y necesario para alcanzar el mejor desempeño.
6. Documentación y registro sistemático  
   Mantener un registro claro de experimentos, parámetros y resultados es fundamental para la reproducibilidad y aprendizaje organizacional, tal como indican los modelos de gestión de lecciones aprendidas. Esto facilita no solo la mejora continua sino también la transferencia de conocimiento a futuros proyectos.

***Limitaciones***

Las principales limitaciones que se pueden presentar en un proyecto basado en un modelo de machine learning como LGBMClassifier son las siguientes:

1. Calidad y cantidad de datos  
   El rendimiento del modelo depende en gran medida de contar con datos suficientes, limpios y representativos. Datos con ruido, sesgos o insuficientes pueden afectar la capacidad del modelo para generalizar correctamente a nuevos casos, lo que puede generar errores o resultados poco confiables.
2. Sesgo en los datos y en el modelo  
   Si el conjunto de datos de entrenamiento no refleja adecuadamente la diversidad del problema real, el modelo puede aprender patrones sesgados, lo que impacta en su equidad y precisión. Esto es especialmente crítico en problemas de seguridad como la detección de phishing, donde un sesgo puede aumentar falsos negativos o positivos.
3. Interpretabilidad del modelo  
   Aunque LGBM es eficiente y preciso, su naturaleza basada en ensamblajes de árboles puede dificultar la interpretación clara de por qué se toman ciertas decisiones, lo que es un reto cuando se requiere explicar resultados a usuarios o stakeholders.
4. Ajuste y optimización de hiperparámetros  
   Encontrar la configuración óptima para parámetros como número de árboles, tasa de aprendizaje o número de hojas es un proceso iterativo y puede ser costoso en tiempo y recursos. Un mal ajuste puede llevar a sobreajuste o bajo ajuste, afectando la capacidad predictiva.
5. Limitaciones computacionales  
   Aunque LGBM es más eficiente que otros modelos, entrenar con grandes volúmenes de datos o realizar múltiples experimentos puede requerir recursos computacionales importantes, especialmente si se busca optimizar hiperparámetros o implementar validaciones cruzadas extensas.
6. Generalización a datos nuevos o cambiantes  
   Los modelos pueden perder precisión si las características del problema cambian con el tiempo (drift de datos), lo que exige actualizar y reentrenar periódicamente el modelo para mantener su efectividad.
7. Aspectos éticos y de responsabilidad  
   En aplicaciones sensibles, como la detección de phishing, es importante considerar quién asume la responsabilidad en caso de errores del modelo y cómo se gestionan los posibles impactos negativos, un aspecto que va más allá de la técnica y requiere políticas claras.

Estas limitaciones no invalidan el uso de LGBMClassifier, pero sí subrayan la necesidad de un manejo cuidadoso de los datos, un ajuste riguroso del modelo, y una comunicación transparente con los usuarios y stakeholders para asegurar un uso responsable y efectivo del sistema.

#### **2.6. Implementación**

Plan de despliegue

## 1. Preparación y Validación Final del Modelo

* Confirmar que el modelo LGBMClassifier está entrenado y validado con métricas satisfactorias (precisión, recall, F1-score, matriz de confusión).
* Guardar el modelo entrenado en un formato serializado (por ejemplo, archivo .pkl o formato nativo de LightGBM) para su reutilización.

## 2. Preparación del Entorno de Producción

* Definir la infraestructura donde se desplegará el modelo: servidor local, nube (AWS, Azure, Google Cloud) o entorno híbrido.
* Configurar el hardware necesario (CPU/GPU, memoria) y el sistema operativo compatible.
* Instalar las dependencias y librerías necesarias (LightGBM, frameworks web, librerías de datos).

## 3. Desarrollo de la API o Servicio de Predicción

* Construir una API RESTful o servicio web que reciba solicitudes de predicción con datos nuevos y devuelva las predicciones generadas por el modelo.
* Implementar validaciones de entrada para asegurar que los datos recibidos estén en el formato esperado.
* Garantizar tiempos de respuesta adecuados para el tipo de predicción (en tiempo real o por lotes).

## 4. Integración con Sistemas y Usuarios Finales

* Integrar la API o servicio con las aplicaciones o plataformas que consumirán las predicciones (por ejemplo, sistemas de monitoreo, dashboards, aplicaciones móviles o web).
* Definir los endpoints y protocolos de comunicación (HTTP, colas de mensajes, sockets) según las necesidades.

## 5. Pruebas en Entorno de Producción

* Realizar pruebas funcionales y de carga para verificar que el modelo responde correctamente bajo condiciones reales.
* Validar que las predicciones sean coherentes y que no haya errores en el proceso de integración.

## 6. Implementación de Monitoreo y Mantenimiento

* Configurar monitoreo continuo para evaluar el desempeño del modelo en producción (precisión, latencia, tasa de errores).
* Establecer alertas para detectar degradación del modelo o fallos en el servicio.
* Planificar el reentrenamiento periódico del modelo con datos nuevos para mantener su efectividad (definir triggers o condiciones para actualizar el modelo).

## 7. Documentación y Capacitación

* Documentar el proceso de despliegue, uso de la API, y procedimientos de mantenimiento.
* Capacitar al equipo de soporte y usuarios clave para garantizar un uso correcto y eficiente del sistema.

## 8. Ciclo de Mejora Continua

* Recoger feedback de usuarios y métricas de producción para identificar oportunidades de mejora.
* Planificar iteraciones futuras para optimizar el modelo, la infraestructura o la experiencia de usuario.

Este plan sigue un enfoque iterativo y multidisciplinario, asegurando que el modelo no solo sea preciso sino también confiable, accesible y sostenible en un entorno real. Además, contempla la importancia de la infraestructura, la integración y el monitoreo continuo, aspectos clave para el éxito del despliegue en machine learning.

## **Herramientas utilizadas y recursos necesarios para el proyecto**

## **1. Hardware**

* Computador personal o servidor:  
  Un equipo con suficiente capacidad de procesamiento (CPU con múltiples núcleos, preferiblemente con GPU para acelerar entrenamiento si se requiere).
* Conexión a internet estable:  
  Para trabajar en Google Colab, descargar librerías, datasets y realizar despliegues en la nube o integraciones.

## **2. Plataformas y entornos de desarrollo**

* Google Colab:  
  Entorno en la nube para desarrollo, experimentación y entrenamiento del modelo sin necesidad de hardware local potente.
* IDE local (opcional):  
  Para desarrollo y pruebas locales, como VS Code o PyCharm.

## **3. Lenguaje y librerías de programación**

* Python 3.x:  
  Lenguaje principal para el desarrollo del modelo y análisis.
* LightGBM:  
  Biblioteca para entrenamiento eficiente de modelos de boosting basados en árboles.
* Pandas y NumPy:  
  Para manipulación y procesamiento de datos.
* Scikit-learn:  
  Para preprocesamiento, evaluación de métricas y comparación con otros modelos.
* Matplotlib y Seaborn:  
  Para visualización de datos y resultados.

## **4. Almacenamiento y gestión de datos**

* Google Drive:  
  Para almacenar datasets y resultados cuando se trabaja en Colab.
* Sistemas de archivos locales o en la nube:  
  Para guardar modelos entrenados y datos en entornos de producción.

## **5. Infraestructura para despliegue**

* Servidor o máquina local para producción:  
  Puede ser un servidor dedicado, un computador con sistema operativo Linux/Windows o una instancia en la nube (AWS, Azure, Google Cloud).
* Sistema operativo compatible:  
  Linux es común para servidores por su estabilidad y soporte, aunque Windows y macOS también son válidos.
* Entorno de ejecución Python configurado:  
  Con todas las dependencias instaladas (LightGBM, librerías auxiliares).

## **6. Herramientas para integración y despliegue**

* Framework para APIs (opcional):  
  Flask, FastAPI o Django para exponer el modelo como un servicio RESTful.
* Docker (opcional):  
  Para contenerizar la aplicación y facilitar el despliegue en diferentes entornos.
* Sistemas de control de versiones:  
  Git para gestionar el código fuente y colaborar en equipo.

## **7. Equipo humano**

* Científico de datos / ingeniero de machine learning:  
  Responsable de desarrollar, entrenar y validar el modelo.
* Ingeniero de datos:  
  Encargado de preparar y gestionar los datos.
* Desarrollador de software / ingeniero de sistemas:  
  Para integrar el modelo en aplicaciones y gestionar el despliegue.
* Equipo de IT / soporte técnico:  
  Para mantener la infraestructura y resolver problemas técnicos.

## **Consideraciones para el Mantenimiento del Modelo**

1. Monitoreo continuo del desempeño  
   Es fundamental implementar un sistema que evalúe periódicamente métricas como precisión, recall, F1-score y tasa de error en datos nuevos o en producción. Esto permite detectar a tiempo cualquier degradación en el rendimiento del modelo causada por cambios en los datos o el entorno.
2. Actualización periódica del modelo  
   Con el tiempo, los patrones en los datos pueden cambiar (fenómeno conocido como *drift*), por lo que es necesario reentrenar o ajustar el modelo con datos recientes para mantener su efectividad. Esto puede hacerse mediante:
   * Tuning o ajuste fino del modelo existente con nuevos datos (similar a transfer learning).
   * Entrenamiento desde cero con un conjunto de datos actualizado si el tuning no mejora el rendimiento.
3. Gestión de versiones y despliegue controlado  
   Para evitar interrupciones en el servicio, las actualizaciones del modelo deben realizarse en una réplica o entorno de prueba. Solo se reemplaza el modelo en producción si la nueva versión demuestra mejor desempeño, asegurando estabilidad y confiabilidad.
4. Optimización de hiperparámetros  
   Durante el mantenimiento, es importante revisar y ajustar parámetros como tasa de aprendizaje, número de iteraciones, profundidad máxima de árboles, y otros, para evitar sobreajuste y mejorar la generalización. Técnicas como la optimización bayesiana pueden ser útiles para este propósito.
5. Manejo eficiente de recursos computacionales  
   El mantenimiento debe considerar el tiempo y costo computacional necesarios para reentrenar y validar el modelo, buscando un balance entre frecuencia de actualización y recursos disponibles.
6. Documentación y trazabilidad  
   Registrar cada versión del modelo, los datos usados, parámetros ajustados y resultados obtenidos es esencial para reproducir experimentos, auditar el desempeño y facilitar futuras mejoras.
7. Consideraciones éticas y de seguridad  
   Mantener la transparencia sobre cambios en el modelo y evaluar el impacto de posibles errores o sesgos en producción, garantizando que el modelo siga cumpliendo con los estándares de responsabilidad y cumplimiento.

| Concepto | Cantidad | Costo Unitario (COP) | Total (COP) |
| --- | --- | --- | --- |
| Computador / Servidor | 1 | 6.192.000(1.500 USD × 4.128) | 6.192.000 |
| GPU para entrenamiento | 1 | 2.889.600 (700 USD × 4.128) | 2.889.600 |
| Servicio en la nube (ej. AWS/GCP/Azure) - computación | 1 mes | 412.800 (100 USD × 4.128) | 412.800 |
| Almacenamiento en la nube (datos y modelos) | 100 GB | 82.560 (0.02 USD × 4.128) | 8.256.000 |
| Google Colab Pro (opcional) | 1 mes | 41.280 (10 USD × 4.128) | 412.800 |
| Framework para API (Flask/FastAPI) | 1 | 0 (gratuito) | 0 |
| Docker para contenerización | 1 | 0 (gratuito) | 0 |
| Dominio web y hosting para API | 1 año | 206.400 (50 USD × 4.128) | 206.400 |
| Control de versiones (GitHub/GitLab) | 1 cuenta | 0 (gratuito) | 0 |
| Licencias software y librerías | - | 0 (gratuito) | 0 |
| Equipo humano (científico de datos, ingeniero, soporte) | 3 personas (por mes) | 4.128.000 (1.000 USD × 4.128 × 3) | 12.384.000 |

Total aproximado inicial en COP: 22.134.336

### **Casos de uso en colombia**

# **Ataques de phishing en Colombia aumentaron un 28%: OlimpIA alerta sobre nuevas amenazas y cómo protegerse**

En un mundo cada vez más digital, **el *phishing* se ha consolidado como una de las formas más comunes de ciberataque.**

Esta técnica de ingeniería social utilizada por ciberdelincuentes se está presentando de manera más sofisticada, **logrando engañar a las víctimas con comunicaciones aparentemente auténticas**. Desde que se popularizó el término en 1990, su objetivo sigue siendo el mismo, **engañar a las personas para robar información sensible**.

Según datos de OlimpIA, empresa líder en ciberseguridad e inteligencia artificial en el país, **los intentos de phishing aumentaron un 28% a nivel mundial,** poniendo en evidencia la necesidad de tomar medidas preventivas contra estos ataques cibernéticos. Además, **la compañía indica que Colombia es uno de los más afectados en la región con un 17% de los incidentes registrados**.

Simbad Ceballos, CEO de ***OlimpIA***, menciona que: “**ahora estamos viviendo el phishing 2.0, el cual emplea inteligencia artificial y aprendizaje automático para crear ataques altamente personalizados y convincentes**. *Los ciberdelincuentes, están perfeccionando sus técnicas, haciendo que los correos electrónicos y los mensajes parezcan más genuinos que nunca. Es fundamental estar al tanto de estas tácticas y tomar medidas de seguridad efectivas para protegerse*", destacó Ceballos.

El *phishing* moderno no solo se limita a correos electrónicos, los ataques vienen disfrazados de mensajes de texto, llamadas telefónicas (vishing) o incluso sitios web falsos que imitan a los originales para robar información.

También existen ataques más avanzados, como el "***watering hole***", denominados así por la similitud de un depredador que acecha a su presa. Esta técnica se dirige generalmente a empresas con altos niveles de seguridad, donde los empleados frecuentan sitios web de confianza relacionados con la organización. Los atacantes primero investigan y contaminan estos sitios, creando un perfil de sus potenciales víctimas. Al visitar el sitio infectado, **el empleado sin saberlo descarga *malware* que permite a los atacantes tomar control de su equipo y robar información confidencial**.

**Recomendaciones para el negocio o para futuras investigaciones**

● Implementar autenticación multifactor en todas las cuentas importantes. Esto añade una capa adicional de seguridad, lo cual dificulta el acceso no autorizado.

● Utilizar gestores de contraseñas para crear y almacenar claves únicas y complejas. Las contraseñas seguras son una de las primeras barreras de defensa.

● Mantenerse informado sobre las últimas técnicas de phishing. Participar en programas de concientización en ciberseguridad ayuda a reconocer señales de posibles ataques.

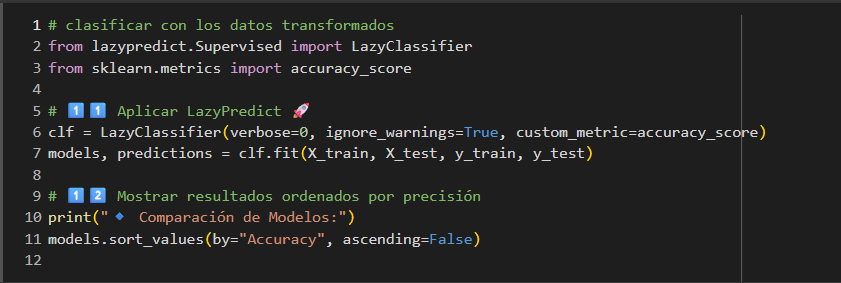
● Verificar siempre la autenticidad de los remitentes y enlaces antes de hacer clic. Dudar de cualquier solicitud inesperada de información es clave para evitar caer en trampas.

El panorama actual del phishing muestra que **los ciberdelincuentes emplean tecnologías como los *deepfakes* para realizar llamadas y suplantar voces**, además de utilizar técnicas de ingeniería social más sofisticadas para manipular a las víctimas.

Ante esta realidad, OlimpIA se posiciona a la vanguardia en la lucha contra estas amenazas emergentes, ofreciendo soluciones de ciberseguridad basadas en inteligencia artificial, para ayudar a las organizaciones a fortalecer sus defensas contra el phishing 2.0 y otros tipos de ciberataques.

Para mitigar los riesgos y reforzar la seguridad digital, el experto recomienda cinco estrategias clave:

1. **Sistemas de detección con IA:** identificar patrones anómalos en tiempo real para mejorar la capacidad de respuesta ante ataques.
2. **Educación y concienciación:** capacitar a empleados y usuarios sobre tácticas avanzadas como deepfakes y phishing automatizado para reducir su impacto.
3. **Autenticación multifactor:** implementar biometría y/o tokens de acceso, para dificultar el ingreso no autorizado a sistemas sensibles.
4. **Marcos éticos y regulaciones claras:** establecer políticas que guíen el uso responsable de la IA y prevengan su aplicación en actividades que comprometan la privacidad y seguridad de la información.
5. **Colaboración internacional:** fortalecer el intercambio de información entre empresas y gobiernos para combatir de manera conjunta las amenazas

soy un estudiante de un bootcamp de inteligencia artificial en el cual necesitamos sustentar el proyecto final y describir el porque elegimos el modelo por el que optamos, hay unas linea de codigo que nos ayudaron a decidirnos por el modelo y es la siguiente

soy estudiante de inteligencia artificial y estoy haciendo un modelo de machine learning sobre pishing creamos el siguiente modelo