INCLUSIÓN DE LA INTELIGENCIA ARTIFICIAL GENERATIVA EN LA DETECCIÓN DE CIBERATAQUES A USUARIOS DEL SECTOR FINANCIERO EN COLOMBIA

Yessica Alejandra Álvarez Carreño[1], Diana Carolina Carrillo Naizaque[1], Luis Alfredo Ortiz Fajardo[1], Estefania Patarroyo Alarcón[1]
[1]Especialización Gerencia en Tecnología – Facultad de Ingeniería.
Universidad Ean.

Resumen.
Actualmente, una de las técnicas utilizadas con mayor frecuencia por los ciberdelincuentes es la llamada Ingeniería social, que consiste en manipular a los usuarios para obtener información confidencial con el fin de usarla en beneficio propio, en el año 2018 las cifras reportada por el Centro Cibernético Policial indica que se registraron cerca de 21.700 denuncias por delitos informáticos en productos financieros, esto representó un aumento del 36 por ciento en lo que respecta a los años anteriores, adicionalmente, en el informe Tanque de Análisis y Creatividad de las TIC TicTac (2023), se contrasta un porcentaje similar de aumento del 34 por ciento entre los años 2021 y 2022, estas cifras son puntualmente de los ciberataques registrados que fueron concluidos. De acuerdo con las cifras mencionadas anteriormente, se acota que el sector financiero es uno de los sectores más afectados por este tipo de ataques tomando en cuenta que para la técnica de ingeniería social no se logra tener control en su totalidad, por lo tanto la mejor forma de prevenir este tipo de ciberataques es la concientización, esta se toma como herramienta para contrarrestar estos ataques y con ello, se emplean y se adaptan modelos tecnológicos usando la inteligencia artificial, todo esto dentro del plan de seguridad tecnológica, el cual permitirá a las entidades financieras adentrarse en la innovación frente a las amenazas en evolución y realizando la detección proactiva de los ciberataques utilizando la ingeniería social para generar conocimiento, experiencia y para lograr disminuir las cifras y regresarle la confianza a los usuarios del sector financiero Colombiano en el uso de canales digitales.

Palabras clave: Inteligencia Artificial, Ciberataques, Ingeniería Social, Concientización, Modelos de Seguridad.

Abstract.
Currently, one of the techniques most frequently used by cybercriminals is so-called social engineering, which consists of manipulating users to obtain confidential information to use it for their own benefit. In 2018, the figures reported by the Cyber Center Police indicate that nearly 21,700 complaints were registered for computer crimes in financial products, this represented an increase of 36% compared to previous years, additionally, in the Analysis and Creativity Tank report of ICT TicTac (2023), a similar percentage increase of 34% is contrasted between the years 2021 and 2022, these figures are specifically from the registered cyberattacks that were concluded. According to the figures mentioned above, it is noted that the financial sector is one of the sectors most affected by this type of attacks, taking into account that the social engineering technique cannot be fully controlled, therefore the best The way to prevent this type of cyberattacks is awareness, this is taken as a tool to counteract these attacks and with this, technological models are used and adapted using artificial intelligence, all of this within the technological security plan, which will allow financial entities delve into innovation against to evolving threats and carrying out proactive detection of cyberattacks using social engineering to generate knowledge, experience and to reduce the numbers and restore confidence to users of the Colombian financial sector in the use of digital channels.

Keywords: Artificial Intelligence, Cyberattacks, Social Engineering, Awareness, Security Model.

1. INTRODUCCIÓN.

Desde la implementación del internet, la comunicación de las personas desde diferentes partes del mundo permitió optimizar tareas, procesos, intercambios de información, que en un pasado eran más complejos o demorados, uno de los primeros usos, fue en el sector militar, en el año 1945, en donde se estaba desarrollando la guerra fría y los equipos militares estaban implementando estrategias para obtener información oportuna en dado caso pudieran sufrir un ataque, esta estrategia se fue extendiendo en otros sectores (Morales J, 2022). De acuerdo con lo anterior, el desarrollo y el uso del internet dio paso a avances significativos que fueron positivos y negativos para la sociedad, también dio paso al uso indebido del mismo, iniciando con el desarrollo de virus maliciosos con el fin de interceptar información confidencial de las personas y las organizaciones con los llamados ciberataques o ataques cibernéticos, uno de los sectores más afectados es el sector financiero.

Entre el 90 por ciento y el 93 por ciento de las entidades financieras en el país, se centran en la implementación de los cortafuegos *(firewalls)* y en las actualizaciones automatizadas de antivirus y de sistemas. Temas como la aplicación de computación cognitiva, internet de las cosas *(Internet of Things –IoT–)* o Registro distribuido *(Blockchain)* para la detección y análisis de eventos de seguridad se encuentran aún muy incipientes con niveles inferiores al 3% en las entidades financieras. (Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, 2020).

Los usuarios se encuentran expuestos de manera significativa ante cada *login,* movimiento y/o transacción que realicen a través de medios digitales ya sea con el teléfono, celular, correo electrónico y/u otro dispositivo o canal. Las principales víctimas de esta técnica son usuarios que pueden tener desde una cuenta de ahorros hasta un portafolio bancario con diferentes productos, sin embargo, los usuarios más expuestos a sufrir este tipo de ataques, son personas con un bajo conocimiento y/o sensibilización de la importancia del resguardo de la información personal o críticamente confidencial, usuarios y/o entidades con precarios estándares de seguridad de la información y para aprovecharse de todo lo anterior, los ciber atacantes utilizan diferentes herramientas como lo son los correos electrónicos con *malware, phishing, baiting, grooming*, entre otras (Méndez-Carvajal, 2018).

Por tanto, la Inteligencia Artificial (IA) empleada para el sector financiero llega como una ayuda a las entidades financieras para fortalecer la seguridad informática de sus productos financieros, donde mencionan que la IA se está convirtiendo en una parte importante de la vida y las expectativas cotidianas de los consumidores, lo que facilita interacciones agradables entre empresas y consumidores. (El Mundo Financiero Newstex, 2023).

Aquí es donde, las entidades deben empezar a implementar estrategias para la mitigación de este tipo de ataques y la inteligencia artificial (IA) entra a ocupar un puesto importante en este asunto, ya que, mediante la implementación y entrenamiento constante de modelos generativos, las inteligencias puestas en marcha logran aprender los diferentes patrones de comportamiento, así identifican las anomalías para adelantarse y prevenir todos estos ataques (Arraz, 2024). Entonces, la adaptación de modelos de Inteligencia Artificial (IA) dentro del plan de seguridad permite a las empresas adentrarse en la innovación frente a las amenazas en evolución ya que va a permitir detección proactiva de los ciberataques, análisis predictivo de los mismos, respuestas automatizadas y una adaptación continua (Acosta, 2024).

De acuerdo con lo anterior, surge la pregunta para la presente investigación ¿En qué medida la inteligencia artificial favorece las medidas de seguridad tecnológica para reducir la ingeniería social en el sector financiero colombiano?

2. MARCO TEORICO.

A continuación, se da a conocer qué aspectos y teorías se han evidenciado sobre el efecto de los ciberataques en la sociedad y en el sector financiero.

Actualmente, una de las grandes amenazas en la sociedad son los ataques cibernéticos, ya que representan una gran amenaza en el ecosistema digital, la mayor amenaza actual, los ciberataques son considerados como todas esas acciones que se

materializan de manera virtual y donde su principal objetivo es obtener información y también destruir la misma para fines ilegales, los ciberataques pueden presentarse de diferentes maneras, todo depende del objetivo que quiera alcanzar el ciber atacante o ciberdelincuente, estas técnicas pueden emplearse de manera individual o en conjunto y pueden llegar a ser virus informáticos, correos no deseados *(spam),* suplantaciones mediante *spoofing,* instalación de archivos espías, entre otros Ureña F. (2015).

De acuerdo con lo anterior, los impactos pueden generar una violación a una vulnerabilidad pueden llegar a ser perjudiciales tanto monetariamente como reputacionalmente, sólo en América Latina y el Caribe, el costo de ciberataques asciende a un promedio de US$90.000 millones al año debido a la falta de una política orientada a la respuesta oportuna de este tipo de incidentes, de acuerdo con la Gestión integral estratégica para el emprendimiento (Universidad de Guanajuato, 2020). Por otro lado, en Colombia el 5 de enero de 2009, en el Congreso de la República se instauró la Ley 1273, en dicha ley se modificó el código penal logrando fortalecer la protección de la información y de los datos en el entorno digital (Congreso de la República, 2009).

En el año de la pandemia 2020 aumentaron los Ciberdelitos, debido a la formalización del trabajo a modalidad virtual en todas las áreas. Por tanto, para ese periodo de tiempo se registraron más de 22.000 casos de Ciberdelitos en comparación con el año 2019 que equivale a un aumento de cerca del 109 por ciento. Sin embargo, los ciberdelitos siguen creciendo para el año 2022 en Colombia, siendo el hurto con mayor número de registros, al transcurrir los años. (Tanque de Análisis y Creatividad de las TIC, 2023).

El Estado de la Ciberseguridad en el Sistema Financiero Colombiano el cual fue preparado y publicado por el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo entre la Asobancaria y la OEA en el año 2020, se menciona en uno de los hallazgos significativos sobre la seguridad digital en las entidades financieras Colombianas desde la perspectiva de usuario de Bancos y otros establecimientos de crédito privilegian los medios virtuales sobre los presenciales, lo cual concuerda con el alto grado de digitalización de los servicios y el impulso a la utilización de estos, ya que el 80 por ciento de los encuestados consulta saldos disponibles y realiza movimientos (transacciones) usando internet, porcentaje muy superior a los que consultan directamente en la oficina con un 22 por ciento, o por línea telefónica 30 por ciento, e igualmente prefieren utilizar las aplicaciones móviles con un 69 por ciento, mientras que lo hacen por cajero automático un 38 por ciento. (Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, 2020, 13).

Por ello, los usuarios prefieren cada día más el uso de canales digitales en las entidades financieras, por tanto, los ciberataques ponen en jaque a estas organizaciones, obligando a mejorar la seguridad de sus plataformas, Las entidades bancarias, los supervisores, las telecos y el Gobierno se han puesto manos a la obra, pero los ciberdelincuentes siempre parecen ir por delante. (Hernández-Sampieri, 2024, 35)

Sin embargo, hoy en día existen varios fraudes que los usuarios de estas entidades financieras viven cada día, entre ellas se encuentran la suplantación de la identidad del usuario, el robo de datos personales e información financiera del usuario; la suplantación de la identidad de la institución de crédito, y evitar el comprometer los medios electrónicos empleados por el usuario, entre otras posibles situaciones. Para ello, la propuesta considera que los bancos deberán contar con un plan de gestión para la prevención del fraude. (Estrada, 2024)

Esto conlleva a afectar la integridad del usuario final, poniendo en peligro su información críticamente confidencial (ICC) y recursos económicos, Además, hay un factor psicológico: los afectados por este tipo de estafas entran en pánico cuando les dicen que su dinero está en riesgo y por eso no dudan en utilizar las credenciales y los datos en el momento en el que se los demandan, aunque eso suponga quedar desprotegidos. (Hernández, 2024, 35).

Los daños psicológicos generan incertidumbre, y se opta por parte de los usuarios afectados, al no uso de los productos financieros, porque se pierde la confianza en la seguridad que brindan las entidades financieras. Motivo por el cual al tener un usuario

en su mayoría digital se debe de implementar en alto grado la ciberseguridad en los canales dispuestos para dicha transaccionalidad.

Por otro lado, en el Estado de la Ciberseguridad en el Sistema Financiero Colombiano se menciona que los riesgos de seguridad de la información de las entidades financieras que merecen mayor atención, sin importar el tamaño de la organización son:

i. Pérdida / robo de activos de información clasificada (confidencial o sensible)
ii. Indisponibilidad de infraestructura crítica
iii. Compromiso de credenciales de usuarios privilegiados. (Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, 2020, 10)

Así mismo, uno de los datos más destacados de dicho informe refiere al 100 por ciento de las entidades financieras de Colombia manifiestan que identificaron algún tipo de evento (ataques exitosos y ataques no exitosos) de seguridad digital en su contra. Los eventos de seguridad digital más comúnmente identificados son:

i. El código malicioso o *malware* el 75 por ciento del total de entidades
ii. El *Phishing, Vishing o Smishing* el 75 por ciento del total de entidades
iii. La violación de políticas de escritorio limpio *(clear desk)* el 70 por ciento del total de entidades

También resulta importante anotar que dentro de las principales motivaciones para la realización de estos ataques se encuentran las económicas con un 75 por ciento y mencionan que no existieron razones como asuntos de reputación personal como *hacker*, asuntos geopolíticos o espionaje. (Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, 2020, 9)

Uno de los principales motivos por los cuales los ciberataques son, en un alto porcentaje exitosos, es porque se aplica la ingeniería social, que son ese conjunto de técnicas psicológicas y habilidades sociales que utilizan los atacantes para obtener información para acceder a diferentes tipos de fuentes, como cuentas bancarias, tarjetas de crédito, redes sociales, entre otras (Ureña J, 2015).

La ingeniería social básicamente se basa en el comportamiento humano y como jugar con las diferentes emociones de las personas, para que, a raíz de diferentes tipos de engaños, los usuarios comprometan sus datos de acceso al sistema y así mismo, revelen información valiosa que esto finalmente entraría a derivar en la pérdida de esa información confidencial (Borghello, 2009).

3. METODOLOGIA.

El enfoque de la investigación tiene una perspectiva mixta, debido a que se analizará la experiencia que han tenido actualmente los usuarios del sector financiero frente al impacto de la ingeniería social, por lo tanto, se analizará cuantitativamente el impacto y cualitativamente la experiencias. Este alcance se define con el fin de dimensionar la experiencia y el conocimiento del usuario con el concepto de la ingeniería social, considerando que tan cercanos han estado a este y qué experiencias positivas o negativas han tenido frente a las técnicas ingeniería social.

El diseño es no experimental dado que las variables no serán manipuladas, porque se obtendrán en un solo momento donde se recolectarán los datos por medio de una encuesta, siendo así un tipo de estudio correlacional, donde se validará la relación que existe entre las variables cualitativas y cuantitativas, analizando las hipótesis que se puedan generar entre ellas.

3.1 Población y muestra.

La muestra que se ha tomado para el presente estudio de investigación consideró los criterios de género, edad, ciudad de residencia, nivel de escolaridad, ocupación y usuario activo en el sistema financiero con al menos un producto bancario. Teniendo en cuenta la última variable se validó con el Reporte de Inclusión Financiera 2023 donde en este año se consideraron 36,1 millones de adultos con productos financieros transaccionales, de ahorro o financiamiento formal. (Superintendencia Financiera de Colombia, 2024).

Conforme a ello la ecuación que se tendrá en cuenta para la muestra corresponde a una variable cualitativa para una proporción de una población conocida, de acuerdo con lo que menciona la Guía para el diseño y desarrollo de trabajos de investigación de Doctorados en la Escuela de Posgrados de la Universidad Wiener. (UNIVERSIDAD NORBERT WIENER, 2013, 38). A continuación, se

definen a que hacen referencia cada una de las variables de la ecuación:

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

- n = Tamaño de la muestra.
- N = Tamaño de la población.
- Z = Valor de la variable de distribución normal estándar correspondiente al nivel de confianza deseado
- p = Proporción estimada de la característica de interés en la población
- E = Margen de error que estás dispuesto a aceptar

Reemplazando los datos, se obtiene:

- n = Tamaño de la muestra.
- N = 36.100.000
- Z = 1.67
- p = 0.3
- E = 0.07
-

$$n = \frac{36.100.000 \times (1.67)^2 \times 0.3 \times (1-0.3)}{(0.07)^2 \times (36.100.000-1) + (1.67)^2 \times 0.3 \times (1-0.3)}$$

$$n = \frac{21.188.369}{177.587{,}543}$$

$$n = 119{,}31$$

$$n \approx 120 \quad (1)$$

El tamaño de la muestra corresponde a 120 encuestas para una población de 36.100.000 personas, con un margen de error del 7 por ciento y un nivel de confianza del 95 por ciento.

3.2 Instrumentos

El instrumento de recolección seleccionado es una encuesta, por medio de ésta, se proyectan los resultados de la muestra a una población más general, adicionalmente, este tipo de instrumento es muy conocido por los individuos y su diligenciamiento es bastante sencillo.

La encuesta que se dividió en dos secciones: la primera sección constó de 15 preguntas en donde se buscó analizar la población encuestada desde los aspectos básicos que van desde género y/o edad hasta conocer a profundidad si han sido víctimas de fraude y de qué tipos de fraude, la segunda sección constó de 14 preguntas tipo escala Likert en donde se buscó medir las percepciones y supuestos de los usuarios del sector financiero frente al uso de la inteligencia artificial y el auge de la ingeniería social, desde los factores de percepción, seguridad, vulnerabilidad y usabilidad.

La encuesta se aplicó de manera virtual mediante un formulario en *Google Forms* que fue compartido a familiares, amigos y conocidos por medio de diferentes redes sociales en donde se obtuvo un total de 120 respuestas que equivale al mismo número de la muestra, en la siguiente tabla se observa el detalle de esta.

3.3 Técnicas de análisis

Para la presente investigación se aplicaron técnicas de análisis cuantitativas, los datos recolectados por medio de una encuesta estructurada serán procesados mediante el *software* estadístico SPSS de IBM. Inicialmente, se analizará la correlación entre las diferentes variables con el fin de identificar si tienen una correlación entre sí, que tan fuerte es y si esta conexión es positiva o negativa, en segundo lugar, se aplicará una prueba de hipótesis con el fin de determinar si los resultados obtenidos son lo suficientemente significativos para tomar decisiones de acuerdo con el objetivo de la investigación. A continuación, se relaciona el detalle de los tipos de análisis usados para la respectiva evaluación de los datos:

Tabla 1. Evaluación de los datos.

Tipo de análisis	Definición	Herramienta
Correlación	Analiza la relación entre dos o más variables cuantitativas, sin inferir causalidad con el fin de determinar si hay o no correlación.	Para obtener este resultado se utilizó el software SPSS de IBM.
Prueba de hipótesis	Esta técnica consiste en una prueba estadística que permite tomar decisiones sobre la población basándose en una muestra, mediante el análisis del p-valor o el valor de significancia.	Para obtener este resultado se utilizó el software SPSS de IBM utilizando el coeficiente de correlación de Pearson

Fuente: Elaboración propia.

Para interpretar los resultados de las variables se establecerá el rechazo y la aprobación de la hipótesis de la siguiente manera:

- Si el p valor o valor de significancia es mayor a 0.05 se rechaza la hipótesis alterna (H1) y se acepta la hipótesis nula (H0). (Triola, 2018)
- Si el p valor o valor de significancia es menor a 0.05 se acepta la hipótesis alterna (H1) y se rechaza la hipótesis nula (H0). (Triola, 2018)

Por lo tanto, si la correlación arroja un resultado -r correlación de Pearson- positiva significa que, si una variable crece la otra variable también, pero si la correlación es negativa indica que si una variable crece la otra variable disminuye. De acuerdo, a cada resultado se obtendrá el resultado de la correlación que permite clasificar cualitativamente de la siguiente manera:

Tabla 2. Niveles de Correlación

R	relación	correlación
r = 0	No existe	nula
0,00< r ≤ 0,20	muy poco intensa	pequeña
0,20< r ≤ 0,40	pequeña/apreciab.	baja
0,40< r ≤ 0,60	considerable	regular
0,60< r ≤ 0,80	intensa	alta
0,80< r ≤ 1,00	muy intensa	muy alta

Fuente: (Triola, 2018)

3.4 Resultados.

Los resultados obtenidos en la presente investigación constan principalmente de las 21 preguntas realizadas a los encuestados, donde se dividió en 4 factores a validar, tales como percepción, privacidad y almacenamiento de los datos, vulnerabilidad y usabilidad. A continuación, se mencionan los resultados de estos y posteriormente el análisis que se dio para estos.

Para el primer factor de Percepción el 51,7 por ciento de la muestra afirma no conocer el concepto de ingeniería social. El 49,1 por ciento está totalmente de acuerdo en el uso de la ingeniería social y que esta puede ser utilizada para realizar fraudes financieros. Por otro lado, el 28,4 por ciento no están de acuerdo ni en desacuerdo con respecto a cómo identificar manipulaciones con ingeniería social y prevenir intentos de fraude. El 42,2 por ciento están totalmente de acuerdo con que la inteligencia artificial puede ayudar a identificar transacciones fraudulentas de manera óptima que los sistemas tradicionales. De esta manera, el 56 por ciento está totalmente de acuerdo que las entidades financieras deberían emplear con mayor frecuencia la inteligencia artificial para combatir los fraudes. Y por último, 39,7 por ciento no está de acuerdo ni en desacuerdo en que la entidad financiera en la que se manejan los productos financieros está utilizando las últimas tecnologías para mitigar los intentos de fraude.

Para el segundo factor de privacidad y almacenamiento de datos, el 49,1 por ciento afirma que confía en cierta medida que los proveedores de servicios en la nube que usa protegen adecuadamente la información financiera del cliente. Por otro lado, el 39,7 por ciento dicen que no es fácil ni difícil gestionar sus preferencias de privacidad y seguridad a través de los canales proporcionados por el banco. Así mismo, el 31 por ciento afirman que son bastantes conscientes de cómo los bancos recopilan y utilizan los datos personales del encuestado. En cuanto a la toma de medidas adecuadas para proteger la privacidad en los servicios bancarios en línea, los encuestados prefieren las siguientes 2, la primera con un 62,1 por ciento de aceptación de utilizar autenticación multifactor para acceder a los servicios bancarios en línea y en el segundo con el 61,2 por ciento revisan regularmente la actividad de la cuenta para detectar transacciones sospechosas. Por último, el 47,4 por ciento considera que las transacciones realizadas a través de su banco en línea son bastantes seguras.

En cuanto al tercer factor de vulnerabilidad, el 45,7 por ciento considera que el ataque de ingeniería social más común que tiene que ver con productos financieros es el Phishing (correos electrónicos fraudulentos). Además, el 36,2 por ciento ocasionalmente (menos de una vez al mes) ha recibido correos electrónicos o mensajes sospechosos solicitando información personal y/o confidencial sobre productos financieros. Por tanto, el 44 por ciento no se siente seguro ni inseguro identificando un intento de ataque de ingeniería social sobre productos financieros. Por ello, el 78,4 por ciento de los encuestados afirma que en caso de recibir un correo de un remitente desconocido solicitando información confidencial sobre un producto financiero, ignora o elimina la comunicación. Finalmente, el 40,5 por ciento no ha recibido formación sobre cómo prevenir ataques de ingeniería social.

Finalmente, para el cuarto y último factor de uso de inteligencia artificial (IA) el 49,1 por ciento de los encuestados afirma que no está de acuerdo ni en desacuerdo en el papel que está desempeñando la Inteligencia Artificial (IA) en la detección de ciberataques en el sector financiero en Colombia está trayendo buenos resultados en materia de ciberseguridad. El 50,9 por ciento de la muestra también afirma que no está de acuerdo ni en desacuerdo en cuanto a la efectividad de las soluciones de Inteligencia Artificial (IA) para detectar ciberataques en comparación con los métodos tradicionales. Por otro lado, el 49,1 por ciento de los encuestados tienen una idea general del uso de inteligencia artificial (IA) en la detección de ciberataques en el sector financiero. Por lo tanto, en las recomendaciones que mayor porcentaje arrojaron en la mejora de la implementación y el uso de Inteligencia Artificial (IA) en la detección de ciberataques en el sector financiero en Colombia están con el 62,1 por ciento una mejor integración con sistemas existentes e Inversión en tecnologías de vanguardia y con un 50,9 por ciento una mayor inversión en formación y capacitación. Finalmente, el 51,7 por ciento considera muy importante las consideraciones regulatorias y éticas en la implementación de Inteligencia Artificial (IA) para la ciberseguridad dentro de la organización.

3.5 Análisis y discusión de resultados.

Para la presente investigación se realizó el análisis de resultados por factores, lo que permite un mejor entendimiento de cada variable definida. Iniciando así con el factor de Percepción en la Tabla 3 y 4

Tabla 3. Hipótesis y resultado del factor de percepción

Hipótesis	Resultado hipótesis	Estadística		Resultado
H1 - Hipótesis alterna De acuerdo con los entrevistados la conciencia de lo que es la ingeniería social y como se utiliza para realizar fraudes tiene correlación con que las entidades financieras deban emplear con mayor frecuencia la inteligencia artificial para combatir fraudes.	Se acepta la hipótesis alterna	**p_valor**	0,001	Los usuarios del sector financiero conocen las implicaciones de la ingeniería social y esperan que las entidades financieras logren implementar con mayor frecuencia medidas para combatir fraudes con el uso de la inteligencia artificial.
		Nivel de Correla-ción	0,535 Regular	
H0 - Hipótesis nula De acuerdo con los entrevistados la conciencia de lo que es la ingeniería social y como se utiliza para realizar fraudes no tiene correlación con que las entidades financieras deban emplear con mayor frecuencia la inteligencia artificial para combatir fraudes.				

Fuente: Elaboración propia.

Tabla 4. Hipótesis y resultado para el factor de percepción

Hipótesis	Resultado hipótesis	Estadística		Resultado
H1 - Hipótesis Alterna De acuerdo con los entrevistados la conciencia de lo que es la ingeniería social y como se utiliza para realizar fraudes tiene	Se acepta la hipótesis alterna	**p_valor**	0,043	Los usuarios del sector financiero conocen las implicaciones de la ingeniería social y esperan que las entidades financieras continúen educando
		Nivel de Correla-ción	0,188 Pequeño	

Hipótesis	Resultado hipótesis	Estadística		Resultado
correlación con que las entidades financieras eduquen en cómo identificar la ingeniería social. **H0 - Hipótesis Nula** De acuerdo con los entrevistados la conciencia de lo que es la ingeniería social y como se utiliza para realizar fraudes no tiene correlación con que las entidades financieras eduquen en cómo identificar la ingeniería social.				con mayor frecuencia las medidas para combatir fraudes de la ingeniería social.

Fuente: Elaboración propia

Para el segundo factor que es privacidad y almacenamiento de datos en la siguiente tabla se presentan las hipótesis y resultados en la tabla 5

Tabla 5. Hipótesis y resultado para el factor de privacidad y almacenamiento de datos.

Hipótesis	Resultado hipótesis	Estadística		Resultado
H1 - Hipótesis alterna De acuerdo con los entrevistados la confianza de los usuarios en las tecnologías utilizadas por las entidades financieras para mitigar el fraude tiene correlación con el nivel de conciencia sobre cómo se recopilan y utilizan sus datos personales. **H0 - Hipótesis nula** De acuerdo con los entrevistados la confianza de los usuarios en las tecnologías utilizadas por las entidades financieras para mitigar el fraude no tiene correlación con el nivel de conciencia sobre cómo se recopilan y utilizan sus datos personales.	Se acepta hipótesis nula	**p_valor** **Nivel de Correla-ción**	0,889 -0,013 Pequeño	Los usuarios del sector financiero pueden estar informados pero esta conciencia no afecta directamente su confianza en las medidas de seguridad implementadas por los bancos.

Fuente: Elaboración propia

Para el tercer factor que es vulnerabilidad en la siguiente tabla se presentan las hipótesis y resultados en la tabla 6

Tabla 6. Hipótesis y resultado para el factor de vulnerabilidad.

Hipótesis	Resultado hipótesis	Estadística		Resultado
H1 - Hipótesis alterna De acuerdo con los entrevistados que tan seguros se sienten identificando un ataque de ingeniería social sobre productos financieros tiene correlación si han recibido formación sobre cómo prevenir ataques de ingeniería social. **H0 - Hipótesis nula** De acuerdo con los entrevistados que tan seguros se sienten identificando un ataque de ingeniería social sobre productos financieros no tiene correlación si han recibido formación sobre cómo prevenir ataques de ingeniería social.	Se acepta hipótesis alterna	**p_valor**	0,001	A pesar de que los usuarios del sector financiero han recibido información sobre cómo prevenir un ciberataque su nivel se seguridad no aumenta esto conlleva a que no se sienten seguros identificando un intento de ciberataque.
		Nivel de Correla-ción	-0,299 Baja	

Fuente: Elaboración propia

Para el último factor que es uso de la inteligencia artificial (IA) en la siguiente tabla se presentan las hipótesis y resultados en la tabla 7

Tabla 7. Hipótesis y resultado para el factor de uso de la inteligencia artificial (IA)

Hipótesis	Resultado hipótesis	Estadística		Resultado
H1 - Hipótesis alterna El desempeño del papel de la Inteligencia Artificial (IA) en detección de ciberataques trae buenos resultados en materia de ciberseguridad tiene correlación con la efectividad de las soluciones de inteligencia artificial para detectar ciberataques en el sector financiero en Colombia en comparación con los métodos tradicionales. **H0 - Hipótesis nula** El desempeño del papel de la Inteligencia Artificial (IA) en detección de ciberataques trae buenos resultados en materia de ciberseguridad no tiene correlación con la efectividad de las soluciones de inteligencia artificial para detectar ciberataques en el sector	Se acepta hipótesis alterna	**p_valor**	0,001	Lo que indican los usuarios es que el papel de la inteligencia artificial en la detección de ciberataques mejora en gran medida al papel ha desempeñado los métodos tradicionales.
		Nivel de Correla-ción	-0,299 Baja	

financiero en Colombia en comparación con los métodos tradicionales.				

Fuente: Elaboración propia

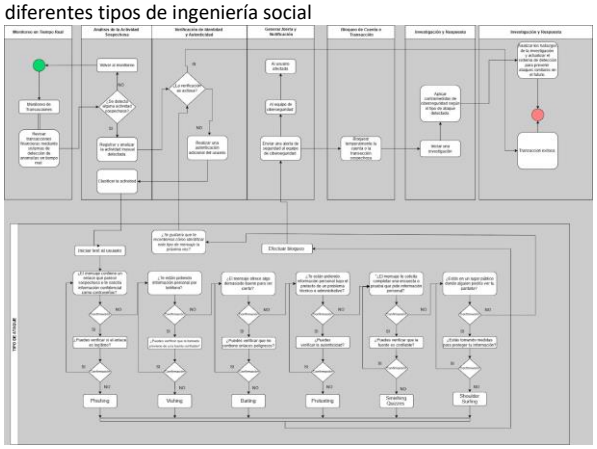
4. PROPUESTA DE SOLUCIÓN.

Se propone un modelo innovador para la identificación y prevención de diferentes tipos de ingeniería social, especialmente enfocado en el sector financiero colombiano. Este modelo se basa en el uso de Inteligencia Artificial (IA) como herramienta clave para no solo detectar y prevenir las tácticas utilizadas por los ciberatacantes, sino también para capacitar al usuario en el reconocimiento de señales de un posible ataque. A través de este enfoque, la IA facilita una retroalimentación continua que permite a los usuarios aprender a identificar y manejar situaciones sospechosas, lo que contribuye a una mayor resiliencia frente a intentos de fraude cibernético.

Además, se propone implementar un sistema que identifique y recopile patrones de fraude a partir de diversas fuentes de datos, como transacciones financieras, registros de acceso y las interacciones en línea. Esta recopilación de datos fortalecería el sistema de Inteligencia Artificial (IA), mejorando la precisión en la detección de ciberataques y adaptando la respuesta a las particularidades del sector financiero colombiano. Al integrar estos datos, el modelo sería capaz de identificar comportamientos anómalos y patrones sospechosos de fraude con mayor efectividad, lo que permitiría una intervención temprana y una protección más robusta.

El modelo también incorpora una funcionalidad interactiva para los usuarios, donde se presenta una ventana de pregunta que invita a reflexionar: "¿Te gustaría que recordemos cómo identificar este tipo de mensaje la próxima vez?" Este mecanismo tiene como objetivo no solo educar al usuario sobre las mejores prácticas para detectar intentos de ingeniería social, sino también aumentar su conciencia sobre los riesgos asociados con los ciberataques, Al integrar esta herramienta educativa, tanto las entidades bancarias como los clientes.

Figura 1. Modelo para la identificación y prevención de diferentes tipos de ingeniería social



Fuente: Elaboración propia

5. DISCUSIÓN.

En la actualidad, la inteligencia artificial (IA) ha emergido como una herramienta clave para mejorar la detección y prevención de ciberataques, especialmente en sectores críticos como el financiero. Si bien los métodos tradicionales de seguridad continúan siendo utilizados, la IA presenta claras ventajas al procesar grandes volúmenes de datos en tiempo real, identificar patrones de comportamiento anómalos y adaptarse a tácticas emergentes de los ciberatacantes.

Sin embargo, a pesar de las mejoras tecnológicas, la confianza de los usuarios en la seguridad de sus instituciones financieras no ha aumentado proporcionalmente. Esto indica que, aunque los usuarios están informados sobre las amenazas cibernéticas y las medidas preventivas, existe una desconexión entre el conocimiento teórico y la capacidad real para identificar y reaccionar ante un ciberataque. Esta situación plantea interrogantes sobre la efectividad de las iniciativas educativas actuales y su capacidad para generar un cambio significativo en los comportamientos de los usuarios.

A medida que las instituciones financieras implementan modelos avanzados de detección basados en IA, la privacidad y la protección de los

datos deben seguir siendo una prioridad. Si bien la IA tiene un enorme potencial para transformar la ciberseguridad, es crucial que estos sistemas sean transparentes, éticos y respeten las normativas de privacidad. La recopilación de datos sobre transacciones y comportamientos de los usuarios puede mejorar la precisión de la detección de fraudes, pero también plantea riesgos en términos de protección de la información sensible. Por lo tanto, es esencial que las entidades financieras aseguran que sus sistemas de IA no solo sean eficaces en la identificación de fraudes, sino también responsables en el manejo de datos personales, lo que contribuiría a generar una mayor confianza en las medidas de seguridad implementadas.

6. CONCLUSIONES.

Los correos electrónicos fraudulentos es la ingeniería social que más se presenta en un mes, donde los usuarios del sector financiero toman la decisión de ignorarlos o eliminarlos, por lo tanto, así las entidades financieras difundan información de cómo prevenir la ingeniería social los usuarios no se sienten seguros identificando un intento de ataque.

Los usuarios del sector financiero colombiano tienen un leve conocimiento en lo que es la ingeniería social y tienen la percepción de que las entidades financieras no los están educando adecuadamente con respecto a esta metodología de fraude, a su vez, consideran que el uso de la inteligencia artificial ayuda a prevenir los fraudes y que las entidades financieras deben aprovechar los beneficios de esta tecnología para combatir este tipo de ciberataques.

Las estrategias para que los usuarios de las entidades financieras colombianas conozcan e implementen las diferentes herramientas de inteligencia artificial (IA) para prevenir los ciberataques requiere de una integración con los sistemas existentes e inversión en tecnologías de vanguardia además de una mayor inversión en formación y capacitación, tanto a los clientes internos como externos de las organizaciones con el fin de mitigar el riesgo actual que se encuentra latente en la sociedad.

7. REFERENCIAS.

Acosta, N. (2024). Impacto de la inteligencia artificial en la ciberseguridad empresarial: un análisis crítico de la evolución de amenazas y medidas preventivas. Tomado de: http://190.15.129.146/bitstream/handle/49000/15738/PI-UTB-FAFI-SIST-00011.pdf?sequence=1&isAllowed=y

Alzahrani, A. (2020). Coronavirus Social Engineering Attacks: Issues and Recommendations [Ataques de Ingeniería Social Relacionados con el Coronavirus: Problemas y Recomendaciones]. 11(IJACS).

Anderson, R. (2001). Security engineering: A guide to building dependable distributed systems. Wiley.

Asobancaria (2019). Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector- financiero-para-Colombia-y-America-Latina.pdf

Arraz, A. (2024). Ciberseguridad empresarial: Ransomware y el impacto de la inteligencia artificial y la inteligencia artificial generativa. Tomado de: https://openaccess.uoc.edu/bitstream/10609/149629/1/aarrazTFM0124.pdf

Avance Jurídico Casa Editorial Ltda. (s. f.). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. Avance Jurídico Casa Editorial Ltda., Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Banco de la República. (2020, June 10). Funciones del Banco de la República. Banco de la República. Retrieved August 29, 2024, from https://www.banrep.gov.co/es/banco/funciones

Banco de la República. (2020, July 03). Bancos comerciales. Banca comercial. https://enciclopedia.banrepcultural.org/index.php?title=Banca_comercial

Bancolombia. (2020, October 23). Normas NIIF Colombia: claves para adoptarlas en las pymes. Bancolombia. Retrieved August 29, 2024, from https://www.bancolombia.com/negocios/actualizat

e/administracion-y-finanzas/normas-niif-pymes-colombia

BBVA Research (2014). Inclusión financiera y el papel de la banca móvil en Colombia: desarrollos y potencialidades. https://www.bbvaresearch.com/wp-content/uploads/mult/WP_1401_tcm346-417763.pdf

Borghello, C. (2009). El arma infalible: la Ingeniería Social. Tomado de: https://acortar.link/DNZlWb

CE Noticias Financieras. (2024, 08). How artificial intelligence will revolutionize financial institutions in Latin America [Cómo la inteligencia artificial revolucionará las instituciones financieras en América Latina].

Congreso de Colombia. (1991, July 04). Decreto 1730 de 1991 - Gestor Normativo. Función Pública. Retrieved August 29, 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=1514

Congreso de Colombia. (1993, December 23). Ley 100 de 1993 - Gestor Normativo. Función Pública. Retrieved August 29, 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=524

Congreso de Colombia. (1999, August 03). Ley 510 de 1999 - Gestor Normativo. Función Pública. Retrieved August 29, 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=9916

Congreso de Colombia. (2009, July 15). Ley 1328 de 2009 - Gestor Normativo. Función Pública. Retrieved August 29, 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36841

Coomeva. (2023, August 23). ¿Qué es una aseguradora y cómo funciona? Coomeva Corredores de Seguros. Retrieved August 29, 2024, from https://corredoresdeseguros.coomeva.com.co/corredor/publicaciones/174836/que-es-una-aseguradora-y-como-funciona/

Departamento Nacional de Planeación. (2023, November 25). ¿Qué es el Plan Nacional de Desarrollo? Departamento Nacional de Planeación. Retrieved August 29, 2024, from https://www.dnp.gov.co/plan-nacional-desarrollo

El Mundo Financiero Newstex (Ed.). (2023, Febrero 16). El Mundo Financiero: IA, metaverso, blockchain y Foundational Tech, tendencias tecnológicas clave para 2023.

Estrada, S. (2024). Fintech ayudarían a modernizar la ciberseguridad bancaria para detectar y prevenir fraudes. CE Noticias Financieras.

Hernández, M. (2024, 01). Las ciberestafas crecen y mutan: spoofing, phising y otras formas virtuales de defraudar. Actualidad Económica, 35.

Hinson, G. (2008, 04). SOCIAL ENGINEERING TECHNIQUES, RISKS, AND CONTROLS. [Técnicas de Ingeniería Social, Riesgos y Controles] 37(EDPACS), 32-46.

ICETEX. (2023, October 06). Defensor del consumidor financiero. ICETEX. Retrieved August 29, 2024, from https://web.icetex.gov.co/es/atencion-al-ciudadano/defensor-del-consumidor-financiero

McCarthy, J. (1956). Programs with common sense. Stanford University.

Mendez, A. (2018). Estudio de metodologías de ingeniería social. Universidad Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/90305/6/amendezcarTFM12189memoria.pdf

Morales, J (2022). Influencia del COVID 19 en el incremento de los Ciberataques a Nivel Mundial, Tomado de: https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11574/Ataques%20ciberneticos_Trabajo%20grado_Juan%20Morales_v2.pdf?sequence=1&isAllowed=y

Piaget, J. (1979). La inteligencia y la percepción. En Psicología de la inteligencia (p. 63). Buenos Aires, Argentina: Editorial Psique.

Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo. (2020).

Estado de la Ciberseguridad en el Sistema Financiero Colombiano. Organización de los Estados Americanos. https://publicaciones.asobancaria.com/wp-content/uploads/Libros/web/Estado%20de%20la%20ciberseguridad%20en%20el%20sistema%20financiero%20colombiano.pdf

Scotiabank Colpatria. (2022, June 30). ¿Qué son las Sociedades Comisionistas? Scotiabank Colpatria. Retrieved August 29, 2024, from https://www.scotiabankcolpatria.com/educacion-financiera/productos-y-servicios/sociedades-comisionistas

Superintendencia Financiera de Colombia. (2024, July 9). Acerca de la SFC. Superintendencia Financiera de Colombia. Retrieved August 29, 2024, from https://www.superfinanciera.gov.co/publicaciones/60607/nuestra-entidadacerca-de-la-sfc-60607/

Superintendencia Financiera de Colombia. (2024, June 4). Reporte de Inclusión Financiera 2023: avances y retos en Colombia. Superintendencia Financiera de Colombia. Retrieved September 13, 2024, from https://www.superfinanciera.gov.co/publicaciones/10115193/reporte-de-inclusion-financiera-2023-avances-y-retos-en-colombia/

Supersolidaria. (1988, December 23). 3. ¿Qué cooperativas pueden ejercer actividad financiera? Supersolidaria. Retrieved August 29, 2024, from https://www.supersolidaria.gov.co/es/content/3-que-cooperativas-pueden-ejercer-actividad-financiera

Tanque de Análisis y Creatividad de las TIC TicTac. (2023, 05). "IA para la protección y prevención de amenazas". https://www.ccit.org.co/estudios/estudio-anual-de-ciberseguridad-2022-2023/

Triola, M. F. (2009). Estadística (Décima ed.). Pearson - Addison Wesley.

Universidad de Guanajuato (2020). Gestión integral estratégica para el emprendimiento de la mipyme. Tomado de: https://acortar.link/6qWUSy

Universidad Jorge Tadeo Lozano. (2021, May 15). Bolsa de Valores de Colombia | Universidad de Bogotá Jorge Tadeo Lozano. Utadeo. Retrieved August 29, 2024, from https://www.utadeo.edu.co/es/proyecto/cuarto-congreso-latinoamericano-de-historia-economica/7516/bolsa-de-valores-de-colombia-0

Universidad Norbert Wiener. (2013). Guía para el diseño y desarrollo de trabajos de investigación de doctorados en la escuela de posgrado de la Universidad Wiener.

Ureña, J. (2015). Ciberataques, la mayor amenaza actual. Tomado de: https://www.ieee.es/

Westin, A. F. (1967). Privacy and freedom. Atheneum, from https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr&ref=hackernoon.com

Unidad Especializada de Ciberseguridad de Entel Digital y su Centro de Ciber Inteligencia (CCI) (2024,4) Reporte de Ciberseguridad. https://enteldigital.cl/reporte-ciberseguridad