SecureNet: Plataforma de prevención y detección de URL inseguros usando IA.

Proyecto de Grado – Pregrado

Integrantes

- Dina Luz Tuesta García

- Gustavo Andrés Sandoval Sánchez

- Juliana Alexandra Moreno Jiménez

Tutor

Lina María Chacón Rivera

Universidad EAN

Facultad de Ingeniería

BOGOTÁ, D.C. 2024

Tabla de contenido

Índice de Figuras

Resumen

El presente proyecto de grado tiene como objetivo desarrollar un prototipo de plataforma web destinada a concientizar a los estudiantes de la Universidad EAN sobre ciberseguridad y ataques de phishing. La plataforma utilizará inteligencia artificial para evaluar la peligrosidad de las URLs, clasificando y proporcionando información sobre las amenazas más comunes, como smishing, vishing, pretexting y pharming. Además, incluirá un chatbot interactivo que permitirá a los usuarios identificar el tipo de ataque que enfrentan y ofrecerá sugerencias para mitigar los riesgos asociados. La creciente dependencia de los estudiantes en plataformas digitales y su falta de capacitación en ciberseguridad los hace vulnerables a los ataques cibernéticos. Este proyecto busca no solo ayudar a los estudiantes a reconocer las amenazas de phishing, sino también proporcionarles herramientas prácticas para responder a estas situaciones de manera efectiva.

Palabras Clave

Ciberseguridad, plataforma web, phishing, smishing, vishing, pretexting, pharming, inteligencia artificial, URL maliciosas, prevención de ataques cibernéticos.

Introducción

Los usuarios están en riesgo de ser atacados por ciberdelincuentes que utilizan la ingeniería social para manipular a sus víctimas en una variedad de formas cada vez que interactúan con páginas web navegando en Internet. El phishing se ha convertido en una de las amenazas cibernéticas más comunes y peligrosas en la era digital actual, afectando a personas y organizaciones de todos los tamaños. Este tipo de ataque, que busca engañar a las víctimas para que revelen información confidencial a través de métodos fraudulentos, ha evolucionado en complejidad y sofisticación, lo que hace que la detección y la prevención sean cada vez más difíciles.

Por lo mismo, algunas organizaciones como la Cámara de comercio electrónico en Colombia han mostrado que uno de los desafíos de la seguridad digital en el país para el 2024 es:

> La educación en ciberseguridad es fundamental para preparar a las personas y las organizaciones para los ciberataques. Las personas deben estar informadas sobre las amenazas cibernéticas y cómo protegerse, y las organizaciones deben capacitar a sus empleados en ciberseguridad para que puedan identificar y evitar los ciberataques. (Cámara de comercio Electrónico, 2024, párr. 8)

El presente proyecto tiene como objetivo desarrollar un prototipo de plataforma web que indique e informe a los estudiantes de la Universidad EAN sobre la ciberseguridad y el phishing. Adicional, utilice inteligencia artificial para determinar si una URL es maliciosa. La plataforma clasificará y proporcionará información sobre las amenazas de phishing en las formas más comunes, como smishing, vishing, pretexting y pharming. Además, la plataforma incluirá un formulario que ayudará a los usuarios a comprender mejor el tipo de ataque que están experimentando y les proporcionará sugerencias para reducir el riesgo.

Este proyecto busca no solo ayudar a los estudiantes de la universidad EAN a identificar los ataques de phishing, sino también concientizarlos, proporcionando herramientas prácticas para identificar y responder a estas amenazas de manera efectiva.

Antecedentes

Hoy en día nos encontramos en la cuarta revolución industrial, la cual demuestra el gran crecimiento computarizado y tecnológico tan apresurado que ha tenido el mundo en los últimos años. La dependencia a la tecnología tuvo su mayor momento en la pandemia de Covid-19 en el año 2020, en dónde personas y empresas se digitalizaron aún más como respuesta al impacto económico y social. Esto para seguir en contacto con familiares, y el teletrabajo o en caso de los estudiantes, las reuniones virtuales con las clases. Así como tratar de suplir la necesidad de asegurar la disponibilidad de alimentos, prendas de vestir, tecnología y otros productos esenciales en el hogar.

Finalmente, la pandemia ha puesto de manifiesto, si es necesario, la importancia crucial de la digitalización en nuestras vidas. Se necesita urgentemente implementar políticas públicas que aceleren la conectividad y la digitalización en América Latina, ya que la pandemia no ha desaparecido y ciertas prácticas como trabajar y comprar a distancia son de esperar que perduren. Además, esta región aún tiene una brecha digital significativa por cerrar. (Jung, J, Katz, R. L, 2022)

Debido al confinamiento que se dio para evitar el esparcimiento del virus en la población, también se recurrió a la compra de servicios y productos digitales, como Netflix, Prime Video, Spotify, videojuegos, entre otros. Lo que también impulsó el crecimiento en el mercado electrónico y benefició a aquellas empresas que lograron manejar este tipo de comercio. Como enfatiza Ríos Ruiz (2020), que todos los negocios que puedan atraer clientes a sus plataformas digitales y satisfacer sus necesidades, sin importar su sector, conseguirán obtener grandes beneficios. La clave para atraer a ese grupo de personas que aún no se habían familiarizado con los servicios en línea es aprovechar la oportunidad, asumir responsabilidades y hacerlo bien.

Por otro lado, no hay que olvidar la propaganda de los días sin IVA y los *BlackFriday* en Colombia que indujeron mucho más rápido la necesidad de compras online durante esos años para impulsar las ganancias de los empresarios que fueron alcanzados por la crisis económica de la pandemia. Según el informe de Cruz Cárdenas (s. f.), señaló que, aunque Black Friday tuvo un rendimiento superior, la participación de compras en el tercer día sin IVA fue mayor que en los primeros dos días sin IVA. Es crucial tener en cuenta que, durante el tercer día, la mayoría de las compras debían realizarse en línea. Uno de los investigadores expresó que durante la cuarentena

se aprendió a manejar la tecnología de manera eficaz, lo que permitió avanzar diez años en el uso de carteras digitales en lugar de dinero en efectivo.

El estudio encontró que el 70% de los encuestados prefirió hacer sus compras en línea en este contexto, mientras que el 15,38% optó por hacerlas en persona. Esto resalta cómo los clientes están eligiendo una variedad de métodos para obtener bienes y servicios. Además, los participantes prefirieron pagar con tarjetas de crédito. (Cruz Cárdenas Lourdes, s. f.)

Por lo que, al estar en constante crecimiento esta modalidad de pagos en línea se debe tener en cuenta los nuevos riesgos que existen en este ámbito. Como lo son los ataques cibernéticos, que buscan lucrarse por medio de estafas en las compras virtuales, atacando no solo a las personas naturales sino también a las empresas.

La envergadura de los daños proyectados evidencia el efecto de la ciberdelincuencia en las economías a nivel mundial. En 2025, los gastos vinculados al delito cibernético alcanzarán los 10,5 billones de dólares anuales, un monto que superará el Producto Interno Bruto (PIB) de varias de las economías más potentes del mundo. (Ruiz Dylan, 2024)

Definición del Problema

Las instituciones educativas, y en particular los estudiantes, se enfrentan a un número creciente de amenazas cibernéticas, siendo el phishing una de las más prevalentes y peligrosas.

> Al examinar las rutas de ataque, el informe revela que, en 2023, el vector de acceso inicial preferido en América Latina fue la explotación de aplicaciones públicas, constituyendo el 45% de los casos observados por X-Force. El phishing y las cuentas válidas ocuparon el segundo lugar con un 22%. (Revista Forbes, 2024, párr. 9)

Este tipo de ataque se ha vuelto cada vez más sofisticado, lo que dificulta su detección y aumenta el riesgo de que los usuarios sean víctimas.

Según Mauricio Lizcano, el ministro de las TIC, se han reportado más de 20,000 millones de ciberataques hasta ahora en el año. En la Convención Bancaria 2024, dio a conocer los datos y los progresos de la estrategia Colombia Potencia Digital. El phishing, el secuestro de datos comerciales y la clonación son las principales amenazas cibernéticas que afectan al sector financiero, destacó. (Cañón A., 2024)

Por esto, apremia la necesidad de prevenir y herramientas de protección a los universitarios, un grupo particularmente vulnerable a los ataques de smishing, vishing, pretexting y pharming, por la falta de información y formación en ciberseguridad. Muchas veces, los estudiantes confían en que los enlaces recibidos a través de correos electrónicos, mensajes de texto y otras plataformas digitales son legítimos, lo que los expone a riesgos significativos. La ausencia de información puntual y herramientas accesibles para validar la autenticidad de las URLs agrava este problema, aumentando la probabilidad de que los estudiantes comprometan información confidencial.

La falta de concientización y medidas adecuadas para detectar y prevenir ataques cibernéticos en el entorno universitario ha puesto a los estudiantes en peligro. La falta de información clara, capacitación en ciberseguridad y herramientas robustas para la validación de la autenticidad de enlaces, hace que sea más probable estar expuesto a ataques y perder información confidencial.

La mayoría de los estudiantes en las universidades confían en que los mensajes y las URL´s recibidos en sus correos electrónicos y otras plataformas digitales sean verdaderos, lo que los hace susceptibles a ser víctimas de la ciberdelincuencia. Además, la desinformación generalizada y la tendencia a subestimar los riesgos cibernéticos hacen que las amenazas de phishing se propaguen fácilmente.

Es crucial que los estudiantes aprendan a proteger sus cuentas de correo electrónico y otras plataformas, como Google o SAP, cuando utilizan los computadores de la universidad. Al dejar estas cuentas abiertas, las personas no autorizadas pueden acceder a información personal y confidencial. Esta falta de cuidado puede conducir a situaciones graves como el robo de datos, el fraude, las estafas, el acoso o el acoso, lo que pone en peligro su seguridad y bienestar. Por lo tanto, es fundamental que adopten hábitos responsables para proteger y garantizar la integridad de su información.

Para tener un vistazo mucho más puntual de la problemática se decidió ir agrupando las ideas en un diagrama de pescado, en la **Figura 1**se puede entender a fondo el análisis. Este problema refleja la necesidad de desarrollar una plataforma que no solo detecte enlaces inseguros, sino que también eduque a los estudiantes sobre los diferentes tipos de ataques cibernéticos más comunes, para que puedan tomar medidas para protegerse de manera efectiva.

Herramienta para definir el problema, proyecto SecureNet como se muestra en la **Figura 1**.

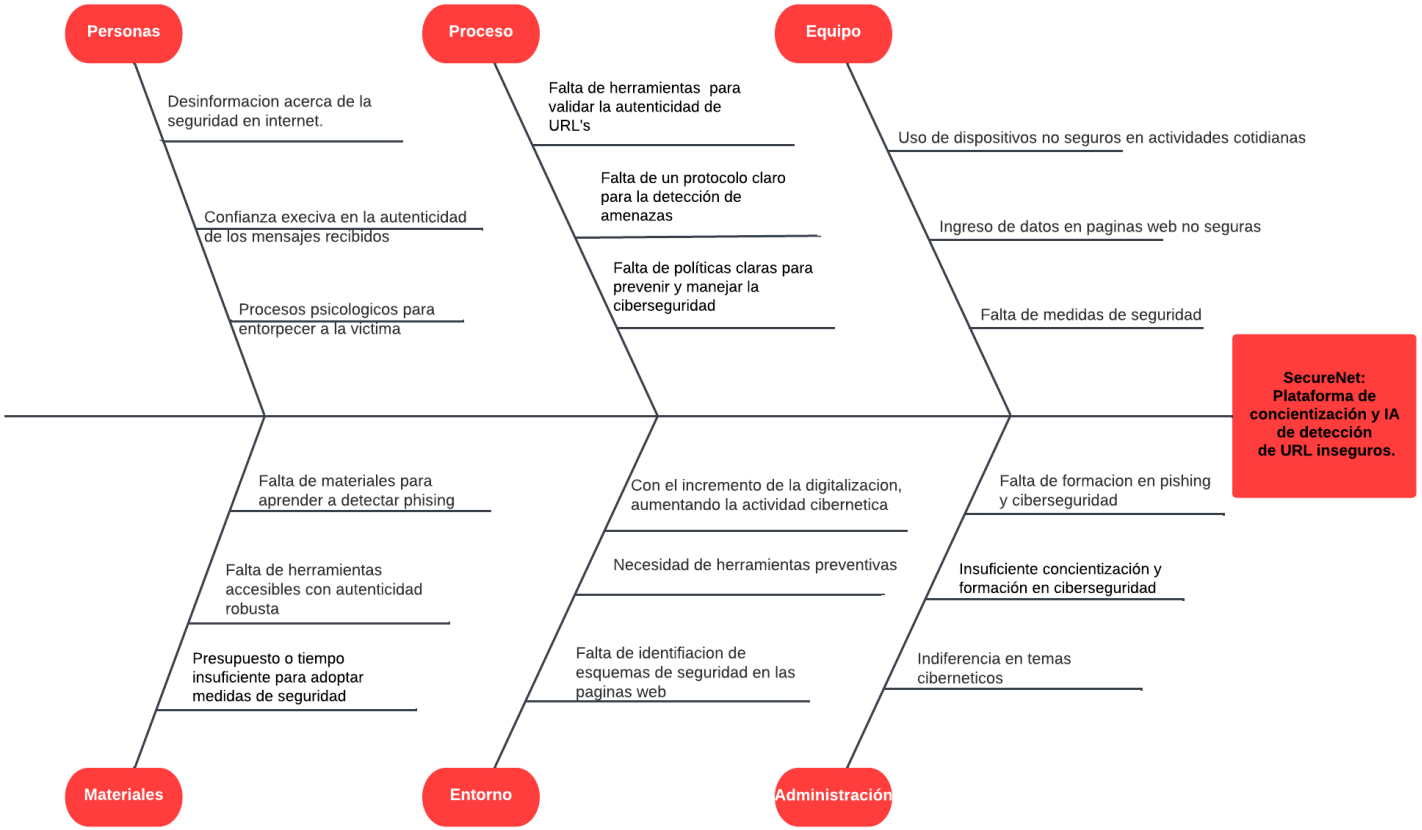

Figura 1. Diagrama de Pescado

Nota. El grafico presenta un diagrama de pescado en donde se determinan las posibles causas que complementan el desarrollo del problema, al que presenta como solución el proyecto de la plataforma de SecureNet. Fuente: Lucidchart – Elaboración propia.

Objetivo General

- Desarrollar un prototipo de un sistema de identificación de phishing en sitios web, analizando las URL para concientizar a los estudiantes de la universidad EAN de posibles ataques cibernéticos y garantizar la seguridad e integridad de la información personal y académica.

Objetivos Específicos

- Diseñar los mock-up para cada sección de la plataforma web con su respectiva información del ataque cibernético (Phishing, smishing, vishing, pretexting y pharming).
- Generar el código de HTML, CSS y JavaScript de las secciones de la página con su respectiva información.
- Entrenar la IA para la detección de anomalías en URL's para la identificación de cuales son seguras.
- Evaluar la efectividad de la IA para la detección de anomalías en URL´s y así poder determinar si es maliciosa o segura.
- Generar una herramienta interactiva en la cual los estudiantes logren interactuar y responder a preguntas para la identificación de diferentes ataques cibernéticos.

Justificación

En un mundo cada vez más interconectado, la seguridad cibernética ha pasado a ser un tema crítico en todos los sectores, incluyendo el ámbito académico. La plataforma reducirá el riesgo de que los estudiantes sean víctimas de ataques de phishing al brindar información sobre la ciberseguridad, protegiendo su información personal y académica. Además, brindará a los usuarios herramientas interactivas que les permitirán identificar el tipo de ataque que enfrentan y tomar medidas preventivas.

La plataforma se dedicará a la innovación y la educación, brindando a los estudiantes las herramientas necesarias para navegar de manera segura en el mundo digital. Este proyecto mejorará la seguridad de los estudiantes y fortalecerá la cultura de ciberseguridad en la universidad. Por su parte, permitirá que las nuevas tecnologías, como

la Inteligencia Artificial, optimicen y logren identificar amenazas de una forma mucho más rápida y brinde información de una debida solución.

Por lo que incorporar un proyecto centrado en la ciberseguridad en el ámbito académico no solo es necesario, sino también altamente conveniente en el contexto actual. La dependencia de las tecnologías digitales en la educación ha aumentado considerablemente los riesgos a los que se exponen los estudiantes, en cuanto a privacidad y seguridad de su información personal y académica. Implementar una plataforma que se enfoque en educar y proteger a los estudiantes en este ámbito no solo mitiga estos riesgos, sino que también fomenta una cultura de ciberseguridad que se alinea con las mejores prácticas globales.

Este proyecto es esencial porque prepara a los estudiantes para enfrentar de manera proactiva los desafíos del entorno digital, dotándolos de herramientas y conocimientos prácticos para identificar y prevenir ataques cibernéticos. Al integrar tecnologías avanzadas, como la Inteligencia Artificial para la detección de phishing, la plataforma no solo educa, sino que también evoluciona constantemente para adaptarse a nuevas amenazas, optimizando así la capacidad de respuesta ante posibles incidentes de seguridad.

Además, este proyecto es conveniente porque contribuye directamente a la mejora de la reputación de la universidad en términos de innovación y responsabilidad en la protección de su comunidad. Al priorizar la ciberseguridad, se genera un entorno más seguro y confiable para los estudiantes, lo que refuerza su confianza en la institución y promueve un uso más seguro y consciente de las tecnologías digitales. En última instancia, este esfuerzo colaborativo hacia una mayor seguridad cibernética no solo protege a los estudiantes, sino que también fortalece el tejido educativo al integrar prácticas esenciales para el mundo interconectado de hoy.

Marco Teórico

Ciberataques:

Un ataque cibernético es cualquier esfuerzo intencional para obtener de forma ilegal información privada con la intención de exponer, alterar, destruir, espiar, suplantar o robar tanto en aplicaciones como en redes, sistemas informáticos y dispositivos.

Debido al aumento de compras en línea y la interacción en el ciberespacio, no es de extrañar que los casos de ciberataques también hayan aumentado, debido a que los usuarios al realizar compras o al registrase las plataformas web de estos negocios, los datos que se ingresan llegan a ser de fácil acceso, como el correo electrónico y el número celular. En los cuales se presenta mayor número de casos de Phishing, smishing, vishing, y pharming con los que se utiliza ingeniería social para que las posibles víctimas caigan en el engaño.

> "Al finalizar noviembre de 2021, se presentaron 46.527 eventos por ciberdelitos en el país, registrando un crecimiento del 21% comparado con 2020, donde se registraron un total de 38.452 ciberdelitos." (TicTac, 2021, párr. 3)

El Phishing es un ciberataque que se basa en ingeniería social. La palabra viene del inglés "fishing" que en español significa *Pescando,* el uso del "*Ph"* viene de lo que se conoce como los primeros hackers del sistema telefónico en los Estados Unidos, "*Phreaks"* cuyos actos se conocieron como "*Phreaking".* Descritos así por Ollmann (2008).

Aunque el phishing sea un ciberataque, su forma de ataque se encuentra más enfocado a manipular a los usuarios ganándose su confianza para obtener una respuesta a las tácticas de presión, esto se ve tanto a las personas del común como en las empresas. Por lo tanto, no se dirige directamente a las redes. Sin embargo, pueden usar el internet como medio para enviar mensajes por medio del correo electrónico, por los cuales llegan enlaces o archivos dónde se direcciona a las personas a sitios web fraudulentos o incluso para descargar un malware dentro del dispositivo. Una vez allí, se pueden obtener los datos sensibles de la víctima, como datos de tarjetas de crédito, credenciales del usuario, entre otros. También se puede suplantar la identidad de la víctima con estos datos, pudiendo perjudicar a su círculo de relaciones cercanos, como la familia o compañeros de trabajo.

> "Las filtraciones causadas por phishing cuestan a las organizaciones una media de 4,76 millones de dólares, cifra superior al coste medio global de las filtraciones, que es de 4,45 millones de dólares." (Kosinski Mateo, 2024, párr. 5)

La razón del porqué es popular y eficaz, es porque a diferencia de un programa maligno, el Phishing no necesita violar los sistemas de protección de los dispositivos, puesto que al tener la autorización de la víctima se da acceso a cualquier tipo de

información. Los ciber delincuentes pueden actuar de forma individual, así como en organizaciones.

El phishing busca engañar tanto a personas comunes como a grandes empresas y entidades gubernamentales. Un caso famoso ocurrió en 2016, cuando hackers rusos enviaron un correo electrónico falso para restablecer contraseñas, logrando robar miles de correos electrónicos de la campaña presidencial de Hillary Clinton. Este ataque se ha convertido en uno de los ejemplos más notorios de phishing en la historia reciente. (Kosinski Mateo, 2024)

La revista Forbes (2024) realizó un estudio en donde la posición de Colombia como el segundo país más atacado en América Latina desde 2022. Las empresas de seguridad cibernética como Eset, Kaspersky y Norton están trabajando para reducir estos peligros. Brasil ocupó el primer lugar con un 68% de ataques, mientras que Chile ocupó el tercer lugar con un 8%. Múltiples sectores fueron afectados por los ataques, con el comercio minorista, las finanzas y el seguro compartiendo el primer puesto con un 25 % del impacto total. Además, el uso de extensiones maliciosas de Chrome dirigidas a instituciones financieras ha aumentado. El informe de X-Force destacó que, en 2023, la explotación de aplicaciones públicas fue el método de acceso inicial más común, representando el 45% de los casos; el phishing y las cuentas válidas fueron los siguientes métodos de acceso con el 22%.

El Smishing es otra forma que los ciberdelincuentes utilizan, está también se utiliza con la táctica de ingeniería social. Se le denomina con el acrónimo SMS que se entiende como “Servicio de Mensajes Cortos”. Por lo que, en este caso, el smishing se centra en enviar mensajes de texto falsos, con los que se pretende engañar a los usuarios para que compartan información sensible o envíen dinero, otro caso puede ser el compartir un enlace por el cual se pueda descargar malware con el fin de vulnerar los teléfonos móviles.

Se registraron 743 casos de smishing en 2023 a través del servicio de asistencia virtual 24/7, lo que representa el 4,5% de este tipo de delitos. Además, el Centro Cibernético Policial publicó 15 alertas preventivas sobre esta amenaza en las redes sociales de CAI Virtual, como Facebook, Instagram y X. (Malaver Carol, 2024)

Debido a que los Smartphones o celulares, se han vuelto en una parte esencial en cualquier área de la cotidianidad, esto los ha convertido en un medio por el cual los delincuentes puedan tratar de obtener los datos sensibles de los usuarios. Y puesto que, las personas también pueden poseer las credenciales de sus trabajos en este dispositivo o bien aplicaciones o acceso a redes, tienen el riesgo de llegar a facilitar los datos de las empresas.

Al igual que el Smishing, el Vishing también es un ciberataque que utiliza los celulares como medio para buscar víctimas, aunque también se hace por medio de teléfono fijo, pero ya no tanto. El término Vishing es la combinación de *Voice* (Voz en español) y *phishing,* es una táctica de manipulación que se realiza por medio de una llamada telefónica. Usualmente los ciberdelincuentes se hacen pasar por personas conocidas u organizaciones como bancos, empresas de telecomunicaciones, tiendas, entre otros. El principal problema del vishing, es que los atacantes pueden cambiar de número telefónico frecuentemente, lo que les permite evitar algunos filtros en llamadas que se hayan puesto en el celular. Su objetivo, al igual que los anteriores, es lograr recopilar datos sensibles de sus víctimas y lucrarse con ellos.

La diferencia entre el Phishing, Smishing y Vishing es que si bien, el phishing abarca estos dos, este se basa más en las estafas por medio del correo electrónico, en el cual se insta a las personas a introducir su información personal por medio de un enlace, entre otras formas para lucrarse. El Smishing por medio de mensajes y el vishing por medio de llamadas o mensajes de voz. Sin embargo, los tres tienen el mismo objetivo.

Maximiliano Cantis, un experto en ciberseguridad afirmó en una entrevista con la VOA que el engaño de identidades es una de las estafas más frecuentes. Esta amenaza se transmite a través de llamadas telefónicas, en las que los atacantes se disfrazan de instituciones gubernamentales o bancarias y solicitan información confidencial a sus víctimas. Pueden solicitar información enviada por mensaje de texto u obligar a las personas a hacer clic en enlaces para obtener sus datos y acceso a sus cuentas bancarias. (Álvarez C., 2023)

El Pharming o *Farming*, que en español significa agricultura puesto que intenta cosechar la información de las personas. Su nombre viene de combinar el *Phishing* y *Farming.* Es un ciberataque que se encarga de redirigir a los usuarios a un sitio web falso,

que imita uno legítimo, lo cual hace por medio de la manipulación de los DNS (Sistema de Nombres de Dominio), esto puede hacer que los usuarios se sientan seguros e ingresen los datos personales que en su mayoría son páginas financieras o de bancos falsas. El pharming trata de apoderarse del patrimonio monetario o los activos en las cuentas corrientes.

Finalmente, el Pretexting o Pretexto es una forma de ingeniería social con la cual los ciberatacantes generan sus historias inventadas para engañar a una víctima y lograr ganarse su confianza. Usualmente se suplanta la identidad de alguien que posee autoridad sobre la víctima, como compañeros del trabajo, miembros de alguna empresa o banco, o un jefe. Incluso se pueden hacer pasar por familiares. Lo que el atacante espera es hacer una buena imitación de su personaje y lograr que la víctima haga algo por él. Por lo general se escogen victimas específicas al igual que escenarios.

Siendo el phishing uno de los ataques más habituales, impactando tanto a personas naturales como a las organizaciones. Los fallos de carácter humano, como el establecimiento de enlaces perjudiciales o la instalación de programas dañinos, continúan siendo una de las principales vías de entrada para los criminales informáticos.

La ciberseguridad es la práctica que se dedica a la protección de aquella información que se encuentra en el ciberespacio, es decir, un espacio virtual creado por medios informáticos es de esta forma que las personas se logran conectar con la ayuda de las redes. La información que se procura proteger son los datos sensibles, planes nacionales, cuentas, medios de comunicación y la estructura de los sistemas operativos.

Legislación:

En Colombia existen leyes en base a estos ataques cibernéticos, el cual procura preservar con integridad los sistemas que empleen tecnologías de información (TI).

El Código Penal se modificó para incluir un nuevo bien jurídico que protege la información y los datos, así como asegurar la integridad de los sistemas que utilizan tecnologías de la información y las comunicaciones. Código Penal [CP]. Ley 1273 de 2009. 05 de enero de 2009 (Colombia).

Dentro de esta ley se encuentran artículos que definen los ataques que pueden ocurrir en lo que es dentro del Phishing, lo cual puede ser suplantación de identidad o de sitos webs, la violación de datos personales o incluso el uso de software maliciosos.

El uso de software malicioso se sanciona con penas de prisión de 48 a 96 meses y multas que van de 100 a 1,000 salarios mínimos legales mensuales para quienes, sin autorización, produzcan, trafiquen, adquieran, distribuyan, vendan, envíen, introduzcan o extraigan este tipo de programas dañinos del país. Código Penal [CP]. Art. 269E. 5 de enero de 2009 (Colombia).

La violación de datos personales se sanciona con penas de prisión de 48 a 96 meses y multas de 100 a 1,000 salarios mínimos legales mensuales para quienes, sin autorización, obtengan, compilen, sustraigan, ofrezcan, vendan, intercambien, envíen, compren, intercepte, divulguen, modifiquen o utilicen códigos o datos personales de ficheros, archivos, bases de datos u otros medios similares, ya sea para beneficio propio o de terceros. Código Penal [CP]. Art. 269F. 5 de enero de 2009 (Colombia).

La suplantación de sitios web para capturar datos personales se sanciona con prisión de 48 a 96 meses y multas de 100 a 1,000 salarios mínimos para quienes, sin autorización, creen páginas electrónicas con fines ilícitos. La misma pena se aplica a quienes redirijan usuarios a direcciones IP engañosas, salvo que se trate de un delito más grave. Si se reclutan víctimas, la pena se agravará entre un tercio y la mitad. Código Penal [CP]. Art. 269G. 5 de enero de 2009 (Colombia).

Diseño Metodológico / Alternativa de Solución

La creación de una plataforma web de identificación de URLs maliciosas con phishing y otros tipos de ataques cibernéticos, surge de la necesidad de informar y concientizar a los estudiantes frente diversas amenazas virtuales, es importante contar con herramientas prácticas para detectar e informar como mitigar estos riesgos que afecta a la integridad y seguridad de los estudiantes de la Universidad EAN.

La plataforma tendrá una interfaz intuitiva para incentivar a una participación más activa y facilitar que el estudiante tenga una mayor comprensión de la información, para el desarrollo frontend, se implementaron programas como:

- Visual Studio Code: Como editor de código principal y punto de inicio para desarrollar la plataforma se está usando este programa debido a su flexibilidad y la cantidad de extensiones disponibles que facilitan el desarrollo para el programador, acorde a la norma de W3C (Wide Web Consortium), podría asegurar que el código sea de alta calidad y adaptable a futuras necesidades, garantizando que sea compatible con múltiples navegadores y sea más eficiente.
- HTML y CSS: Fundamentales para estructurar y darle estilo a la presentación visual que llevara la plataforma, además de dar cumplimiento con la normativa de WCAG 2.1 (Web Content Accessibility Guidelines), promueven la creación de contenidos inclusivos y fáciles de usar para todos los estudiantes.
- JavaScript: Usado para añadir más interactividad y hacer que la página sea un poco más dinámica mediante diversas animaciones, además relacionado también con la norma W3C (Wide Web Consortium), pues asegura una funcionalidad entre diferentes navegadores, especialmente compatible con Google Chrome.
- Bootstrap es otro framework de diseño utilizado para agilizar el desarrollo mediante plantillas que permiten usar diseños responsivos (se adapta a cualquier pantalla) de forma más eficiente, lo que indica que también se aplica la norma W3C (Wide Web Consortium).

Para el desarrollo de la inteligencia artificial que detecta las URLs falsas, se usaron librerías y lenguajes de programación, como:

- TensorFlow; reconocida como una de las librerías más usadas para el desarrollo de modelos de inteligencia artificial y a su vez permitiendo entrenar la red neuronal para que pueda detectar qué tipo de enlaces son maliciosos. Se aplica a la norma de seguridad ISO/IEC 27001, pue se encarga de regular la gestión de la seguridad de la información y protección contra ciberataques y proteger la integridad e información personal y académica de los usuarios.
- Python; es el lenguaje de programación usado por la mayoría de los modelos de inteligencia artificial ya que tiene bastante capacidad para manejar grandes cantidades de datos de manera eficiente en campos como el aprendizaje automático y accesorios bibliotecas como tensorFlow, lo que facilita el proceso de

entrenamiento e integración del modelo. En este lenguaje de programación se aplica la norma ISO 29148, que regula la definición de los requisitos del software asegurando que el sistema cumpla con las expectativas funcionales y técnicas.

- JavaScript; no solo se implementará para incluir animaciones a la plataforma asilo también fue implementarse en la integración de la inteligencia artificial con la plataforma web, ya que no es necesario enviar los datos a un servidor y así mejorando la seguridad y la velocidad en la que se analiza los enlaces. En este caso también se aplica la norma ISO/IEC 27001 debido a que JavaScript reduce el riesgo de la exposición de datos personales en la aplicación de la integración de la inteligencia artificial con el proyecto.
- Voiceflow: Se utiliza este api para la creación del chat-bot, en donde esta se utiliza para todo lo que es el análisis de la información de la página del proyecto para suministrar información puntual de la página, también incluirá unas preguntas en donde ayuda a los usuarios a reconocer el tipo de ataque que están siendo víctimas o están siendo involucrados, por lo tanto, este api será una guía para la página con información precisa de esta, y mejorando la facilidad de acceso a la información de la página.
- Page Rank: Se integra este api para la creación de la pequeña inteligencia artificial en donde esta es la encargada de enviar información puntual del posicionamiento online del enlace del cual se le envía la información, para que el algoritmo reciba este dato para la IA y este de su veredicto en base a esta información que le suministra esta API.
- Google Index: Esta API de la empresa Google se utiliza porque gracias a su base de datos en la que Google almacena y organiza toda la información de las páginas web que ha descubierto mediante su proceso de rastreo (o "crawling"). Este índice envía unos datos importantes en los cuales ayuda al rastreo de la web en la cual se envía el enlace para encontrar parámetros en donde esta si fue creada hace poco o esta tiene un dominio completamente legal, en donde muestra si la página tiene un dominio totalmente visible para el público o este es relevante en la búsqueda en base a otras webs que compara con esta API.

Análisis de Costos

Simulador Financiero 2024 SecureNet.xlsx

	INVERSIÓN INICIAL
TERRENOS	$ 404.546,00
PROPIEDAD PLANTA Y EQUIPO	$ 3.564.998,00
MUEBLES Y ENSERES	
EQUIPO DE OFICINA	$ 2.000.000,00
EQUIPO DE TRANSPORTE	$ -
FRANQUICIAS	$ -
PATENTES /INV en INTANGIBLES	$ 2.405.899,00
GASTOS DE PUESTA EN MARCHA	$ 3.217.500,00
TOTAL INVERSIONES	$ 11.592.943,00

Figura 2. Inversión Inicial

NOMBRE DEL PRODUCTO O SERVICIO	CANTIDADES	PRECIO DE VENTA UNITARIO SIN IVA	INGRESOS TOTALES
Suscripción Empresarial	8,00	$ 3.600.000,00	$ 28.800.000
Suscripción Anual Personal	20,00	$ 570.000,00	$ 11.400.000
Suscripción Mensual Personal	30,00	$ 69.900,00	$ 2.097.000
Sponsor	5,00	$ 439.147,00	$ 2.195.735

Figura 3. Lista y precio de productos

TASA DE INT ANUAL CRÉDITO		AÑOS DE CRÉDITO	
6,00%			3

Figura 4. Tasa de interés anual

TOTAL INVERSIÓN	$	11.592.943,00
APORTE DE LOS EMPRENDEDORES	$	3.000.000,00
PRÉSTAMO A SOLICITAR	$	8.592.943,00

Figura 5. Inversión y prestamo

PERIODO DE RECUPERACIÓN:	4,00 AÑOS

Figura 6. Años de recuperación

VALOR PRESENTE NETO DEL PROYECTO =	$ 2.893.169,62
TASA INTERNA DE RETORNO =	35,50%

Figura 7. Tasa de Retorno

Análisis de Sostenibilidad

- La implementación de tecnologías de código abierto como HTML, CSS JavaScript y tensorFlow reduce costos de licencia, lo que indica que es una implementación podría ser más accesible y escalable.
- Tiene un diseño inclusivo, pues permite el acceso a todos los estudiantes para promover la conciencia y la educación sobre la ciberseguridad dentro de una comunidad estudiantil, creando una cultura de sensibilización ante ataques cibernéticos.
- Al ser una plataforma digital reduce el uso de materiales impresos, lo que minimiza el impacto ecológico.
- Con el uso de la inteligencia artificial se asegura la correcta detención de amenazas en URLs para promover un entorno más seguro en los estudiantes.
- A futuro este proyecto podría vincularse con otros programas académicos para fortalecer la comunidad educativa en temas de ciberseguridad, además, aportar más prestigio de la Universidad por formar estudiantes responsables en ambientes digitales, ampliando su reconocimiento social.

Discusión de los resultados

El desarrollo del aplicativo SecureNet ha representado un avance significativo en la prevención y mitigación de riesgos asociados a los ataques cibernéticos, en particular el phishing, entre los estudiantes de la Universidad EAN. A continuación, se analizan los resultados más relevantes obtenidos durante la creación y evaluación de la plataforma.

Relevancia de la concientización en ciberseguridad

SecureNet surge como respuesta a la creciente exposición de los estudiantes frente a amenazas cibernéticas. La falta de formación en ciberseguridad se identificó como una de las principales causas que los hace más vulnerables. Al ofrecer información clara y accesible sobre amenazas comunes como smishing, vishing, pretexting y pharming, SecureNet no solo educa, sino que empodera a los usuarios para que puedan identificar y actuar frente a estos riesgos. Este enfoque es fundamental, ya que muchos estudiantes tienden a confiar en la legitimidad de los enlaces que reciben, lo que aumenta su vulnerabilidad ante fraudes.

Eficiencia en el uso de inteligencia artificial

Uno de los aspectos más innovadores de SecureNet es la incorporación de inteligencia artificial para analizar la seguridad de las URLs. Los algoritmos diseñados para detectar anomalías han mostrado una alta precisión al clasificar enlaces como seguros o maliciosos durante las pruebas realizadas. Este logro valida la decisión de integrar IA en el desarrollo de la plataforma. Además, no solo mejora la experiencia del usuario al proporcionar respuestas rápidas y confiables, sino que establece un estándar elevado para futuros proyectos en ciberseguridad.

Interactividad y experiencia del usuario

La inclusión de un chatbot interactivo, desarrollado mediante Voiceflow, ha añadido un valor significativo a la funcionalidad de la plataforma. Este asistente virtual analiza las respuestas de los usuarios, permitiendo una interacción más personalizada y dinámica. Durante las pruebas realizadas, en el equipo se destacaron lo sencillo que era navegar por la plataforma y acceder a información relevante gracias a esta herramienta. Asimismo, la

interfaz intuitiva, muestra de manera ordenada cada aspecto del chat-bot, por lo que este contribuye a una experiencia agradable, lo que es clave para mantener el interés y la participación de los estudiantes en su aprendizaje sobre ciberseguridad.

Impacto en la cultura universitaria

SecureNet no solo tiene el potencial de mejorar las competencias individuales de los estudiantes en ciberseguridad, sino que también puede influir positivamente en la cultura universitaria en general. Al adoptar prácticas más seguras en su vida académica y personal, los estudiantes pueden convertirse en promotores de la seguridad digital dentro de la comunidad educativa. Este cambio cultural es esencial para reducir los riesgos generales en el campus y fomentar un entorno digital más seguro para todos.

Limitaciones y áreas de mejora

A pesar de la creación de las diversas funcionalidades innovadoras que aborda la página SecureNet, también se identificaron algunos puntos que requieren atención. Es crucial actualizar regularmente la plataforma para abordar nuevas amenazas cibernéticas, dado el ritmo acelerado con el que evolucionan las tácticas de los ciberdelincuentes. Además, sería beneficioso implementar un sistema de retroalimentación donde los usuarios puedan compartir sus experiencias o problemas al utilizar SecureNet. Esto no solo enriquecerá el desarrollo continuo de la herramienta, sino que también fomentará un mayor involucramiento de los estudiantes en su mejora.

Plan de Implementación

Al momento de realizar la implementación de la plataforma Web lo primero que se debe realizar es la generación del hosting y obtener el dominio. Luego se debe decidir el mejor método para atraer a los usuarios y de que el proyecto sea visible. Para ello se debe realizar una investigación del mercado para estructurar una estrategia de lanzamiento mucho más organizada. Se crean los canales para responder de manera oportuna las preguntas y mostrar el funcionamiento de la plataforma a los posibles clientes. Luego, se realiza el lanzamiento de la plataforma, dónde se busqué la retención de los usuarios y la mejora continua de la experiencia al usuario.

El primer lanzamiento, que sería un demo, se realizaría dentro de la universidad EAN, para que los estudiantes logren manipular y familiarizarse con la plataforma, para darle un mejor manejo y minimicen la posibilidad de ser víctimas de estas modalidades. De esta forma comiencen a identificar un poco más sobre los diferentes ataques cibernéticos con relación al Phishing que existen. Y puedan adquirir más conocimientos de la ciberseguridad.

Después, se crearía una estrategia de difusión y concientización para que las personas en general tengan en cuenta los procedimientos de cuidado en ciberseguridad, al mismo tiempo que se promociona la plataforma. Para esta fase, la interfaz será más profesional, también será monetizada para ir optimizándola con nueva información y herramientas que otorguen un mejor análisis y protección cibernético a los usuarios, extendiéndose más allá de solo verificar URLs.

Conclusiones

- La herramienta clasifica los ciberataques más comunes, como phishing, smishing, vishing, pretexting y pharming, y proporciona una experiencia de usuario educativa e interactiva que refuerza los conocimientos de los estudiantes sobre ciberseguridad.
- La implementación de mockups y el desarrollo de secciones detalladas para cada tipo de ataque cibernético brindan una estructura clara y accesible, mejorando la comprensión y la experiencia de los usuarios al interactuar con la plataforma.
- El entrenamiento y evaluación de la IA en la detección de anomalías en URLs, demostró ser un recurso eficaz debido a su alto porcentaje en el entrenamiento,

capaz de identificar amenazas potenciales mediante enlaces y así garantizar una mayor integridad de los datos en el entorno universitario.

- La plataforma permite analizar URLs mediante inteligencia artificial, facilitando la identificación de sitios web seguros y maliciosos, lo cual contribuye a la seguridad de la información personal y académica de los usuarios.
- La implementación del chatbot a nuestra plataforma brinda al estudiante un entorno más dinámico y personalizado, a su vez brindará información más puntual y algunas recomendaciones acordé del ataque al que este confrontando.

Referencias

- *¿Qué es Smishing (phishing por SMS)? | IBM*. (s. f.). https://www.ibm.com/es-es/topics/smishing#:~:text=IBM&text=%C2%BFQu%C3%A9%20es%20el%20smishing%3F,env%C3%ADen%20dinero%20a%20los%20ciberdelincuentes.
- Admin. (s. f.). *Conozca los principales desafíos de seguridad digital que tiene Colombia para el 2024*. Cámara Colombiana de Comercio Electrónico. https://www.ccce.org.co/noticias/conozca-los-principales-desafios-de-seguridad-digital-que-tiene-colombia-para-el-2024/
- Álvarez, C. (2023, 13 enero). Colombia registró un crecimiento de ataques informáticos en el último año. *Voz de América*. https://www.vozdeamerica.com/a/colombia-registro-crecimiento-ataques-informaticos-ultimo-ano-/6916577.html
- Cámara Colombiana de Informática y Telecomunicaciones. (2022, 23 marzo). *Tendencias del cibercrimen 2021 -2022 Nuevas amenazas al comercio electrónico - CCIT - Cámara Colombiana de Informática y Telecomunicaciones*. CCIT - CáMara Colombiana de InformáTica y Telecomunicaciones.

https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-2021-2022-nuevas-amenazas-al-comercio-electronico/

- Cañon, A. M. C. A. (2024, 11 junio). *Colombia es el país más afectado por ataques cibernéticos en América Latina*. Cambio. https://cambiocolombia.com/tecnologia/emcali-registra-un-ciberataque-contra-los-sistemas-de-informacion-de-los-pagos-de
- Casco, A. R. (2020). Efectos de la pandemia de COVID-19 en el comportamiento del consumidor. *Innovare Revista de Ciencia y Tecnología*, *9*(2), 98-105. https://doi.org/10.5377/innovare.v9i2.10208
- Castillo, C. (2024, 4 julio). «Phishing», «vishing», «smishing», ¿qué son y cómo protegerse de estas amenazas? *BBVA NOTICIAS*. https://bbva.com/es/innovacion/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/
- *Ciberseguridad*. (s. f.). Google Books. https://books.google.es/books?hl=es&lr=&id=ZqHDDwAAQBAJ&oi=fnd&pg=PT5&dq=ciberseguridad+que+es&ots=yibb29_yc5&sig=lYVjqmWvz-3sB1HkVPOMy3_PniU#v=onepage&q=ciberseguridad%20que%20es&f=false
- Eugenia, Z. L. M., & Renato, R. C. L. (2023). *Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021*. https://repositorio.ucv.edu.pe/handle/20.500.12692/124989
- Forbes. (2024, 28 febrero). Colombia sigue siendo el país con más ataques de ciberseguridad en Latinoamérica, según IBM. *Forbes Colombia*. https://forbes.co/2024/02/28/tecnologia/colombia-es-el-pais-con-mas-ataques-de-ciberseguridad-en-latinoamerica
- García, J. (2022, 29 septiembre). *Qué es el «vishing» y en qué consiste el timo de la doble llamada del que han alertado la OCU y la. . .* Xataka. https://www.xataka.com/seguridad/que-vishing-que-consiste-timo-doble-llamada-que-han-alertado-ocu-guardia-civil

- Giraldo, L. A. (2022-05-30). Análisis de los tipos de ataques cibernéticos ocurridos en Colombia durante la pandemia covid-19 entre los años 2020 y 2021 Recovered from: http://hdl.handle.net/10654/43621
- Ibm. (2024, 18 julio). ¿Qué es el pretexto? | IBM. *Temas*. https://www.ibm.com/mx-es/topics/pretexting
- Initiative, W. W. A. (s. f.). *Resumen de los estándares de accesibilidad de W3C*. Web Accessibility Initiative (WAI). https://www.w3.org/WAI/standards-guidelines/es
- Instituto Nacional de Ciber Seguridad & Gobierno de España. (2020). *Glosario de términos de ciberseguridad*. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
- *ISO27001 Seguridad Información*. (s. f.). DNV. https://www.dnv.com/ar/services/iso-27001-sistema-de-gestion-de-seguridad-de-la-informacion-3327/#:~:text=%E2%80%8BQu%C3%A9%20es%20la%20norma%20ISO%2027001&text=Ayuda%20a%20las%20organizaciones%20a,la%20seguridad%20de%20la%20informaci%C3%B3n.
- Jiménez-Almeira, G. A., & López, D. E. (2023). *Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. [Cybersecurity and Integral Security: an analysis of regulatory progress in Colombia].* Revista Ibérica De Sistemas e Tecnologias De Informação, , 16-31. https://login.bdbiblioteca.universidadean.edu.co/login?url=https://www-proquest-com.bdbiblioteca.universidadean.edu.co/scholarly-journals/ciberseguridad-y-seguridad-integral-un-análisis/docview/2880949554/se-2
- Jung, J., & Katz, R. L. (2022, 16 noviembre). *Impacto del COVID-19 en la digitalización de América Latina*. https://repositorio.cepal.org/items/cdc4aa8b-7deb-4eb7-a5fd-b72eb4fb699c
- *Kosinski, M. ¿Qué es el phishing? | IBM*. (2024, 17 mayo). https://www.ibm.com/es-es/topics/phishing#:~:text=Colaborador%3A%20Mateo%20Kosinski-,%C2%BFQu

%C3%A9%20es%20el%20phishing%3F,otro%20modo%20a%20la%20ciberdelincuencia.

- *Ley 1273 de 2009 - Gestor Normativo*. (s. f.). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492
- Malaver, C. (2024, 17 enero). Smishing: lea de qué trata este fraude en el que han caído varios bogotanos. *El Tiempo*. https://www.eltiempo.com/bogota/fraude-en-bogota-a-traves-de-mensajes-de-texto-donde-roban-informacion-845090
- Manzanelli. (2023, 10 febrero). *Norma ISO 29148*. NormasISO.org. https://normasiso.org/norma-iso-29148/
- Maroto, J. P. (2009). El ciberespionaje y la ciberseguridad. In *La violencia del siglo XXI. Nuevas dimensiones de la guerra* (pp. 45-76). Instituto Español de Estudios Estratégicos.
- Online, T. H. (2023, 21 diciembre). Smishing vs. Phishing vs. Vishing. *HP TECH TAKES /*. https://www.hp.com/mx-es/shop/tech-takes/smishing-vs-phishing-vs-vishing#:~:text=Por%20ejemplo%2C%20el%20%E2%80%9Cphishing%E2%80%9D,voz%20para%20obtener%20informaci%C3%B3n%20sensible.
- Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del" phishing" y el" pharming". *Revista de derecho (Valparaíso)*, (41), 211-262.
- *Pharming*. (s. f.). https://www.mintic.gov.co/portal/inicio/18805:Pharming
- Ramírez, D. M. R., Garcés-Giraldo, L. F., Doria-Orozco, T., Franco-Castaño, S., Valencia-Arias, A., Rodríguez-Correa, P. A., & Román, J. E. (2023). *Tendencias investigativas en el uso de Machine Learning en la ciberseguridad. [Bibliometric analysis on the use of Machine Learning in cybersecurity].* Revista Ibérica De Sistemas e Tecnologias De Informação, , 60-72. https://login.bdbiblioteca.universidadean.edu.co/login?url=https://www-proquest-com.bdbiblioteca.universidadean.edu.co/scholarly-journals/tendencias-investigativas-en-el-uso-de-machine/docview/2880950428/se-2
- Ríos Ruíz, A. de los Á. (2020). *Vista de EMERGENCIA SANITARIA y TRANSACCIONES ELECTRÓNICAS: COVID – 19 CASO MÉXICO*. https://revistas.ujat.mx/index.php/perfiles/article/view/3901/2939

- Rueda, C. (2024, 24 julio). *¿Qué es el El Vishing y cómo reconocerlo?* Datablog. https://www.datacredito.com.co/blogs/datablog/que-es-el-el-vishing-y-como-reconocerlo/#:~:text=El%20Vishing%20(abreviatura%20de%20phishing,o%20bancarios%20de%20una%20persona.
- Ruiz, D. E. (2024, 22 noviembre). Récord histórico de ciberataques en todo el mundo y las pérdidas de billones de dólares de las empresas en 2025. *Infobae*. https://www.infobae.com/tecno/2024/11/22/record-historico-de-ciberataques-en-todo-el-mundo-y-las-perdida-de-billones-de-dolares-de-las-empresas-en-2025/
- *Smishing*. (s. f.). https://mintic.gov.co/portal/inicio/5796:Smishing
- Torresburriel Estudio. (2022, 8 febrero). *WCAG 2.1: qué son y cómo respetarlas | Torresburriel Estudio*. Blog - UX Torresburriel Estudio. https://torresburriel.com/weblog/wcag-2-1-que-son-y-como-respetarlas/
- Universidad de Antioquia, & Cruz Cárdenas, C. C. (s. f.). *Días sin IVA y Black Friday, ¿cómo compraron los colombianos?* https://www.udea.edu.co/wps/portal/udea/web/generales/interna/!ut/p/z0/vVLLbsIwEPwVc-AY2QQKyRFFlBJBxUNCkEu12A5xcexgG9r8fR1Kq8KhRy7Wjnd3ZndsnOENzhScxR6c0Aqkx9us_xbFSdgZ9sh0vEwTMuwnw9FgtZ6GUYhTnPmC18XTqBMmZEpWkz5ZTObpS9ofJNFz2DCEZpbM9jirwBWBULnGG6qV40owH4ItuTpJcNw0gq7gqACz0wZR4eqmX7wfj9kQZ5emT4c3lTYO5IlxaBOwt6jQJf-OT54fGLcIKLAW7bYgLgUF2yZUcEUFWMQ9ZZPZda8ZoNxQQIwjCSgHepIOWJswXoEX8YM6bW9hU8utuyow6zwRqlHp9ykvVx13Ff1ZuZnyz8ptcr_ynafjdJmQRa-7XpM4nkSj7kM9uU7zzxd48AvZXyMvSIrGfG8q8-WBFSoQZwjqYCeBHoLceIU6oLrUzVEZMFoFUluPpC53ApS2uDpk2_k0n7mo_vgCwXckVQ!!/