UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingeniería de Sistemas Informáticos

El papel de la Inteligencia Artificial en la detección del fraude del correo electrónico: Un estudio sistemático de los modelos actuales de Machine Learning y Deep Learning.

PROYECTO FIN DE GRADO

Yassmin Biratate Metni
Grado en Ingeniería de Software
Madrid, 2025

UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingeniería de Sistemas Informáticos

Grado en Ingeniería de Computadores

El papel de la Inteligencia Artificial en la detección del fraude del correo electrónico: Un estudio sistemático de los modelos actuales de Machine Learning y Deep Learning.

PROYECTO FIN DE GRADO

Yassmin Biratate Metni
Grado en Ingeniería de Software

Bajo la dirección de:
Dr. Giannicola Scarpia
Madrid, 2025

Título: El papel de la Inteligencia Artificial en la detección del fraude del correo electrónico: Un estudio sistemático de los modelos actuales de Machine Learning y Deep Learning.

Autor: Yassmin Biratate Metni

Grado en Ingeniería de Software

Dirección:

Dr. Giannicola Scarpia

Este trabajo, la antesala a la etapa final de todo un proyecto de formación de muchos años se lo quiero dedicar a la persona más importante de mi vida, mi madre, que en todas de las tardes desde infantil hasta en la universidad tras la vuelta de clases me esperaba con su taza de café en mano apoyándome en las largas sesiones de estudio, sin faltar, a ella, esto es suyo.

El resto de mi familia, a mi padre y a mi hermano que siempre han hecho todo lo posible para que este camino sea lo más ameno posible con los viajes de ida y venida a la escuela siempre que la situación lo permitía y necesitaba, el recambio de la tinta de la impresora y su apoyo emocional que sin lugar a duda son pequeños detalles que me han sido de gran ayuda.

A mis profesores de todas las etapas a los que siempre me han ayudado desde las cuestiones más sencillas hasta las más complejas, a ellos les debo el haberme formado y encaminado hasta este punto, en especial a mi tutor de este trabajo quien ha sido también mi profesor de las materias de Fundamentos de Computadores y Quantum Computing, Gianni que siempre me ha ayudado incluso en mis peores momentos e interesado y charlando por todos los temas de referencia en el mundo de la informática, a todos ellos quiero darles las gracias por haber confiado en mí y por toda la persistencia y ganas de aprendizaje que habéis cultivado en mí, mil gracias.

También quiero darle las gracias a mis compañeros de todas las etapas a las que la vida y los tiempos nos han separado los caminos, me lo he pasado de maravilla aprendiendo junto con vosotros, a mis amigos que siempre me han dado un hombro en el que apoyar a mi pareja que, a pesar de la distancia a través de sus ojos, las cuestiones más difíciles se hacían las más sencillas y como no a Marta, futura médico con la que he disfrutado de las sesiones de estudio en las etapas finales de mi trayectoria universitaria siendo la mejor compañera de estudio.

¡Muchas gracias a todos y a los que leáis este trabajo, espero que disfrutéis del mismo tanto como yo haciéndolo!

Agradecimientos

¡A todas aquellas cincuenta y cinco personas anónimas que participaron en las preguntas de la encuesta y a mi tutor Gianni por la guía durante todo este proyecto y paciencia hasta el final, muchas gracias a todos por vuestro apoyo ante esta iniciativa!

Abstract

This study aims to systematically review and synthesize information about models for detecting and classifying phishing e-mails attacks. These attacks consist of launching a malicious e-mail to a victim in order to obtain personal information such as credentials, bank details, personal data among other substantial information, or for the installation of malicious software on the victim's device. To this end, a questionnaire was conducted in order to support the veracity of the statistics regarding this problem with participants in Europe, Africa, North America and South America in order to identify trends of phishing attacks including phishing e-mail attacks with different age groups and locations around the world.

Moreover, searches have been made in IEEE Xplore and ScienceDirect databases in order to synthesize and analyze information on the proposed models to serve as a basis for the study of new models. These proposed models essentially use supervised machine learning algorithms such as Support Vector Machine, Decision Tree, Random Forest, k-Nearest Neighbours, Naïve Bayes and Logistic Regression. In addition, deep learning algorithms like recurrent neural networks such as Long-Short Term Memory, Bidirectional Long-Short Term Memory, Gated Recurrent Units and Bidirectional Encoder Representations from Transformers in natural language processing. The performance of each model is measured with a confusion matrix deriving measurements about the percentage of accuracy of the models in the detection of true positives, also their precision, sensitivity and F1 score.

Once the results have been obtained, a future trend is identified for machine learning and deep learning algorithms, as a reinforcement for novel architecture or comparison with emerging algorithms like metaheuristic algorithms inspired in biology. For conclusions, the lack of standardization in the industry is observed, for the implementation in e-mail messaging services. Also, the urgency to bring up new proposals is raised.

Keywords: machine learning, deep learning, emails, phishing attacks

Resumen

El trabajo trata del estudio de los ataques de *phishing* que consiste en el lanzamiento de un correo malicioso sobre una víctima con el objetivo de conseguir información personal como pueden ser credenciales, datos bancarios, datos personales entre otros o para la instalación de un software malicioso en el dispositivo de la víctima. Con tal fin se ha realizado una encuesta a efectos de respaldar la veracidad de las estadísticas con respecto a esta problemática a participantes de los continentes de Europa, África, América del Norte y América del Sur con el fin de identificar las tendencias de los ataques de *phishing* en los diferentes grupos de edad y ubicaciones.

Asimismo se ha realizado búsquedas en las bases de datos de IEEE Xplore y ScienceDirect con el fin de sintetizar y analizar la información sobre los modelos propuestos que sirvan como base a la hora de estudiar nuevos modelos de detección y clasificación de correos electrónicos fraudulentos, se han observado tendencias en el uso de modelos con algoritmos de *machine learning* supervisados como máquinas de vectores de soporte o *Support Vector Machine*, árbol de decisión o *Decision Tree*, bosque aleatorio o *Random Forest,* k vecinos más cercanos *o k-Nearest Neighbours,* Naïve Bayes, regresión logística o *Logistic Regression* y algoritmos de *deep learning* como las redes neuronales recurrentes o *recurrent neural network, Long-Short Term Memory, Bidirectional Long-Short Term Memory, Gated Recurrent Units, Bidirectional Encoder Representations from Transformers* en el procesamiento de lenguaje natural e inclusive medido a partir de la matriz de confusión dando lugar a mediciones relacionadas con el porcentaje de exactitud del modelo en la detección de verdaderos positivos, precisión, sensitividad y puntuación F1.

Una vez hallado los resultados se observa la tendencia futura de los algoritmos de *machine learning* y *deep learning* como algoritmos de refuerzo en las arquitecturas o de comparación principalmente esto último ante algoritmos emergentes como son los algoritmos metaheurísticos inspirados en la biología indicando con estas nuevas propuestas la falta de estandarización de modelos para su implantación en todos los servicios de mensajería de correo electrónico y la urgencia de llevar a cabo nuevos modelos.

Palabras clave: Machine learning, deep learning, correos electrónicos, ataques de phishing

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Abreviaturas y Acrónimos

AOL	America Online
APWG	Anti-Phishing Working Group
BERT	Bidirectional Encoder Representations from Transformers
BiLSTM	Bidirectional Long-Short Term Memory
BPTT	Backpropagation Through Time
BRRN	Bidireccional Recurrent Neural Network
CERT	Equipo de Respuesta a Incidentes de Ciberseguridad
CCN	Centro Criptológico Nacional
DT	Decission Tree
HTML	HyperText Markup Language
GA	Genetic Algorithm
GOA	Grasshopper Optimization Algorithm
GRU	Gated Recurrent Unit
FOA	Firefly Optimization Algorithm
IA	Inteligencia Artificial
IBM	International Business Machine
INCIBE	Instituto Nacional de Ciberseguridad
IP	Internet Protocol
ISP	Proveedor de Servicios de Internet
kNN	k-Nearest Neighbours
LSTM	Long-Short Term Memory
LR	Logistic Regression
ML	Machine Learning
NB	Naive Bayes
NBM	Multinominal Naive Bayes
NLP	Natural Language Processing

PCA	Principal component analsysis-
PSO	Particle Swarm Optimization
RNN	Recurrent Neural Networks
SGD	Stochastic Gradient Descent
SKFCV	Stratified K-fold Cross Validation
SMS	Short Message Service
SVM	Support Vector Machine
SVR	Support Vector Regression
TF-IDF	Term frequency – Inverse document frequency
RF	Random Forest
URL	Uniform Resource Locator
WOA	Whale Optimization Algorithm

1. Introducción

El auge de los ataques cibernéticos está a la orden del día. Cada vez más actores maliciosos intentan acceder de forma ilícita a la información tanto de individuos como de organizaciones. En consecuencia, numerosas entidades han implementado medidas disuasorias cada vez más elaboradas y desarrolladas con el objetivo de dificultar el acceso no autorizado a sus sistemas y proteger la confidencialidad, integridad y disponibilidad de los datos.

En los últimos años, la ciberseguridad ha alcanzado una mayor relevancia debido a factores como el aumento de la tensión geopolítica mundial Centro Criptológico Nacional - Equipo de Respuesta a Incidentes de Ciberseguridad (CCN-CERT, 2024). Diferentes países han sido objetivo de ataques de forma continuada en sus infraestructuras tecnológicas, especialmente en las operaciones del área de ciberespionaje. Estos ataques intervienen asimismo en procesos electorales viéndose afectados por estrategias políticas en la influencia de resultados. En consecuencia, de estos acontecimientos, este ámbito se ha visto fortalecido en el tiempo con una mayor capacidad en materia de ciberseguridad para afrontar los posibles incidentes que puedan o no materializarse.

Factores como la tendencia del Ransomware as a Service (RaaS) (International Business Machines, (IBM, 2024c) que consiste en la compraventa de *ransomware*, para conseguir beneficios económicos por medio de rescates ofrecidos a la víctima obteniendo la posibilidad de evitar la filtración de información por los extorsionistas y la recuperación del acceso a los mismos. Los atacantes son afiliados del servicio que otorgan a los desarrolladores del *ramsomware* un porcentaje del rescate. Estos servicios no requieren de la posesión de conocimientos técnicos en el campo y posibilita el lanzamiento de ataques con una mayor frecuencia.

Varios de estos grupos criminales que proporcionan un servicio de RaaS reconocidos por las agencias de ciberseguridad son LockBit, BlackBasta, REvil entre otros. “Sin embargo, junto con los incidentes de seguridad donde se usan técnicas de extorsión y donde ambos comparten actores de amenaza, los ataques de *ransomware* abarca el 32% de estos incidentes siendo uno de los líderes de amenazas del 92% de la industria” (Verizon, 2024, p.7).

Adicionalmente con la aparición de la Inteligencia Artificial, en adelante nombrado adicionalmente con el acrónimo IA, ha sido impulsada su aplicación en diversos ámbitos, entre ellos en el reconocimiento y recogida de datos precisos de los territorios de guerra (CCN, 2024) en vista de la gran eficacia que ofrece permitiendo una comprensión más profunda de la situación en zonas bélicas y favoreciendo así a la toma de decisiones con una mayor rapidez y precisión.

Los actores maliciosos utilizan esta nueva herramienta para la generación de ataques más sofisticados, rentabilizando el tiempo para la realización de estos y obteniendo mejores resultados. Debido a su gran popularización surgen nuevos métodos de ingeniería social como el auge de campañas de publicidad para la utilización de esta consiguiendo así un mayor número de víctimas.

Además, según el balance de actividad en materia de ciberseguridad del 2024 publicado por el Instituto Nacional de Ciberseguridad (INCIBE, 2025), a través de su equipo de respuesta a incidentes de ciberseguridad (CERT) gestionó un total de 97.438 incidentes con un incremento del 16,6% con respecto al año 2023. De estos incidentes, el 67,6% (65.808 incidentes) afectaron a los ciudadanos con respecto al 32,4% afectando a entidades (31.450 incidentes) que incluye pymes, micropymes y autónomos. Con relación a la taxonomía destacan aquellos provenientes por *malware,* intrusiones, intentos de acceso no autorizados, tiendas online fraudulentas y por fraude online.

Los incidentes de fraude online componen el 43,2% del total de incidentes (38.000 incidentes) donde el vector más recurrente es aquellos producidos por phishing con un total de 21.571 casos donde destaca los correos con suplantación hacia entidades bancarias y empresas de confianza conocido como *spoofing.*

A nivel global, según el reporte del último cuatrimestre de 2024 aportado por Anti-Phishing Working Group (APWG, 2024) se han detectado 989.123 ataques de phishing siendo un total de 3.763.576 ataques detectados con un descenso del 24,73% en comparación con el año 2023.

Ante estos datos, el objetivo del trabajo consiste en el estudio de métodos y técnicas de detección actuales de la técnica más usada por los atacantes, email-phishing para evitar posibles riesgos en individuos y organizaciones mediante la revisión de la literatura publicada desde el año 2019 hasta el día de hoy observando así el uso frecuente de los algoritmos de *machine learning y deep learning* además de las tendencias futuras en los modelos de detección.

Se organiza en varias partes la sección 2 explica los inicios de la era de los ataques de phishing y su evolución destacando dos ataques que marcaron un antes y un después en el ámbito de la ciberseguridad donde se explicará además de la taxonomía de los correos electrónicos de phishing y las técnicas de detección ante los ataques desde correo electrónico antes del impulso de la IA.

En la sección 3 da lugar a la encuesta que tiene como objetivo de respaldar la veracidad de la problemática indicada y la búsqueda de artículos científicos que ofrezcan soluciones de modelos capaces de detectar y clasificar correctamente grandes volúmenes de correos electrónicos.

En la sección 4 cabe destacar los resultados de la encuesta y de la información encontrada en los artículos científicos con respecto a modelos y algoritmos utilizados para su resolución con el fin de ser estudiados en la sección 5 y en la sección 6 se indican las conclusiones de la elaboración y resultados del trabajo

2. Estado de la cuestión

Phishing también conocido como e-mail phishing o correos de phishing es una técnica de ingeniería social que consiste en la elaboración de correos electrónicos con apariencia legítima de organizaciones e individuos con el fin de obtener información confidencial de la víctima bien sea credenciales, información sensible de la propia víctima e incluso con la instalación de software malicioso en el dispositivo con el fin de monitorizar la información o generar dispositivos *zombies* formando parte de una amplia red para la realización de ataques de denegación de servicio distribuidos (DDoS) entre otros ataques maliciosos.

2.1. Primeros ataques de phishing

Los primeros ataques se remontan a mediados de los años 90 (Cofense, 2023). Si bien no se encuentran datos del primero de ellos debido a la falta de mecanismos

de reporte, hay información registrada sobre el primer incidente desde la masificación de internet en el momento en el que fue cogiendo más fuerza.

America Online, comúnmente conocido como AOL (empresa pionera en la época con sede en Estados Unidos) ofrecía servicios de internet a través de disquetes. Debido a la gran demanda de acceso a internet, la empresa redujo su accesibilidad mediante tarifas. Ante la negativa del coste de la tarifa entre los clientes, ofreció inclusive una versión gratuita de 30 días. Con el fin de evitar el periodo de prueba, varias personas realizaron cambios en los nombres de las versiones gratuitas donde tomaban la identidad de administradores del servicio comenzando así las primeras búsquedas de credenciales por internet para su uso continuo de manera gratuita. Con la popularidad de la red de comunicaciones, comenzaron las primeras tácticas de ataque a través de cuentas de correo electrónico donde los atacantes suplantaron la identidad de administradores del proveedor de servicio de internet (ISP) para la obtención de credenciales tras el inicio sesión por la víctima con el objetivo de conseguir navegar por internet mientras enviaban masificaciones de correos electrónicos maliciosos desde las credenciales obtenidas. En este periodo de tiempo, la concienciación ante estos ataques no existía debido a la falta de registros de este tipo de ataques.

En 2020 (Telefónica, 2018) se produjo uno de los incidentes con las consecuencias más graves a escala mundial. El ataque que originó dicho incidente consistía en un correo electrónico con asunto "I LOVE YOU" y un archivo adjunto que recibe el nombre y extensión "LOVE-LETTER-FOR-YOU.TXT.vbs." Una vez abierto el archivo, ejecutaba el código del virus implementado en el archivo. El virus fue creado para el rastreo de las direcciones de correo de la víctima. Mediante la recopilación de credenciales de manera automática recreaba el correo reenviado a los contactos listados llegando así a propagarse en cuestión de horas desde su origen en Filipinas a nivel mundial. En las últimas declaraciones, Onel de Guzmán afirmó ser el creador del virus diseñado para un proyecto final universitario que debido a un descuido fue difundido fuera de este ámbito causando grandes pérdidas millonarias e incluso llegando a afectar a figuras referentes en el Pentágono, la Reserva Federal y el Parlamento Británico. Este incidente se convirtió en una referencia para la mejora continua y concienciación de la ciberseguridad.

2.2. Evolución de los ataques de phishing

Este tipo de ataques han ido mejorando y cambiando su objetivo paulatinamente en el tiempo. Los primeros intentos como los mencionados anteriormente consistían en la masificación de generación de correos y los primeros ataques de *spoofing* (Osamor et al.,2025) mediante formato de HTML básico en servicios de mensajería disponibles de forma gratuita además del uso de páginas web sencillas siendo fáciles de detectar por su poca complejidad en parte debido a las pocas medidas de seguridad y protocolos de autentificación de los correos electrónicos. Tras el auge de las *botnets,* los filtros de spam implementados no tenían la suficiente capacidad para bloquear estas campañas correctamente debido a la distribución masiva entre diversas IPs para el envío de los correos. Estas técnicas de ataque cambiaron hacia un objetivo determinado como organizaciones e individuos específicos dando lugar al *spear phishing.* Estos ataques consiguieron una mayor probabilidad de éxito comenzando así las primeras búsquedas automatizadas de información pública profesional y personal en redes sociales para la elaboración de correos con información verídica y conociendo previamente el contexto actual de la víctima realizando los ataques en momentos específicos como adquisiciones o cambios de grandes cargos en las organizaciones. Adicionalmente con la llegada de los ataques de ingeniería social donde se persuade a la víctima con manipulación psicológica indicando con urgencia posibles avisos, estafas, renovaciones, las tasas de éxito entre los atacantes aumentaron gracias a la credibilidad de la información empleando mecanismos para la elaboración de ataques con mayor realismo aumentando así la probabilidad de éxito.

2.3. Taxonomía de los correos electrónicos usados en ataques de phishing

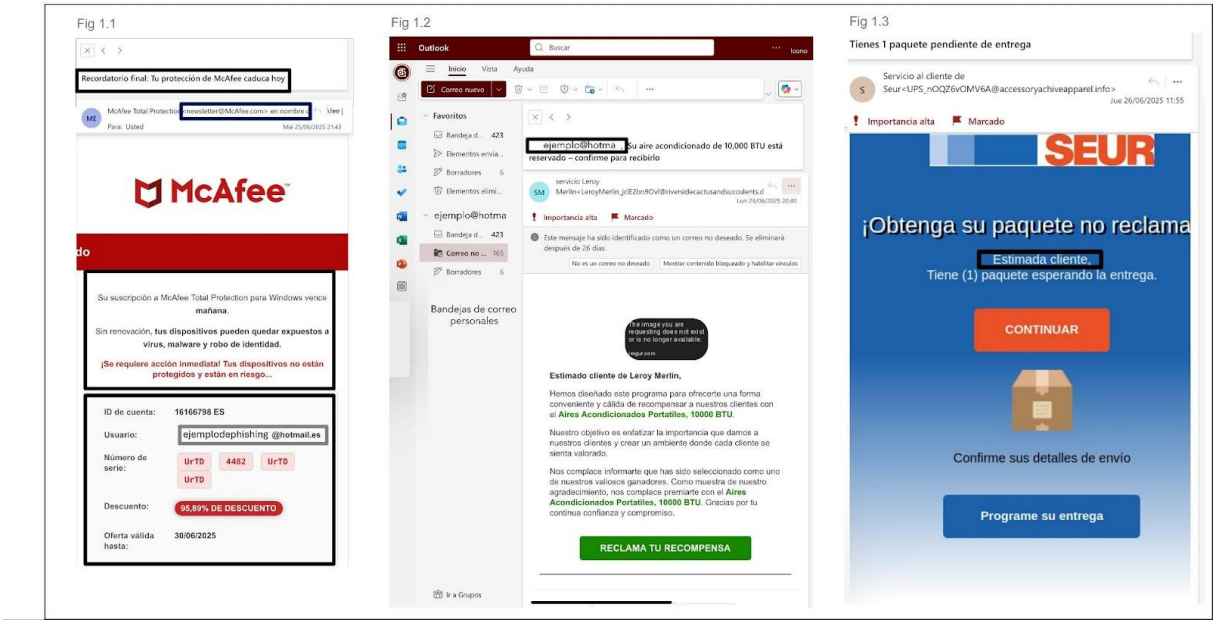


Figura 1 Ejemplos de correos electrónicos maliciosos reales en la actualidad donde asumen ilegítimamente la identidad de varias organizaciones

Con relación a la figura anterior, los correos electrónicos no legítimos usados en los ataques de phishing actuales poseen dicha apariencia con similitudes en la estructura. Con referencia a la figura 1.1, en el encabezado resalta el contenido hacia la víctima ante la adquisición de la protección del antivirus previa a la caducidad de este induciendo un sentimiento de preocupación a la misma. Se observa además la dirección de correo electrónico similar al correo electrónico oficial del remitente con el fin de dar credibilidad a la información indicada. Con respecto al cuerpo del correo reitera la preocupación de la caducidad de la protección mencionando las posibles consecuencias en caso de no obtener la misma elevando la sensación de inquietud. Presenta datos reconocidos por la víctima siendo en este caso la dirección de correo electrónico a fin de lograr una mayor semejanza a los emails electrónicos legítimos y se incluye al final de este el enlace malicioso con el acceso a la página web para realizar la compra. En las figuras 1.2 y 1.3 se visualiza una disposición similar al de la primera figura con información conocida por la víctima en el encabezado y al principio del cuerpo de correo respectivamente consiguiendo así una mayor credibilidad.

En general, los ataques de phishing siguen una estructura similar al mencionado anteriormente con mayor o menor elaboración en las diferentes partes de esta. Se manifiesta en distintos entornos como en las bandejas de entrada de correos corporativos, educativos y en su gran mayoría a correos personales.

Previo a la utilización de la IA como técnica de detección de correos maliciosos en ataques de phishing, se usaban técnicas de análisis por parte del usuario ante posibles indicios tanto del cuerpo como de la cabecera con respecto a la comunicación escrita del remitente indicado anteriormente. El uso de la urgencia por parte del emisor mediante palabras clave como "Urgente" en la expresión y el énfasis del tema además del mal uso de la gramática y la ortografía, coherencia y cohesión con la búsqueda de datos verídicos tanto en el encabezado analizando el nombre del remitente, correo electrónico y asunto como en el cuerpo del mensaje otorgan indicios de un posible ataque. Otras técnicas son la utilización de listas negras *(blacklists)* y listas blancas *(whitelists)* (Kalaharsha & Mehtre, s. f.; Shahrivari et al., s. f.) que recopilan características como direcciones de correo electrónico, IP, URL entre otros con carácter no legítimo y legítimo respectivamente con el fin de evitar futuros ataques gracias al bloqueo previo. En el caso de las *whitelists* tiene como fin permitir que características de confianza introducidas previamente en las listas negras sean levantadas del veto inclusive sin caso previo ante el error tras la incorporación a las listas negras.

Adicionalmente se utilizan técnicas basadas en la detección mediante la heurística siendo estas técnicas una extensión de la anterior que consisten en la implementación de reglas ante tendencias detectadas a través de la comparación de características extraídas previamente con otras utilizadas en casos previos de phishing. Tiene el fin de detectar a tiempo posibles ataques evitando que la amenaza llegue al receptor.

Estas técnicas se siguen usando hoy en día complementando entre sí logrando entornos más seguros.

3. Material y métodos

El trabajo estudia la posible problemática a través de una encuesta a una muestra de la población mundial más pequeña y las soluciones estudiadas por investigadores y expertos en la materia frente a esta adversidad ofreciendo así los puntos de vista desde el problema y las posibles soluciones. A lo largo del trabajo se dividirán las secciones en dos grandes grupos para distinguir de manera más eficaz y rápida ambos puntos de vista.

3.1. Descripción de la encuesta y participantes

En vista de las estadísticas mostradas en la sección 1. Introducción, se ha llevado a cabo un estudio dirigido a una muestra de la población a nivel internacional con datos recogidos en los continentes de Europa, América y África sobre el impacto de los ataques de *phishing* en la vida cotidiana con el objetivo de afirmar las tendencias de esta técnica de ingeniería social en los últimos años en un conjunto de la población cercana a la autora de este trabajo.

Para la elaboración del estudio se ha efectuado una encuesta realizada en Google Forms en lenguaje español (véase Anexo A) con un total de 28 preguntas que recogen anónimamente diferentes factores de interés (rango de edad donde se sitúan los participantes, lugar de residencia en base al continente, nivel del lenguaje español, estudios, dispositivos de comunicación en posesión, grado de detección, frecuencia y rasgos de los ataques de *phishing* recibidos) en el que se incorpora información sobre esta técnica además de concienciar a los participantes con el objetivo de evitar convertirse en futuras víctimas de un ataque a lo largo del cuestionario. Adicionalmente se incluye al final de este, un enlace al foro oficial de consulta de INCIBE (INCIBE, s.f.). con datos de contacto en caso de duda sobre la legitimidad del contenido recibido.

El formulario cuenta con un total de 55 entradas registrándose la última de ellas a fecha de 20 de junio de 2025. Los participantes comprenden edades desde los 11 años hasta más de 65 años. El grupo mayoritario de 25 a 34 años de 45,5% seguido de 30,9% para las edades comprendidas entre los 19 y 24 años y el grupo minoritario encontrándose entre los 11 y 18 años con un 1,8%. En cuanto a las zonas geográficas, se ha hecho distinción entre los diferentes continentes y España

para la evaluación de resultados, los encuestados residentes en España son el grupo mayoritario representando el 85,4% seguido de África representando 7,3% y América del Norte con un 3,6% además de Centroamérica y América del Sur (distinguida de América del Norte debido a la predominancia del idioma inglés y español en las respectivas zonas) con el mismo porcentaje. Con respecto a las competencias sobre el lenguaje español predomina con un 87,3% y 9,1% nivel nativo y competente respectivamente frente a 1,8% representando nivel intermedio. Acerca del nivel de estudios predomina las enseñanzas universitarias representando el 54,5% de la muestra seguido de los estudios de Formación Profesional con 29,1%, Educación Secundaria Obligatoria (10,9%) y Bachillerato (5,5%). Entre los encuestados 25,5% pertenece al ámbito de TI y ciberseguridad (5,4%) frente a 69,1% que se encuentran fuera de estas áreas.

Edad	**Residencia**	**Nivel español**	**Estudios**	**Ámbito**	**Tecnología**
11 y 18 años (1,8%)	España - Europa (83,6%)	Nativo (87,3%)	Enseñanzas universitarias (54,5%)	TI (25,5%)	Uso: • A diario (100%)
19 y 24 años (30,9%)	América del Norte (3,6%)	Competente (9,1%)	Formación Profesional (29,1%)	Ciberseguridad (5,4%)	Número de dispositivos: • Cuatro o más (25,5%)

					• Tres (43,6 %) • Dos (23,6 %) • Uno (7,3%)
25 y 34 años (45,5%)	Centroamérica y América del Sur (3,6%)	Intermedio (1,8%)	Bachillerato (5,5%)	Fuera del ámbito TI y ciberseguridad (69,1%)	<u>Grado de conocimiento en cuanto al uso</u>: • Total (45,4 %) • Alto (41,8 %) • Parcial (12,7 %)
35 y 44 años (5,5%)	África (7,3%)	-	Educación Secundaria Obligatoria (10,9%)	-	-
45 y 54 años	-	-	-	-	-

(7,3%)					
55 y 64 años (5,5%)	-	-	-	-	-
65 años o más (3,6%)	-	-	-		-

Tabla 1 Resumen de las características de los 55 participantes de la encuesta

3.2. Definición y alcance de la investigación

Con el fin de otorgar soluciones óptimas ante esta problemática en estos últimos años, se han abierto numerosas investigaciones para eficientar la detección temprana mediante el uso del aprendizaje automático conocido como *Machine Learning (ML)* y aprendizaje profundo conocido como *Deep Learning (DL)* con el objetivo de evitar posibles incidentes a usuarios y organizaciones.

Este trabajo de investigación analiza y sintetiza de forma estructurada información actualizada de artículos científicos de libre acceso publicados en las bases de datos reconocidas de IEEE Xplore y ScienceDirect (Elsevier) publicados desde el año 2019 hasta el año en curso 2025 con el objetivo de informar a la comunidad académica y científica sobre las últimas tendencias en los modelos de detección y clasificación de correos electrónicos fraudulentos usados en ataques de *phishing*.

Con respecto a la definición del alcance y finalidad del estudio, se han llevado a cabo las siguientes preguntas quedando determinadas en este apartado:

Pregunta 1. ¿Cuáles son los modelos de detección de *Machine Learning* y *Deep Learning* usados en la actualidad en el ámbito de aplicación?

Pregunta 2. ¿Qué soluciones ofrecen con respecto a las técnicas en uso sin aplicación de la Inteligencia Artificial?

Pregunta 3. ¿Existen sinergias entre los diferentes modelos?

Pregunta 4. ¿Cuáles son las tendencias futuras con respecto a esta metodología?

3.2.1. Recopilación de artículos científicos para el estudio

Con el objetivo de responder a las cuestiones planteadas anteriormente se han llevado a cabo los siguientes criterios de búsqueda de los artículos científicos presentados posteriormente y que se encuentran en libre disposición hacia académicos para su consulta mediante el uso y refinamiento de las consultas realizadas en el motor de búsqueda descritas en inglés que gracias a su uso estandarizado y extendido internacionalmente en el campo de la investigación ofrece un mayor grado de conocimiento con respecto a los idiomas locales. Estas consultas contienen las palabras clave *"machine learning"* y *"deep learning"* acotado en el ámbito de aplicación de detección de fraude electrónico junto con los términos extendidos de *"email detection"* y *"phishing email"* descritas por los investigadores en los trabajos en referencia al análisis en los sistemas de identificación de estas prácticas.

Tras la obtención de las publicaciones científicas como resultado de las búsquedas realizadas se ha realizado la reducción del alcance en el rango de años desde 2019 a 2025 para lograr mayor precisión en los resultados con información actualizada y de interés en el marco científico situado con respecto a la IA incluyendo inclusive un filtrado de artículos excluyendo duplicados, no se encuentren dentro del alcance de la investigación, sean acotados a un único escenario, no consisten en la descripción de arquitecturas novedosas planteadas y no queden descritas las métricas utilizadas para su evaluación conforme al rendimiento y grado de mejora con respecto a modelos anteriores.

Asimismo, se ha realizado la búsqueda de artículos científicos en la herramienta OpenAlex (OpenAlex, s.f.) como método de refinamiento y mejora con respecto a la búsqueda manual mediante filtros en las bases de datos obteniendo como resultado de la combinación de ambas búsquedas cuatro artículos científicos de especial interés donde recogen los algoritmos de *machine learning* y *deep learning* utilizados para la investigación.

Consultas	Total	2019 - 2025	Aplicadas condiciones descritas arriba	Artículos científicos elegidos como modelos
(machine learning OR deep learning) AND email detection	8.641	6.322	9	4
(email detection OR phishing email) AND (machine learning OR deep learning)	8.836	6.453		

Tabla 2 Filtrado de artículos científicos empleados en la investigación

Los artículos científicos obtenidos de la aplicación de los filtros y criterios definidos anteriormente describen nuevas arquitecturas propuestas de futuros modelos de detección y clasificación de correo electrónico malicioso en base a algoritmos de *Machine Learning* y *Deep Learning*.

4. Resultados

4.1. Resultados obtenidos de la encuesta

Una vez identificadas las características de los participantes, se recopila respuestas relacionadas con los ataques de *phishing,* el 65,4% de los encuestados identifican el término *"phishing"* con la significación asociada frente a 18,2% que afirman reconocer este término, pero desconocen su significado y el 16,4% que no identifican el mismo.

Como refuerzo adicional, se ha llevado a cabo un ejercicio de *phishing* con escenario en el cual los participantes reciben un correo de petición de cambio de dirección de entrega de un pedido por parte de la empresa de envíos debido a que es errónea dando dos opciones a los participantes sobre cómo deberían actuar ante esta situación, la primera opción consiste en seguir los pasos indicados en el correo y la segunda opción de respuesta libre, obteniéndose los siguientes resultados:

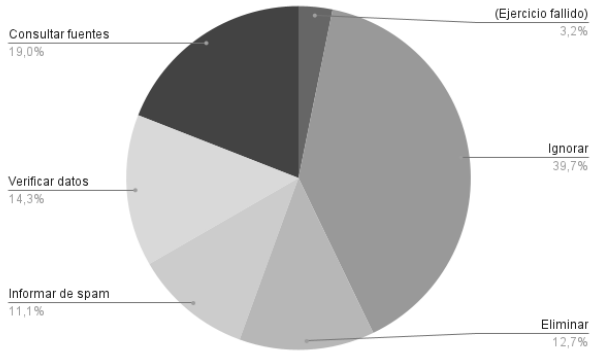


Figura 2 Resultados del ejercicio de phishing

Como se puede observar, el 96,8% de los encuestados superan el ejercicio satisfactoriamente frente al 3,2%.

A continuación, se realiza una serie de cuestiones con respecto a los rasgos de los ataques recibidos por los participantes englobando adicionalmente a los recibidos vía email que reciben el nombre de *phishing* o *e-mail phishing*, otras vías como son los ataques de *smishing* (ataques vía SMS), *vishing* o *voice phishing* (ataques por

llamadas telefónicas) entre otros, los entornos a los que van dirigidos, la frecuencia con la que se reciben y los idiomas empleados para la elaboración de estos ataques.

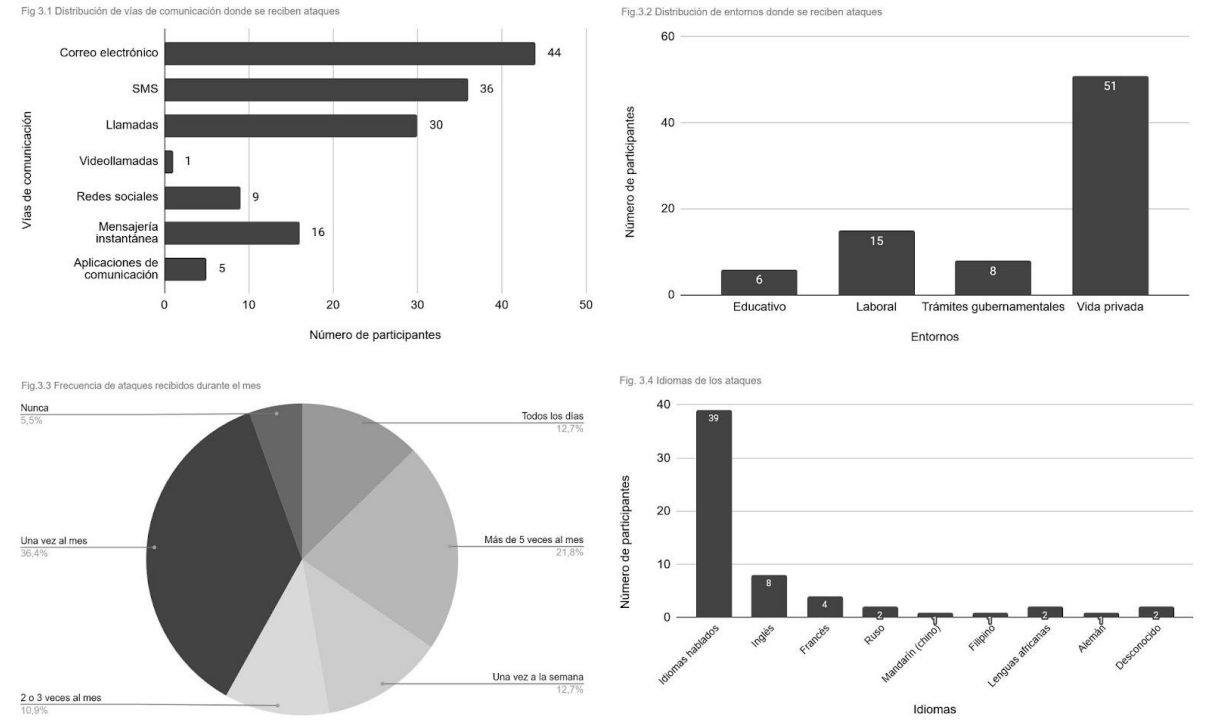


Figura 3 Resumen de las características de los ataques de phishing recibidos por los 55 participantes de la encuesta

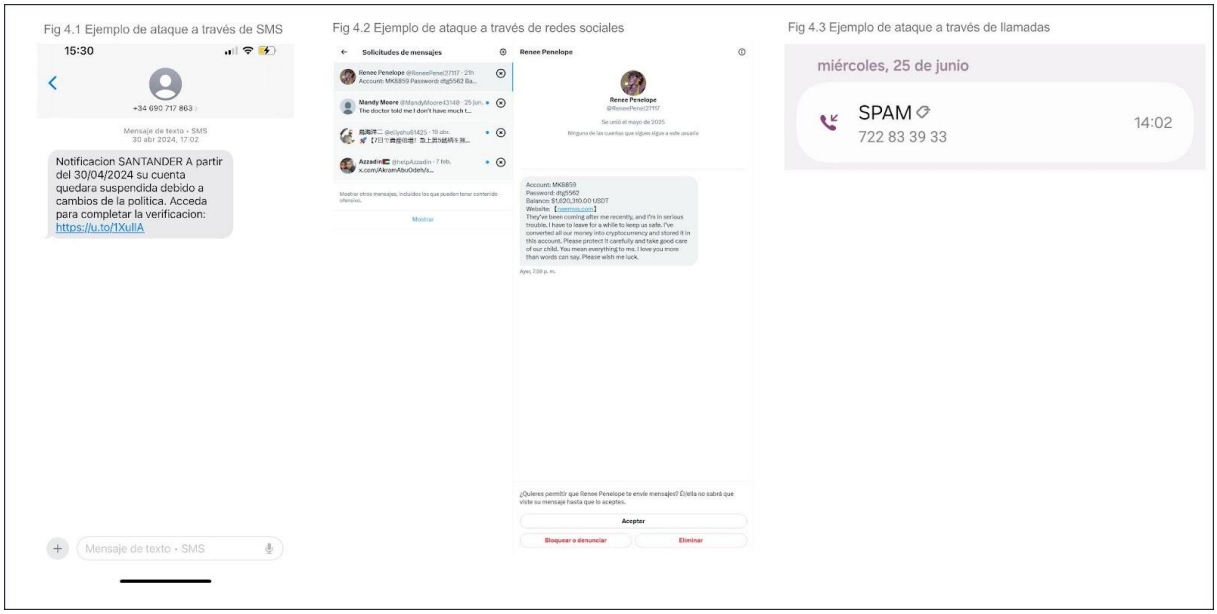


Figura 4 Ejemplos de ataques reales de phishing a través de SMS (4.1), redes sociales (4.2) y llamadas (4.3)

Con respecto a la frecuencia de los ataques recibidos durante el mes, 61,8% de los encuestados indican esta constancia durante los meses del año, 10,9% con intervalos de 2 a 3 meses. Con menor frecuencia siendo momentos puntuales del año (21,8%), una vez (3,6%) y nunca (1,8%).

Con respecto a las vías y entornos donde se reciben este tipo de ataques destaca la vía por correo electrónico como la vía donde se produce el mayor número entre los participantes con un 68,5% seguido de vía SMS y llamadas con 31,5% y 29,6% respectivamente y en menor cantidad por redes sociales con 3,7%, servicios de mensajería instantánea y aplicaciones de comunicación con reuniones virtuales (3,8%) coincidiendo con los resultados presentados en la figura anterior. En entornos el 87,3% afirma recibir la mayoría de estos en entornos privados con respecto al entorno laboral (7,3%), trámites gubernamentales (3,6%) y educativo (1,8%).

En referencia a los idiomas utilizados para el desarrollo de los ataques recibidos por los participantes suelen ser en idiomas hablados por los propios participantes en los diferentes entornos cotidianos, se observa una pequeña tendencia en algunas regiones. Entre los participantes, en España se recibe una gran diversidad de ataques en otros idiomas como son el ruso, inglés, francés, alemán, árabe, mandarín, filipino y lenguas africanas. En África, el francés e idiomas africanos no propios del país son los idiomas no hablados por los participantes con los que se reciben estos ataques. En América del Norte y América del Sur los idiomas de los ataques son propios del país o de los idiomas de los entornos.

Cabe destacar que estos ataques son sencillos de detectar por los participantes (72,7%) donde la tendencia en el tiempo sigue siendo la misma (61,8%) con mayor realismo en cuanto a la comunicación (30,9%) y datos (21,8%). Estos ataques suelen suplantar entidades como bancos, tiendas, entidades gubernamentales e incluso propios empleados de las organizaciones (63,6%) frente a individuos como puede ser desconocidos o conocidos del participante (9,1%).

4.2. Resultados obtenidos de los artículos científicos

4.2.1. Algoritmos de Machine Learning

Con respecto a los modelos de detección y clasificación, los algoritmos de *Machine Learning* en el ámbito de detección de correo malicioso destacan aquellos que requieren de la supervisión del ser humano mediante el uso de etiquetas en los

datos para el reconocimiento de nuevos datos entrantes gracias a la detección de patrones en los datos aprendidos anteriormente bajo el etiquetado realizado. Estos algoritmos se encuentran catalogados bajo el nombre de "algoritmos supervisados" con respecto a los algoritmos no supervisados donde no es necesaria la intervención humana como en los algoritmos descritos previamente debido a que el propio modelo es capaz de reconocer desde un inicio los datos recibidos.

4.2.1.1. Principales algoritmos supervisados utilizados en la detección y clasificación de correos fraudulentos

Los algoritmos supervisados se agrupan en dos tipos de categorías dependiendo de si son diseñados para la clasificación de nuevos datos gracias a los datos de entrenamiento etiquetados por el ser humano perfeccionando de esta manera la correcta distribución de los datos conocidos como "algoritmos de clasificación" (IBM, 2024a) o para detectar la relación entre las variables dependientes e independientes con el fin de determinar predicciones futuras apoyándose en las similitudes respecto a datos anteriores, estos algoritmos reciben el nombre de "algoritmos de regresión" y son utilizados mayoritariamente para la predicción de valores como los ingresos de una empresa en el próximo mes.

En el estudio de correos electrónicos maliciosos usados en los ataques de *phishing*, los investigadores emplean los algoritmos supervisados de clasificación frente a los algoritmos de regresión etiquetando los correos en función de si son correos electrónicos maliciosos que reciben la etiqueta de *"Spam"* o correos electrónicos verídicos que son catalogados frecuentemente bajo la etiqueta de *"Ham"* inclusive se puede clasificar en más clases dependiendo de la tipología de correo, intención del remitente entre otros factores.

Los algoritmos supervisados de clasificación que han sido utilizados en los artículos científicos son las máquinas de vectores de soporte o conocidas por su nombre inglés como *Support Vector Machine (SVM)* (Gibson et al., 2020; IBM, 2023) clasificando los datos mediante la separación lineal en un espacio dimensional N consiguiendo así un hiperplano que separa ambas categorías y son delimitadas por los datos más cercanos al margen. Cabe la posibilidad de separar los datos por un hiperplano no lineal si los datos no permiten dicha división. En este último caso debido a la complejidad para realizar la clasificación los datos mediante el hiperplano no lineal son transformados a través de funciones *kernel* con la finalidad de realizar la separación lineal. Este algoritmo resuelve problemas de predicción continua gracias a la variante de algoritmo de regresión que recibe el

nombre de vectores de soporte o conocido en inglés como *Support Vector Regression (SVR)*. Existe una variante denominada *Stochastic Gradient Descent (SGD)* en inglés que ofrece la posibilidad de trabajar con grandes volúmenes de datos con respecto a los algoritmos SVM, los algoritmos SVM son altamente usados en la detección de ataques de *phishing* gracias a su capacidad de procesamiento del lenguaje natural por su rendimiento satisfactorio con datos altamente dimensionados.

El algoritmo de árbol de decisión o *Decision Tree (DT)* en inglés (Gibson et al., 2020; IBM, s.f._2) es usado tanto en algoritmos supervisados de clasificación y de regresión. Recibe este nombre debido a la estructura jerárquica similar a un árbol formado por un nodo raíz en su estructura inicial, nodos internos o de decisión que clasifican los datos en conjuntos más pequeños y homogéneos contenidos en los nodos finales denominados nodos hoja. Estos nodos ofrecen la información necesaria para la clasificación de los datos en los diferentes grupos debido a la clasificación realizada por las características en los nodos. La desventaja que presenta este tipo de algoritmos es la posibilidad de producirse un sobreajuste u *overfitting* en inglés teniendo en cuenta que los nodos de la estructura condicionan los datos introduciendo conjuntos más pequeños en caso de que la jerarquía aumenta, dificultando el mantenimiento de la homogeneidad de los datos produciéndose conjuntos heterogéneos no válidos. En estos casos, la aplicación de la poda permite la reducción del riesgo ante la posibilidad de manifestar *overfitting* eliminando aquellas ramas cuyas características no sean necesarias para la clasificación incluso logrando resultados más precisos en conjunto con otros árboles de decisión, esta combinación da origen al algoritmo *Random Forest (RF)* (Gibson et al., 2020; IBM, s.f._4) o bosque aleatorio para la creación de árboles de decisión de forma aleatoria, esta creación se debe a la generación de conjuntos de datos o *datasets* con datos aleatorios e inclusive repetidos determinados de manera aleatoria sobre el *dataset* original permitiendo así conjuntos más flexibles con mayor robustez y precisión con respecto a un único árbol de decisión.

Otros algoritmos de supervisión ampliamente utilizados en la detección de correos maliciosos son el algoritmo de k vecinos más cercanos conocido en inglés como *k-Nearest Neighbours (kNN)* (Batra et al., 2021; IBM, s.f_1) utilizado inclusive como algoritmo de regresión. Aplicado en la clasificación, este algoritmo se basa en la asignación del etiquetado del dato entrante en base a la frecuencia de los datos etiquetados cercanos a este dato si uno de los conjuntos de datos etiquetados obtiene una frecuencia superior a la estipulada dependiendo del número de

conjuntos, este dato será etiquetado con la etiqueta perteneciente a la clase correspondiente, el método descrito recibe el nombre de "votación por mayoría". A efectos de determinar el conjunto de datos cercanos al dato a etiquetar es necesario definir previamente la variable k que representa el número de datos etiquetados cercanos al dato a etiquetar que reciben el nombre común de datos "vecinos" cuya finalidad es mediante la medición de la distancia entre el dato a categorizar y sus vecinos determinar la etiqueta con mayor frecuencia a fin de ser asignada.

El algoritmo supervisado de clasificación Naive Bayes (Gibson et al., 2020; IBM; s.f._3) es uno de los algoritmos de clasificación de texto altamente utilizados en la detección de correos maliciosos, su nombre se debe al teorema de Bayes o también conocido como regla de Bayes siendo una de las fórmulas matemáticas más conocidas en el campo de la probabilidad y estadística y se basa en la probabilidad de que se produzca un suceso A habiéndose producido previamente otro suceso B conocido como la probabilidad condicionada $P(A|B)$ tomando conocimiento de la información previa para conocer la probabilidad de que se produzca el suceso B basándose en esta información expresándose de forma reducida como $P(B|A) = \frac{((P(A|B)\cdot P(B))}{P(A)}$. Con respecto al algoritmo de Naïve Bayes las características obtenidas son valiosas de manera equitativa para la determinación del etiquetado de un dato poniendo de ejemplo en el caso de las detecciones de correo electrónico donde la probabilidad de que el correo electrónico sea originario de un posible ataque de *phishing* en base al extracto de las palabras compuestas en la cabecera como "Estimado cliente" con correos electrónicos previos etiquetados como *spam* donde la probabilidad de que el correo recibido se catalogue como *spam* o *ham.* Existen diferentes tipos dependiendo de los valores de las características entre ellos se encuentran *Gaussian Naive Bayes* (en distribuciones gaussianas utilizándose para la localización de la desviación típica y la media de cada clase), *Multinomial Naive Bayes* (en distribuciones nominales altamente usado en procesamiento de texto y en clasificación de correos electrónicos) y *Bernoulli Naive Bayes* (se utiliza en variables de dos valores frecuentemente en valores booleanos).

El algoritmo de regresión logística o "modelo logit" (Hina et al., 2021; IBM, 2025c] conocido en inglés como *logistic regression* a pesar de ser nombrado como regresión no está basado en la predicción de valores si no para el cálculo de probabilidades entre dos conjuntos de datos de entrada con valores categóricos donde se observa la relación entre variables independientes denominadas variables predictoras y

variables de salida con valores entre 0 y 1 pudiendo tratar de variables dependientes, objetivo o respuesta.

Como se ha mencionado previamente los algoritmos de *machine learning* pueden ser supervisados por el ser humano en el entrenamiento del *dataset* con datos etiquetados que ayudan a la comprensión de los algoritmos o al contrario ser no supervisados. En la detección de correos electrónicos destaca el algoritmo no supervisado la agrupación de medias k denominado en inglés como *k-means clusters* que consiste en la agrupación de datos en *clusters* o grupos con el objetivo de refinar la agrupación en datos similares, en la creación de grupos es necesario indicar el punto medio mediante el cálculo de la media o mediana de los datos denominado centroide asignando cada dato de entrada al centroide más cercano, este proceso se realiza en varias iteraciones hasta la estabilización de los centroides.

4.2.2. Algoritmos de Deep Learning

Los algoritmos de *deep learning poseen* una mayor complejidad con respecto a los algoritmos de *machine learning*, son conformados por redes neuronales profundas donde cada neurona es capaz de realizar predicciones en base a los datos de entrada. Su funcionamiento se basa en las redes neuronales biológicas transmitiendo la información de una capa de neuronas a otras mediante los algoritmos de propagación.

4.2.2.1. Principales algoritmos de redes neuronales recurrentes utilizados en la detección y clasificación de correos fraudulentos

En el área de los ataques de *phishing*, los modelos de redes neuronales artificiales los artículos científicos destacan los modelos de redes neuronales recurrentes (Nasreen et al., 2024; IBM,2025d) denominados *recurrent neural network (RNN)* que se difieren de las redes neuronales tradicionales debido a que los datos de entrada se transmiten a la neurona que precede de manera secuencial siendo las entradas y salidas dependientes entre sí guardando el dato obtenido en estados ocultos de cada iteración consiguiendo así capacidad de "memorizar" los datos. Asimismo, son caracterizadas por la compartición de peso que realiza el aprendizaje de la neurona en cada capa de la red neuronal siendo de especial interés siendo ajustados mediante los algoritmos de retropropagación conocido también como *backpropagation* y descenso del gradiente reduciendo el error

provocado en la predicción de salidas generando algoritmos en el tiempo conocidos como *backpropagation through time (BPTT)*.

Existen variantes de las redes neuronales recurrentes con un uso extendido en el ámbito de aplicación de detección de correos maliciosos como las redes neuronales recurrentes bidireccionales denominado en inglés como *bidireccional recurrent neural network (BRRN)* que permite el entrenamiento de datos futuros para predecir posibles salidas conociendo los datos anteriores y actuales. Debido al problema de pérdida de memoria a largo plazo por las modificaciones generadas para reducir los errores que puedan manifestarse en las redes neuronales, se ha creado una variante denominada memoria a corto plazo o conocido en inglés como *Long-Short Term Memory (LSTM)* en el cual sus estados ocultos contienen "celdas de estado" capaces de controlar los flujos de información mediante tres puertas de entrada, salida y olvido con distintas funcionalidades de entrada, salida y eliminación de información respectivamente logrando de esta manera mantener la información a lo largo de la red neuronal otorgando resultados más precisos. Las redes neuronales LSTM son ampliamente extendidos en diferentes escenarios ofreciendo además una variante bidireccional formada por dos arquitecturas LSTM denominada BiLSTM (Nasreen et al., 2024) donde cada capa contiene estados ocultos y celdas de memoria, la funcionalidad de esta variante es a través de cada arquitectura LSTM realizar recorridos hacia adelante y hacia atrás desde sus primeras capas hasta las últimas capas con el fin de preservar la información ofrecida en los datos en cada uno de sus estados evitando así almacenar información anterior de las primeras capas si no reconocer información de posibles datos futuros. Otro modelo de *Deep Learning* utilizado para la resolución del problema de memoria de datos es la arquitectura de unidades recurrentes bloqueadas o *Gated Recurrent Units (GRU)* similar a la arquitectura LSTM mencionada anteriormente con dos puertas que controlan el flujo de información permitiendo el restablecimiento y la actualización de la misma sin recurrir a las celdas de memoria únicamente a los estados ocultos.

Por último, cabe destacar los modelos de *Deep Learning* enfocados al procesamiento del texto que son basados en las arquitecturas de *Transformers* (bloques de codificadores que transforman los datos recibidos en la entrada por datos menos dimensionados y bloques de decodificadores que reconstruyen los datos a su estado original con un bloque de atención utilizado para relacionar los datos de entrada, estas arquitecturas han sido creadas creadas como alternativas de las redes neuronales recurrentes ofreciendo una mayor precisión en los

resultados) concretamente el modelo reconocido por sus siglas en inglés *BERT (Bidirectional Encoder Representations from Transformers)* (Nasreen et al.,2024;Devlin et al.,2018] creado por Google AI, se encuentra formado por un conjunto de capas bidireccionales de codificadores propios de la arquitectura de los *Transformers* para la capacidad de entender textos desde el principio hasta el final y viceversa consiguiendo un mayor entendimiento de los datos de entrada recibidos en las primeras instancias y últimas logrando ser similar a la comprensión del ser humano.

4.2.2.2. Descripción de la arquitectura generalizada para el procesamiento del lenguaje natural

Los algoritmos y modelos mencionados anteriormente tanto de *machine learning* como *deep learning* son una pieza fundamental de la arquitectura para la detección y clasificación de correos electrónicos maliciosos. De forma general, (Batra et al., 2021; Devlin et al., 2018; Gibson et al., 2020; Hina et al., 2021; Nasreen et al.,2024) las arquitecturas propuestas utilizan conjunto de datasets entre los que destacan Enron, LingSpam, SpamAssassin, Kaggle Email Spam y PUA formado por las cabeceras y el cuerpo de correo. Estos datos en formato texto son divididos en palabras denominadas *tokens* almacenados en un array con el fin de detectar la frecuencia con la que son repetidas en los distintos tipos de correo mediante técnicas como TF-IDF y *Bag of Words* una vez preprocesado los datos ayudando así a los modelos en su clasificación. Los *tokens* son convertidos a minúsculas para mantener la consistencia eliminando impurezas tales como *stop-words* que son aquellas palabras que no ofrecen información a analizar cómo pueden ser conectores, signos de puntuación, espacios en blanco e inclusive URLs*,* tras que son transformados de formato texto a formato numérico frecuentemente en vectores reconocibles para los algoritmos mediante técnicas de transformación como word2vec y doc2vec que transforman palabras y documentos a vectores respectivamente. Una vez obtenidos los datos a formato numérico comienza la fase de selección de características, una vez extraídas comienza el entrenamiento de los modelos correspondientes de cada arquitectura para su categorización entre correos electrónicos verídicos o ataques de phishing e inclusive en las clases consideradas. El proceso descrito anteriormente recibe el nombre de procesamiento del lenguaje natural o *natural language process (NLP)*.

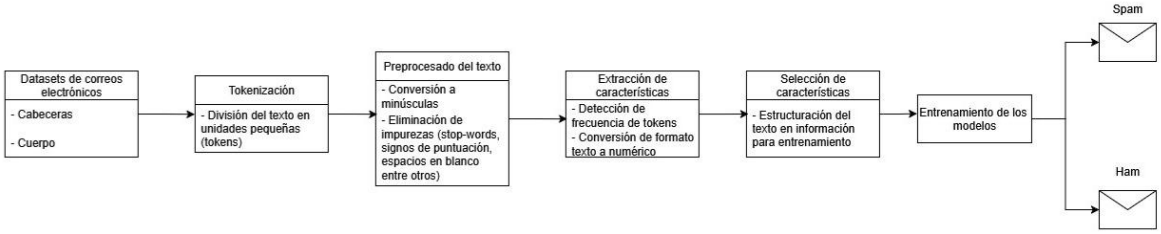


Figura 5 Estructura general del procesamiento del lenguaje natural para la clasificación de correos maliciosos

4.2.3. Metodología de evaluación del rendimiento de los modelos

Con respecto a la evaluación del rendimiento de los modelos de detección principalmente se utiliza la matriz de confusión (IBM,2024b) cuyo objetivo es comparar de manera visual los valores predecidos por los modelos en relación con los valores reales de un conjunto de datos clasificando entre verdaderos positivos (número total de predicciones correctas que realmente son correctas), verdaderos negativos (número total de predicciones incorrectas que realmente son incorrectas), falsos positivos (número total de predicciones incorrectas que realmente son correctas) y falsos negativos (número total de predicciones correctas que realmente son incorrectas). Se distribuyen en la matriz de izquierda a derecha empezando por arriba en el siguiente orden: Verdaderos positivos (cuadro superior izquierda), falsos negativos (cuadro superior derecha), falsos positivos (cuadro inferior izquierda) y verdaderos negativos (cuadro inferior derecha).

Gracias a la matriz de confusión, se consideran métricas derivadas para la evaluación del modelo, las métricas más utilizadas son la exactitud o *accuracy* en inglés que representa la proporción de correos electrónicos correctamente clasificados, la precisión o *precision* en inglés indica la proporción de verdaderos positivos de los correos electrónicos predecidos, la sensibilidad o *recall* muestra la habilidad que tiene el modelo de identificar los correos electrónicos que contiene *phishing* cuanto mayor sea el valor, el modelo identificará este tipo de correos electrónicos como verdaderos positivos, la puntuación F1 o también conocido como *F1 score* en inglés calcula el rendimiento general del modelo cuanto más cercano sea a uno, mayor balance y precisión tendrá el modelo.

$$Accuracy = \frac{VP + VN}{(VP + VN + FP + FN)}$$

$$Precision = \frac{VP}{(VP + FP)}$$

$$Recall = \frac{VP}{(VP + FN)}$$

$$F1\ score = \frac{2 \cdot Precision \cdot Recall}{(Precision + Recall)}$$

4.2.4. Modelos de referencia escogidos para la síntesis

En la tabla descrita a continuación, se recoge los datos destacados sobre los artículos científicos que mayor visión ofrecen sobre los algoritmos descritos anteriormente además de futuros avances en el campo de detección de correos electrónicos:

Autor Año Descripción	Datasets	Software y Hardware	Algoritmos y técnicas	Accuracy	Precision	Recall	F1 Score	Resultado general
(Gibson et al., 2020) Consiste en experimentos usando algoritmos de *machine learning* con algoritmos metaheu	Ling-Spam (2893 correos) PU1(1099 correos) SpamAssasin (6047 correos) PUA (1142 correos) PU2 (721 correos)	Python 3.4 Google Collaboratoy Kaggle Portátil de 8 GB de RAM y procesador AMD Ryzen 3 3200U (2.60	Modelos de ML (*Multinomial Naïve Bayes (MNB)* *Support Vector Machine (Stochastic Gradient Descent (SGD))* *Decission Tree Classifier (DT)*	PSO - Split set 60:40				**Ling Spam** **GA-SGD:** Accuracy: 98.77% Precision: 100% Recall: 94.21% **Enron** **GA-SGD:**
				SGD: 97,37%	SGD: 97,18%	SGD: 93,83%	SGD: 95,37%	
				MNB: 98,41%	MNB: 97,55%	MNB: 97,55%	MNB: 97,80%	
				RF: 91,94%	RF: 94,23%	RF: 74,76%	RF: 79,57%	
				DT: 91,37%	DT: 88,10%	DT: 83,24%	DT: 85,16%	
				MLP: -	MLP: -	MLP: -	MLP: -	

<table>
<tr>
<td rowspan="15">rísticos inspirados en la biología siendo concretamente Particle Swarm Optimization (PSO) y Genetic Algorithm (GA) para la división de los correos electrónicos individuales en “Spam” y “Ham”.</td>
<td rowspan="15">PU3 (4139 correos)
Enron 1-6 Spam (36715correos)</td>
<td rowspan="15">GHz) procesador.</td>
<td rowspan="15">Random Forest Classifier (RF)
Modelos de DL (Perceptrón multicapa)
Algoritmos metaheurísticos inspirado en la biología
((Particle Swarm Optimization (PSO) y Genetic Algorithm (GA)
Módulos: “Count vectorizer” de Shiki-learn para asignar la ocurrencia de cada token
“TfidfTransformer”
Validación de los datos mediante Stratified K-fold Cross Validation (SKFCV)</td>
<td colspan="4">PSO - Split set 70:30</td>
<td rowspan="15">Accuracy = 99.21%
Precision = 98.68%
Recall = 99.54%

<u>SpamAssassin</u>
GA-MNB
Accuracy = 100%
Precisison = 100%
Recall = 100%

<u>PU1</u>
GA-MNB
Accuracy = 99.08%
Precision = 99.31%
Recall = 98.63%

<u>PU2</u>
GA-MNB
Accuracy = 97.89%</td>
</tr>
<tr>
<td>SGD: 97,54%</td>
<td>SGD: 97,24%</td>
<td>SGD: 95,20%</td>
<td>SGD: 96,21%</td>
</tr>
<tr>
<td>MNB: 98,38%</td>
<td>MNB: 97,82%</td>
<td>MNB: 97,31%</td>
<td>MNB: 97,51%</td>
</tr>
<tr>
<td>RF: 91,37%</td>
<td>RF: 96,95%</td>
<td>RF: 70,36%</td>
<td>RF: 77,67%</td>
</tr>
<tr>
<td>DT: 91,65%</td>
<td>DT: 87,81%</td>
<td>DT: 85,96%</td>
<td>DT: 86,64%</td>
</tr>
<tr>
<td>MLP: -</td>
<td>MLP: -</td>
<td>MLP: -</td>
<td>MLP: -</td>
</tr>
<tr>
<td colspan="4">PSO - Split set 75:25</td>
</tr>
<tr>
<td>SGD: 97,21%</td>
<td>SGD: 97,11%</td>
<td>SGD: 93,11%</td>
<td>SGD: 94,79%</td>
</tr>
<tr>
<td>MNB: 98,43%</td>
<td>MNB: 97,73%</td>
<td>MNB: 97,24%</td>
<td>MNB: 97,60%</td>
</tr>
<tr>
<td>RF: 91,62%</td>
<td>RF: 96,58%</td>
<td>RF: 92,51%</td>
<td>RF: 77,88%</td>
</tr>
<tr>
<td>DT: 92,29%</td>
<td>DT: 88,27%</td>
<td>DT: 88,04%</td>
<td>DT: 87,48%</td>
</tr>
<tr>
<td>MLP: 97,11%</td>
<td>MLP: -</td>
<td>MLP: -</td>
<td>MLP: -</td>
</tr>
<tr>
<td colspan="4">PSO - Split set 80:20</td>
</tr>
<tr>
<td>SGD: 97,64%</td>
<td>SGD: 96,80%</td>
<td>SGD: 95,59%</td>
<td>SGD: 95,78%</td>
</tr>
<tr>
<td>MNB: 98,47%</td>
<td>MNB: 97,23%</td>
<td>MNB: 97,86%</td>
<td>MNB: 97,54%</td>
</tr>
</table>

				RF: 90,81%	RF: 96,11%	RF: 66,49%	RF: 74,79%	Precision = 90.62% Recall = 100% **PU3** **GA-MNB** Accuracy = 97.04% Precision = 98.61% Recall = 96.74% **PUA** **GA-MNB** Accuracy = 97.81% Precision = 97.76% Recall = 96.46%
				DT: 92,28%	DT: 88,07%	DT: 86,45%	DT: 86,71%	
				MLP: 97,18%	MLP: -	MLP: -	MLP: -	
				GA - Split set 60:40				
				SGD: 96,92%	SGD: 96,59%	SGD: 94,13%	SGD: 95,27%	
				MNB: 98,27%	MNB: 97,38%	MNB: 84,63%	MNB: 97,32%	
				RF: 93,11%	RF: 96,51%	RF: 77,16%	RF: 83,13%	
				DT: 93,50%	DT: 90,02%	DT: 86,96%	DT: 8842%	
				MLP: -	MLP: -	MLP: -	MLP: -	
				GA - Split set 70:30				
				SGD: 97,37%	SGD: 96,98%	SGD: 94,52%	SGD: 95,61%	
				MNB: 98,43%	MNB: 97,76%	MNB: 97,61%	MNB: 97,64%	
				RF: 93,69%	RF: 97,00%	RF: 80,11%	RF: 85,83%	
				DT: 92,76%	DT: 89,34%	DT: 87,48%	DT: 88,25%	
				MLP: -	MLP: -	MLP: -	MLP: -	
				GA - Split set 75:25				

				SGD: 97,39%	SGD: 97,48%	SGD: 94,03%	SGD: 95,68%	
				MNB: 98,40%	MNB: 98,09%	MNB: 97,11%	MNB: 97,57%	
				RF: 93,72%	RF: 97,25%	RF: 80,43%	RF: 85,73%	
				DT: 93,27%	DT: 90,68%	DT: 87,55%	DT: 88,72%	
				MLP: 97,02%	MLP: -	MLP: -	MLP: -	
				GA - Split set 80:20				
				SGD: 97,77%	SGD: 97,61%	SGD: 95,97%	SGD: 96,71%	
				MNB: 98,47%	MNB: 98,01%	MNB: 97,59%	MNB: 97,67%	
				RF: 94,36%	RF: 97,79%	RF: 81,74%	RF: 87,42%	
				DT: 93,42%	DT: 91,07%	DT: 88,51%	DT: 89,54%	
				MLP: 96,39%	MLP: -	MLP: -	MLP: -	
(Batra et al., 2021) Nuevo método de clasificación de correos electrónicos fraudule	UCI Machine Learning Repository - Hopkins et al., 1999)	Matlab 2018a Portátil Dell Inspiron 35567 Intel(R) Core (TM) i3-6006U	Modelos de *machine learning (k-Nearest Neighbours (kNN))* Algoritmos metaheurísticos inspirados en la	GWO: 65,64%	GWO: 62,31%	GWO: 100%	GWO: 73,7%	Resultados indicados en las columnas de medición.
				CSO: 65.95%	CSO: 62,5%	CSO: 100%	CSO: 73,86%	
				FOA: 65.35%	FOA: 62,16%	FOA: 100%	FOA: 73,55%	
				GOA: 74%	GOA: 67,39%	GOA: 35,44%	GOA: 37,15%	

ntos y legítimos en base al uso de técnicas de optimización inspiradas en la biología.		CPU @ 2.00 GHz, Procesador, 4 GB de RAM 64-bit Operating System, and HDD	biología (*Grey Wolf Optimization (GWO), Firefly Optimization Algorithm (FOA), Chicken Swarm Optimization (CSO), Grasshopper Optimization Algorithm (GOA), Whale Optimization Algorithm (WOA*)	WOA: 70.58%	WOA: 69,83%	WOA: 94,34%	WOA: 74,46%	
(Hina et al.,2021) Nueva arquitectura de clasificación de correos electrónicos en cuatro clases catalogadas como normales, fraudulentas, amenazantes y	Enron Corpora dataset (correos electrónicos normales: 9001), Phished corpora (correos electrónicos fraudulentos: 9001) dataset de los propios autores sobre sus propios	Python Google Collaboratoy	Modelos de *Deep Learning* (*Long-Short Term Memory (LSTM), Gated Recurrent Units (GRU))* Modelos de *Machine Learning (Logistic Regression (LR), Support Vector*	LR: 0.9191%	LR: 0.96%	LR: 0.68%	LR: 0.80%	Resultados indicados en las columnas de medición.
				SVM: 0.9001%	SVM: 0.91%	SVM: 0.90%	SVM: 0.89%	
				SGD: 0.8763%	SGD: 0.89%	SGD: 0.85%	SGD: 0.86%	
				NB: 0.9045%	NB: 0.91%	NB: 0.90%	NB: 0.90%	
				RF: 0.9054%	RF: 0.92%	RF: 0.91%	RF: 0.90%	
				LSTM+ConvID: 0.9316%	LSTM+ConvID: 0.93%	LSTM+ConvID: 0.93%	LSTM+ConvID: 0.93%	

sospechosas, este nuevo sistema se denomina SeFACED.	correos y correo de Twitter (correos electrónicos sospechosos y amenazantes: 5287 y 9138 respectivamente)		*Machine (SVM), Stochastic Gradient Descent (SGD),* *Naive Bayes (NB), Random Forest (RF))* Extracción de características: TF-IDF, Bag of Words, word2vector y word embedding	Stack of LSTM: 0.9391%	Stack of LSTM: 0.94%	Stack of LSTM: 0.94%	Stack of LSTM: 0.94%	
				LSTM +GRU: 0.9500%	LSTM +GRU: 0.95%	LSTM +GRU: 0.95%	LSTM +GRU: 0.95%	
(Nasreen et al., 2024) Nueva arquitectura de detección de correos electrónicos fraudulentos que mejora la capacidad de seleccion	Ling spam (2894 correos)	Python 3.7.6 Windows 8th Gen Intel core i7 12 GB	Selección de características *(Principal component anal-ysis (PCA), Grey Wolf Optimization (GWO))* Modelos de *deep learning (Long-Short Term*	CNN: 92 %	CNN:95 %	CNN: 92 %	CNN: 91 %	**Lingspam** **Modelo propuesto:** Accuracy: 99.14%
				LSTM: 96%	LSTM: 94 %	LSTM: 96.5 %	LSTM: 94 %	
				TD-IDF-RF: 93.89 %	TD-IDF-RF: 94.69 %	TD-IDF-RF: 96.85 %	TD-IDF-RF: 95.72 %	
				GWO-BERT-CNN: 97.28 %	GWO-BERT-CNN: 94.16 %	GWO-BERT-CNN: 97.28 %	GWO-BERT-CNN: 96.11 %	

ar las características relevantes de un dataset original.			*Memory (LSTM), Bidirectional Long-Short Term Memory (BiLSTM), convolutional neural network (CNN), Bidirectional Encoder Representations from Transformers (BERT))* Comparación con modelos de machine learning (*Random Forest (RF)*)	GWO-BERT-LSTM: 98.80 %	GWO-BERT-LSTM: 97.65 %	GWO-BERT-LSTM: 97.24 %	GWO-BERT-LSTM: 96.43 %	
				GWO-BERT-biLSTM: 99.14 %	GWO-BERT-biLSTM: 99.89 %	GWO-BERT-biLSTM: 94.73 %	GWO-BERT-biLSTM: 97.29 %	

Tabla 3 Resumen con los datos más relevantes de los estudios a destacar (Batra et al., 2021; Devlin et al., 2018; Gibson et al., 2020; Hina et al., 2021; Nasreen et al.,2024)

5. Discusión

5.1. Puntos principales sobre la encuesta

Con respecto a la elaboración de la encuesta se planteó introducir rangos de edad más pequeños para añadir además al sector de la población más joven, sin embargo, esta idea fue descartada debido a que, en los rangos de edades descritos, los participantes no reconocerían los ataques de *phishing* inclusive no utilizarían de manera asidua los servicios de mensajería dificultando así la posibilidad de recibir información relativa al contexto preguntado. En cuanto a la expansión del alcance de la población fue llevada a cabo para observar cómo influye los ataques de *phishing* en las distintas zonas geográficas asimismo se pregunta sobre el grado de habilidad en el manejo de dispositivos siendo una pregunta para identificar posibles relaciones con respecto a los ataques de *phishing* debido a la hipótesis correlativa entre la experiencia en el uso de dispositivos y el reconocimiento de un ataque. Asimismo, se vio la necesidad de aportar esta iniciativa a una muestra de la población aún más grande para contrastar con mayor enfoque dichos resultados.

5.1.1. Conclusiones planteadas tras la vista hacia los resultados

Con relación a las preguntas se identifica con respecto al conocimiento del término de *phishing* una tendencia con relación a la edad y la familiaridad en el ámbito tecnológico pudiendo explicar el desconocimiento del concepto en edades más tempranas por la falta de conocimiento en el campo y las más avanzadas al asentamiento y la rápida evolución tecnológica en la actualidad junto con la posibilidad del poco grado de conocimiento en la misma.

Estudiando la causa del porcentaje minoritario sobre el ejercicio de *phishing*, se detecta el desconocimiento de este tipo de correos (exceptuando un caso) y la relación con la definición del término que resulta desconocido además de la no pertenencia en el campo tecnológico clarificando la toma de decisión de optar por la opción 1 frente a la opción 2. Adicionalmente se identifica la falta de información en cuanto a medidas a tomar ante un ataque de esta índole predominando la opción de ignorar el correo frente a informar de spam añadiendo a continuación información de interés a los encuestados.

Con relación a la frecuencia mensual, según los datos recogidos a lo largo de la encuesta se estima que los participantes que reciben una menor frecuencia de estos ataques pueden deberse a que hay una tendencia mayoritaria con respecto al ejercicio de *phishing* entre el grupo de encuestados que hasta el momento no habían recibido un correo como el adjuntado en el ejercicio sin embargo si han recibido ataques por correo y con tendencia mayoritaria a detectar si el ataque recibido es fraudulento. Comparando las características obtenidas, indica como hipótesis la posibilidad de poca frecuencia de consulta a los entornos por parte de este grupo generando un mayor desconocimiento del momento en el que se produce el ataque observándose con ello una menor frecuencia con respecto al resto de grupos.

Siguiendo los resultados descritos anteriormente induciendo a la tendencia de ataques por correo electrónico, SMS y llamadas en entornos privados, esto puede ser debido a la filtración de datos introducidos en servicios donde hayan sido atacados posteriormente y recopilado por los propios atacantes impulsando campañas de ataques con los datos obtenidos.

Con respecto al idioma de los ataques se llega a la conclusión de que los atacantes realizan sus actividades en los idiomas en los que son desarrollados, exceptuando América del Norte y América del Sur sin embargo cabe destacar la posibilidad de la menor participación en estas regiones, en general se observa una mayor tendencia situar estos mismos con los idiomas hablados en la región para una mayor probabilidad de que la actividad efectuada sea satisfactoria.

En definitiva, los resultados de la encuesta reflejan con bastante verosimilitud el panorama actual otorgando así una mayor veracidad a los hechos y a las soluciones necesarias para resolver dicha problemática.

5.2. Puntos principales sobre los modelos

En los resultados descritos anteriormente limitados a libre acceso debido a la falta de suscripción en estas bases de datos, se observa diferentes algoritmos de clasificación tanto de *machine learning* como de *deep learning* incluso nuevos algoritmos metaheurísticos inspirados en la biología junto con novedosos *datasets* entre los que destacan LingSpam y Ernon entre otros muchos, esto causa una complejidad a la hora de analizar los resultados obtenidos con cada una de las novedosas arquitecturas ya que no se utilizan los mismos datos ni los mismos modelos o arquitecturas de detección y clasificación sin embargo gracias a las

mediciones realizadas podemos identificar que algoritmos consiguen una mayor exactitud a la hora de detectar verdaderos positivos.

Los modelos híbridos de algoritmos metaheurísticos inspirados en la biología y algoritmos de *machine learning* o *deep learning* destacan consiguiendo mejores resultados que las arquitecturas basadas en un único tipo de algoritmo.

Como se ha podido observar existen numerosos modelos en el campo de *machine learning* y *deep learning* siendo de especial relevancia varios de estos modelos en el procesamiento del lenguaje natural conllevando así a la utilización en la detección y clasificación de los correos electrónicos maliciosos e inclusive en la sinergía con otros tipos de algoritmos como los algoritmos metaheurísticos inspirados en la biología consiguiendo así una mayor exactitud en la clasificación de diferentes clases de los correos electrónicos.

Debido al surgimiento de nuevos algoritmos se identifica la falta de estandarización en los artículos científicos de la resolución de clasificación de algoritmos siendo de especial interés para una evolución guiada en los diferentes servicios de mensajería sin embargo se observa la necesidad de resolver esta problemática con respecto a años anteriores.

A continuación, se plantean las preguntas mencionadas en el punto 3. Resultados con las respuestas encontradas gracias a los artículos científicos mencionados anteriormente (Batra et al., 2021; Devlin et al., 2018; Gibson et al., 2020; Hina et al., 2021; Nasreen et al.,2024)) pudiendo destacar la efectividad de los algoritmos y la tendencia futura de los mismos.

5.2.1. Respuestas a las preguntas planteadas

Pregunta 1. ¿Cuáles son los modelos de detección de *Machine Learning* y *Deep Learning* usados en la actualidad en el ámbito de aplicación?

Los modelos de detección de *Machine Learning* y *Deep Learning* son los mencionados en el punto 4. Resultados siendo los más destacados en los modelos de *Machine Learning, Support Vector Machine (SVM)*, *Logistic Regression (LR)*, *Stochastic Gradient Descent (SGD)*, *Naive Bayes (NB)*, *Random Forest (RF)* y en los modelos de *Deep Learning* destacan *Long-Short Term Memory (LSTM)*, *Gated Recurrent Units (GRU) y Bidirectional Encoder Representations from Transformers (BERT)* obteniéndose mejores resultados según el apartado anterior en los modelos de *Deep Learning* esto se debe gracias a su capacidad de aprendizaje

autónomo con respecto a los algoritmos de *machine learning* y su capacidad para el procesamiento de texto gracias a la relación de los diferentes datos en cada una de las capas con respecto a posibles datos pasados y futuros o algoritmos como *Long-Short Term Memory (LSTM)* capaces de guardar en estados ocultos información de los datos recibidos siendo esta ventaja de utilidad a la hora de detectar y clasificar correos electrónicos sin embargo está más extendido el uso hasta hace unos años de los algoritmos de *machine learning* debido principalmente a su coste computacional bajo con respecto a los algoritmos de *deep learning* sin embargo últimamente se opta por el uso de modelos de *deep learning* en especial relacionados con algoritmo BERT debido a la similitud a la compresión humana gracias a su arquitectura con respecto al resto de algoritmos.

Pregunta 2. ¿Qué soluciones ofrecen con respecto a las técnicas en uso sin aplicación de la Inteligencia Artificial?

Las soluciones que ofrecen este tipo de algoritmos con respecto a la técnicas donde no se usan la Inteligencia Artificial es en definitiva el procesamiento del lenguaje del texto con la capacidad para detectar posibles verdaderos positivos gracias a las relaciones entre los valores y los patrones hallados en los conjuntos de entrenamiento haciendo que sea una solución eficaz en la detección de *phishing*, no obstante cabe destacar que este tipo de modelos son muy costosos y requieren de suficiente entrenamiento para su correcto funcionamiento es por ello que a día de hoy se sigue usando en primer lugar para descarte rápido de *phishing* las técnicas sin requerimiento de IA y consecutivamente los modelos basados en Inteligencia Artificial.

Pregunta 3. ¿Existen sinergias entre los diferentes modelos?

Existen sinergias entre los modelos basados en *machine learning* y *deep learning* con otros tipos de algoritmos que se mencionan a continuación consiguiendo arquitecturas híbridas donde se obtiene una mayor precisión en la clasificación de correos electrónicos con *datasets* muy amplios inclusive con la posibilidad de añadir más clases en la categorización sin embargo se usan con frecuencia para realizar comparaciones entre modelos para la identificación en cuanto al grado de exactitud sobre la clasificación y detección de *phishing* en estos modelos.

Pregunta 4. ¿Cuáles son las tendencias futuras con respecto a esta metodología?

Sobre las tendencias futuras cabe destacar el uso de algoritmos metaheurísticos inspirados en la biología como son *Grey Wolf Optimization (GWO), Firefly Optimization Algorithm (FOA), Chicken Swarm Optimization (CSO), Grasshopper*

Optimization Algorithm (GOA), Whale Optimization Algorithm (WOA) mencionados en anteriormente que se basan en los comportamientos de los lobos, luciérnagas, gallinas, saltamontes y ballenas respectivamente en la naturaleza, estos algoritmos resuelven problemas complejos gracias a la similitud con los procesos realizados por los organismos en la naturaleza consiguiendo un mayor reconocimiento y popularidad a la hora de resolver los problemas de clasificación de correo electrónico.

En resumen, los algoritmos vistos de *machine learning* y *deep learning* servirán como algoritmos de comparación y refuerzo de los algoritmos metaheurísticos inspirados en la biología ofreciendo así una mayor amplitud y precisión durante la evolutiva de los ataques de phishing en correo electrónico.

6. Conclusiones

En definitiva, los resultados obtenidos en el estudio sobre una muestra pequeña de la población global afirman las tendencias globales y regionales respecto al panorama de la ciberseguridad y de los ataques de *phishing* siendo parte de un problema generalizado que afecta a todos los grupos de edad descritos a nivel mundial.

Ante esta problemática que ha ido emergiendo a lo largo de los años se observa una tendencia en la complejidad de los algoritmos consiguiendo así resolver escenarios más complejos donde se muestra un mayor interés con respecto a los algoritmos de *machine learning* y *deep learning* utilizados para la comparativa o refuerzo de la arquitectura sin embargo se destaca además los algoritmos de *deep learning* sobre *machine learning* donde se indica una mayor precisión a la hora de clasificar los correos electrónicos originarios de los *datasets*. Este documento tiene como objetivo evidenciar la problemática actual en base a datos del año en curso 2025 y sintetizar los recursos actuales para su solución como base para investigaciones futuras.

Este trabajo cumple con el impacto social y ambiental descrito en los objetivos de desarrollo sostenible conocido por las siglas ODS en ODS 4. Educación de calidad, ODS 8. Trabajo creciente y crecimiento económico, ODS 9. Industria, innovación e infraestructura y ODS. 16 Paz, justicia e instituciones sólidas.

Referencias

Anti-Phishing Working Group (s.f.) *Phishing Activity Trends Reports* https://apwg.org/trendsreports/

Batra, J., Jain, R., Tikkiwal, V. A., & Chakraborty, A. (2021). A comprehensive study of spam detection in e-mails using bio-inspired optimization techniques. International Journal of Information Management Data Insights, 1(1), 100006. https://doi.org/10.1016/J.JJIMEI.2020.100006

Centro Criptológico Nacional - Equipo de Respuesta ante Incidentes de Ciberseguridad (2024). *Ciberamenazas y tendencias* (Edición 2024). https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html.

Cofense (2023, Junio) *The History of Phishing Attacks* https://cofense.com/knowledge-center/history-of-phishing/

Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2018). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. NAACL HLT 2019 - 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies - Proceedings of the Conference, 1, 4171-4186. https://doi.org/10.48550/arXiv.1810.04805

Gibson, S., Issac, B., Zhang, L., & Jacob, S. M. (2020). Detecting spam email with machine learning optimized with bio-inspired metaheuristic algorithms. IEEE Access, 8, 187914-187932. https://doi.org/10.1109/ACCESS.2020.3030751

Google Forms (s.f) https://docs.google.com/forms/u/0/

Hina, M., Ali, M., Javed, A. R., Ghabban, F., Khan, L. A., & Jalil, Z. (2021). SeFACED: Semantic-Based Forensic Analysis and Classification of E-Mail Data Using Deep Learning. IEEE Access, 9, 98398-98411. https://doi.org/10.1109/ACCESS.2021.3095730

International Business Machines (IBM). (2023, Diciembre). *¿Qué son las máquinas de vectores de soporte?* https://www.ibm.com/es-es/think/topics/support-vector-machine

International Business Machines (2024a, Octubre). *What is classification in machine learning?* https://www.ibm.com/think/topics/classification-machine-learning

International Business Machines (IBM). (2024b, Enero) *¿Qué es una matriz de confusión?*. https://www.ibm.com/es-es/think/topics/confusion-matrix

International Business Machines (2024c, Septiembre). *¿Qué es el ransomware como servicio (RaaS).* https://www.ibm.com/es-es/think/topics/ransomware-as-a-service

International Business Machines (IBM). (2024d, Octubre). *¿Qué es una red neuronal recurrente (RNN)?* https://www.ibm.com/es-es/think/topics/recurrent-neural-networks

International Business Machines (IBM). (2025, Mayo). *What is logistic regression?* https://www.ibm.com/think/topics/logistic-regression

International Business Machines (IBM). (s.f._1). *¿Qué es el algoritmo de k vecinos más cercanos?* https://www.ibm.com/es-es/think/topics/knn

International Business Machines (IBM). (s.f._2). *¿Qué es un árbol de decisión?* https://www.ibm.com/es-es/think/topics/decision-trees

International Business Machines (IBM). (s.f._3). *What are Naïve Bayes classifiers?* https://www.ibm.com/think/topics/naive-bayes

International Business Machines (IBM). (s.f._4). *What is random forest?* https://www.ibm.com/think/topics/random-forest

Instituto Nacional de Ciberseguridad (2025, Marzo) *INCIBE presenta su balance de ciberseguridad 2024 con más de 97.000 incidentes gestionados.* https://www.incibe.es/incibe/sala-de-prensa/incibe-presenta-su-balance-de-ciberseguridad-2024-con-mas-de-97000-incidentes

Instituto Nacional de Ciberseguridad (s.f.) *FAQ Tu Ayuda en Ciberseguridad* https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/faq

Kalaharsha, P., & Mehtre, B. M. (s. f.). Detecting Phishing Sites-An Overview.

Nasreen, G., Murad Khan, M., Younus, M., Zafar, B., & Kashif Hanif, M. (2024). Email spam detection by deep learning models using novel feature selection technique and BERT. Egyptian Informatics Journal, 26, 100473. https://doi.org/10.1016/J.EIJ.2024.100473.

OpenAlex (s.f) https://openalex.org/

Osamor, J., Ashawa, M., Shahrabi, A., Philip, A., & Iwendi, C. (2025). The Evolution of Phishing and Future Directions: A Review. International Conference on Cyber Warfare and Security, 20(1), 361–368. https://doi.org/10.34190/ICCWS.20.1.3366

Shahrivari, V., Darabi, M. M., & Izadi, M. (s. f.). Phishing Detection Using Machine Learning Techniques.

Telefónica (2018) *I LOVE YOU: el virus más famoso del mundo ya es mayor de edad* https://blogthinkbig.com/virus-informatico-i-love-you

Verizon (2024). 2024 Data Breach Investigations *Report* *https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf*

Anexos

En este anexo se indican las preguntas realizadas en la encuesta, así como las respuestas recogidas anónimamente.

A.1 Phishing: ¿Cuánto sabemos y qué tan cerca está de nuestras vidas?

Esta encuesta tiene como objetivo recoger estadísticas en base al conocimiento y vivencias que hayan tenido las personas que la completen. Servirá de información para indicar en el trabajo final de carrera que estoy realizando donde refleja la situación actual y la problemática que vivimos en estos años, cada vez más candente. ¡No te preocupes por las preguntas, las respuestas **se recogerán anónimamente y se tarda 5 minutos aproximadamente en rellenar la encuesta** que servirá para aprender entre todos (yo incluida) sobre este tema así que no te dé miedo a responder, muchas gracias por participar!

* Indica que la pregunta es obligatoria

Pregunta 1. ¿En qué rango de edad te encuentras? *

- Entre 11 y 18 años
- Entre 19 y 24 años
- Entre 25 y 34 años
- Entre 35 y 44 años
- Entre 45 y 54 años
- Entre 55 y 64 años
- Entre 65 años o más

Pregunta 2. ¿Vives en España o en qué zona geográfica **resides actualmente**? *

- España (Europa)
- Europa
- América del Norte
- Centroamérica y América del Sur
- África
- Asia
- Oceanía

Comentario aclaratorio al trabajo: Asia y Oceanía fueron descartadas en el estudio debido a la falta de participantes.

Pregunta 3. ¿Qué nivel de español consideras que tienes?

Esta encuesta está dirigida a personas que tienen al menos alguna parte de su entorno comunicación en español *

- Soy nativo (Lengua materna)
- Competente (Buen nivel de fluidez y comprensión amplia del lenguaje español)
- Intermedio (Domino perfectamente la lectura y escritura)
- Básico (Algunas frases simples y algo de vocabulario)
- Principiante

Si has contestado a la pregunta anterior con las opciones **"Principiante" y "Básico"** y sientes que puede resultar difícil rellenar esta encuesta puedes pedir ayuda a una persona de confianza para poder rellenarlo sin ningún problema.

¡Tus respuestas son bastante valiosas para este proyecto!

Pregunta 4. ¿Cuáles son los últimos estudios que posees o que estás cursando actualmente?

Si estos estudios no corresponden con los que cursaste en su día debido a los cambios producidos o no eres de España te recomiendo buscar por internet la equivalencia en el año en que los cursaste o en tu país de origen. *

- No tengo estudios
- Educación Primaria
- Educación Secundaria Obligatoria (ESO)
- Bachillerato
- Formación Profesional (FP)
- Enseñanzas universitarias

Pregunta 5. ¿Cursas estudios o trabajas en el ámbito de TI/OT/ciberseguridad?

Si estás estudiando y trabajando a la vez en estos sectores indica la respuesta con respecto a tu trabajo actual. *

- Sí, curso estudios/trabajos relacionados con las TI
- Sí, curso estudios/trabajos relacionados con las OT
- Sí, curso estudios/trabajos relacionados con la ciberseguridad
- Ninguna de las anteriores

Sobre la tecnología

Pregunta 6.1. ¿Con qué frecuencia usas tus dispositivos? (siendo estos dispositivos móviles, tabletas, ordenadores entre otros) *

- A diario
- Ocasionalmente
- Puntualmente
- Nada

Pregunta 6.2. ¿Cuántos dispositivos tienes? *

- 4 o más
- 3
- 2
- 1

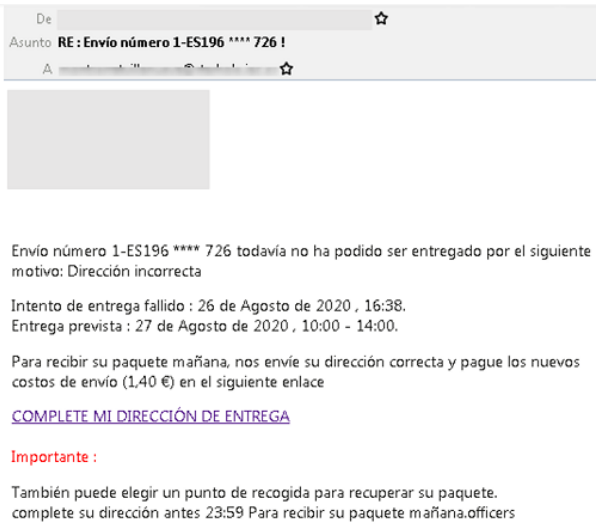
Pregunta 6.3. ¿Conoces todas las funcionalidades que ofrecen tus dispositivos? *

- Sí, conozco todo el potencial de mis dispositivos
- Me defiendo
- Poco
- Casi nada, lo justo y necesario
- Nada

Pregunta 7. ¿Sabes lo que significa la palabra "phishing"? *

- Sí, sé perfectamente lo que significa
- Creo haber escuchado/leído el término por algún lado, pero no sé muy bien lo qué es
- No, no lo había escuchado o leído nunca

Pregunta 8. ¿Has recibido algún correo similar al adjuntado en esta fotografía? *


De
Asunto RE : Envío número 1-ES196 **** 726 !
A

Envío número 1-ES196 **** 726 todavía no ha podido ser entregado por el siguiente motivo: Dirección incorrecta

Intento de entrega fallido : 26 de Agosto de 2020 , 16:38.
Entrega prevista : 27 de Agosto de 2020 , 10:00 - 14:00.

Para recibir su paquete mañana, nos envíe su dirección correcta y pague los nuevos costos de envío (1,40 €) en el siguiente enlace

COMPLETE MI DIRECCIÓN DE ENTREGA

Importante :

También puede elegir un punto de recogida para recuperar su paquete.
complete su dirección antes 23:59 Para recibir su paquete mañana.officers

Figura A. Imagen de un correo electrónico fraudulento
Fuente: INCIBE (s.f.) - OSI (Blog para la ciudadanía)

- Sí
- No

Pregunta 9. *"Durante estos días has realizado un pedido y recibes el correo indicado anteriormente en tu buzón..."* ¿Qué harías en esta situación? *

- Completar la dirección para la entrega del paquete tal y como se indica en el correo
- Otro:

El correo adjunto en la imagen anterior **no** muestra información verídica y de confianza. Este tipo de ataques recibe el nombre generalizado de **"phishing"** donde los propios atacantes intentan conseguir información de la víctima **suplantando la identidad de entidades/personas de confianza** con el objetivo de que pique el anzuelo (de ahí su nombre en inglés) haciendo click al enlace adjunto para la instalación de software malicioso en el dispositivo y/o con campos donde la víctima rellena sus datos para posteriormente el atacante hacerse pasar por la propia víctima.

Se puede manifestar con **diferentes escenarios**: pagar una multa, seguir un pedido, una petición del banco, la compra de unas entradas, un mensaje de un "conocido" entre otros y **diferentes vías** (correos, SMS, llamadas/videollamadas, redes sociales y mensajería instantánea: por ejemplo, WhatsApp) consiguiendo así poder obtener los datos de la víctima (tarjeta de crédito, dirección de residencia...) para que el atacante puede suplantar finalmente la identidad de la víctima.

En caso de llamadas/videollamadas que son ataques más sofisticados y recientes con el auge de la Inteligencia Artificial (IA) la víctima responde estas preguntas aportando sus datos más **los datos biométricos de la víctima (voz y cara) en las que incluye una afirmación (si, ok, de acuerdo, vale)** para que el atacante pueda suplantar finalmente la identidad de la víctima.

Ahora que ya sabes (o sabías) de qué estamos hablando.

Pregunta 10. ¿Con qué frecuencia **durante el mes** recibes los ataques mencionados anteriormente?

Si no es cada mes, contesta con la frecuencia en que los recibes de manera aproximada. *

- Todos los días
- Más de 5 veces al mes
- Una vez a la semana (4 veces)
- 2 o 3 veces al mes
- Una vez al mes

- Nunca

Pregunta 11. ¿Con qué frecuencia **durante el año** los ataques mencionados anteriormente? *

- Sí, en cada mes recibo esta frecuencia de ataques
- No, suele ser cada 2 o 3 meses
- No, suele ser pocas veces durante el año
- Una vez al año
- Nunca

Pregunta 12. ¿**Dónde** recibes estos ataques? Puedes elegir varias opciones para esta pregunta. *

- Mediante correo electrónico
- SMS
- Llamadas
- Videollamadas
- Redes sociales (Facebook, Instagram, X, Tiktok entre otros)
- Mensajería instantánea (WhatsApp, Telegram entre otros)
- Aplicaciones de comunicación (Microsoft Teams, Zoom, Discord entre otros)

Pregunta 13. ¿En cuáles de ellas recibes **el mayor número de estos ataques**? Puedes elegir varias opciones para esta pregunta. *

- Mediante correo electrónico
- SMS
- Llamadas
- Videollamadas
- Redes sociales (Facebook, Instagram, X, Tiktok entre otros)
- Mensajería instantánea (WhatsApp, Telegram entre otros)
- Aplicaciones de comunicación (Microsoft Teams, Zoom, Discord entre otros)

Pregunta 14. ¿En qué **entornos** recibes estos ataques? Puedes elegir varias opciones para esta pregunta. *

- Educativo
- Laboral
- Trámites gubernamentales
- Vida privada

Pregunta 15. ¿En cuál de ellas recibes **el mayor número de estos ataques**? *

- Educativo
- Laboral
- Trámites gubernamentales
- Vida privada

Pregunta 16. ¿Recibes más ataques en estos entornos con respecto a años anteriores? *

- Sí, ahora recibo mucho más que antes
- Veo la misma cantidad que en años anteriores
- No, ahora recibo mucho menos

Pregunta 17. ¿Sabes detectar **sin inconvenientes** si es un ataque o no? *

- Sí, no tengo mucho problema
- Con algunas sí con otras no
- No, no lo sé detectar la verdad

Pregunta 18 ¿Con el tiempo estás recibiendo **ataques cada vez más difíciles de detectar**? *

- Sí, cada vez es más difícil
- Sigue siendo igual para mí
- No, es cada vez más fácil

Pregunta 19. ¿Notas algún cambio en estos ataques con respecto a años anteriores? *

- Sí, con respecto a la manera de comunicarse, es más realista (expresión del lenguaje, escritura, voz e imagen)

- Sí, los datos que ofrecen son bastante similares a la realidad (datos personales y de entidades)
- Todas las anteriores
- No, no he notado ningún cambio
- Otro:

Pregunta 20. ¿Los ataques que has recibido suplantan **ENTIDADES**? *(bancos, tiendas, entidades gubernamentales incluyendo también a empleados...)* **siendo 1 nada y 5 todos los ataques los recibes con estas suplantaciones de identidad**

- 1
- 2
- 3
- 4
- 5

Pregunta 21. ¿Los ataques que has recibido suplantan **PERSONAS**? *(desconocidos, conocidos, compañeros, amigos o familia)* **siendo 1 nada y 5 todos los ataques los recibes con estas suplantaciones de identidad** *

- 1
- 2
- 3
- 4
- 5

Pregunta 22. ¿Has caído en algún ataque que suplantan **ENTIDADES**?

Si es así, indica si se pudo resolver a tiempo y de forma satisfactoria además de cómo te afectó *

- No, no he caído ante ningún ataque
- Si, se pudo resolver en tiempo y satisfactoriamente, me afectó poco
- Si, se pudo resolver en tiempo y satisfactoriamente, me afectó mucho
- Si, no se pudo resolver en tiempo y satisfactoriamente, me afectó bastante
- Otro:

Pregunta 23. ¿Has caído en algún ataque que suplanten **PERSONAS**?

Si es así, indica si se pudo resolver en tiempo y forma además del grado de impacto *

- No, no he caído ante ningún ataque
- Si, se pudo resolver en tiempo y satisfactoriamente, me afectó poco
- Si, se pudo resolver en tiempo y satisfactoriamente, me afectó mucho
- Si, no se pudo resolver en tiempo y satisfactoriamente, me afectó bastante
- Otro:

Pregunta 24. Si en las dos preguntas anteriores has indicado que **has caído ante un ataque** sea en una de las preguntas o ambas.

¿Podrías contar cómo era el ataque o ataques y las repercusiones que tuvo? En caso contrario responde con **"Nada"**

Pregunta 25. Por último ¿Has recibido algún ataque en **otro idioma que no sea el que uses en los diferentes entornos de tu vida diaria**? Si es así, indica cuáles han sido (si no lo recuerdas con exactitud, puedes responder con la zona geográfica donde se habla). *

- No, los ataques son con el idioma o idiomas de mis entornos
- Otro:

¡Con esto sería todo! ¡Como ves los ataques de phishing por muy inofensivos que parezcan puede causar consecuencias económicas y de integridad devastadoras tanto a las víctimas como a las entidades así que para cerrar la encuesta te dejo una serie de consejos para que sea más difícil caer en ellos!

¡Muchas gracias por tu participación!

Consejos ante el phishing:

- Si es un correo **revisa el correo electrónico del remitente carácter por carácter** mirando si coincide con correos que has recibido previamente **sobre todo lo que aparece después del** @. Ejemplo: @amaz0n.es
- Si estás en el ordenador **pasa la dirección del enlace/URL por encima** para ver si el link te redirige a un sitio de confianza o por el contrario a un sitio que no conoces **¡No te olvides de aplicar la revisión de carácter por carácter!**

- Si son peticiones de urgencia **revisa con cuidado** ya que el mayor porcentaje de estos ataques son de esta índole porque la víctima se preocupa mucho por la situación y por ello se vuelve más vulnerable.
- **No descargues archivos adjuntos si no reconoces la identidad que te entrego esos archivos.**
- **Si es una llamada o videollamada** asegúrate de que la persona o personas con la que estás hablando sea una identidad reconocida **ya sea por el número al que te llama o porque estás esperando esa llamada, no confíes únicamente** de la voz y de la cara que veas en la videollamada. Con la implantación de la Inteligencia Artificial se puede suplantar cada vez más fácilmente sin levantar sospechas.
- **No confíes en los mensajes de personas que desconoces** por las redes sociales o por mensajerías instantáneas incluso de llegar a conocerlas, si consideras que mantienen un comportamiento poco habitual con mensajes de participación a links sin contexto alguno, esa persona podría haber caído en un intento de phishing y su identidad haber sido suplantada.
- **En cualquier caso,** si dudas de si estás recibiendo en ese momento un ataque de phishing **no dudes de contactar con las entidades y personas verídicas correspondientes** que estarán encantados de ayudarte.
- ¡Y por último, **nunca te olvides de informar del ataque que has recibido** con las opciones de reporte!

Cualquier duda o consulta que tengas sobre ciberseguridad en su canal de comunicación podrás dirigirlas en Tu Ayuda en Ciberseguridad - INCIBE

A.2 Respuestas recogidas en la encuesta

Las respuestas recogidas se han desglosado en varias imágenes para su correcta visualización debido a la densidad de las preguntas y respuestas.

Marca temporal	¿En qué rango de edad te encuentras?	¿Vives en España o en que zona geográfica reside	¿Qué nivel de español consideras que tienes? Esta encuesta está dirigida a personas que tienen a	¿Cuáles son los últimos estudios que posees o que Si estos estudios no corresponden con los que curs	¿Cursas estudios o trabajas en el ámbito de TI/OT/ Si estás estudiando y trabajando a la vez en estos s
5/30/2025 13:09:25	Entre 35 y 44 años	España (Europa)	Competente (Buen nivel de fluidez y compresión an	Enseñanzas universitarias	Si, curso estudios/trabajo relacionados con la ciber
6/1/2025 21:12:04	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	SÍ, curso estudios/trabajo relacionados con las TI
6/1/2025 21:12:53	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	SÍ, curso estudios/trabajo relacionados con la ciber
6/1/2025 21:13:46	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Educación Secundaria Obligatoria (ESO)	Ninguna de las anteriores
6/1/2025 21:14:04	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	SÍ, curso estudios/trabajo relacionados con las TI
6/1/2025 21:51:13	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/1/2025 21:54:55	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/1/2025 22:10:32	Entre 55 y 64 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/1/2025 22:34:52	Entre 19 y 24 años	España (Europa)	Competente (Buen nivel de fluidez y compresión an	Enseñanzas universitarias	Ninguna de las anteriores
6/1/2025 22:35:42	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/1/2025 23:38:01	Entre 35 y 44 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/1/2025 23:52:12	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Educación Secundaria Obligatoria (ESO)	Ninguna de las anteriores
6/2/2025 7:48:46	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/2/2025 9:07:55	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/2/2025 9:08:47	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/2/2025 10:38:27	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	SÍ, curso estudios/trabajo relacionados con las TI
6/2/2025 13:09:11	Entre 35 y 44 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	Ninguna de las anteriores
6/2/2025 17:26:11	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/2/2025 17:30:26	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/2/2025 17:38:40	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	SÍ, curso estudios/trabajo relacionados con las TI
6/2/2025 17:47:29	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/2/2025 17:55:35	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	SÍ, curso estudios/trabajo relacionados con las TI
6/2/2025 18:03:12	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	SÍ, curso estudios/trabajo relacionados con las TI
6/2/2025 18:24:38	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	SÍ, curso estudios/trabajo relacionados con las TI
6/2/2025 18:33:43	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	Ninguna de las anteriores
6/2/2025 19:16:46	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	SÍ, curso estudios/trabajo relacionados con las TI
6/2/2025 19:16:58	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	Ninguna de las anteriores
6/2/2025 19:29:18	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/2/2025 20:13:15	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	SÍ, curso estudios/trabajo relacionados con las TI
6/2/2025 20:18:00	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	Ninguna de las anteriores
6/2/2025 20:37:48	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/2/2025 21:13:55	Entre 11 y 18 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/2/2025 21:58:33	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	Ninguna de las anteriores
6/2/2025 22:08:21	Entre 25 y 34 años	España (Europa)	Competente (Buen nivel de fluidez y compresión an	Formación Profesional (FP)	SÍ, curso estudios/trabajo relacionados con las TI
6/2/2025 22:34:08	Entre 25 y 34 años	Centroamérica y América del Sur	Soy nativo (Lengua materna)	Formación Profesional (FP)	SÍ, curso estudios/trabajo relacionados con las TI
6/2/2025 23:47:58	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/3/2025 0:53:34	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	Ninguna de las anteriores
6/3/2025 7:10:22	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/7/2025 15:36:37	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/7/2025 18:22:26	Entre 45 y 54 años	España (Europa)	Competente (Buen nivel de fluidez y compresión an	Bachillerato	Ninguna de las anteriores
6/7/2025 18:34:21	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	SÍ, curso estudios/trabajo relacionados con las TI
6/7/2025 18:47:03	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	SÍ, curso estudios/trabajo relacionados con las TI
6/7/2025 18:57:22	Entre 55 y 64 años	España (Europa)	Competente (Buen nivel de fluidez y compresión an	Educación Secundaria Obligatoria (ESO)	Ninguna de las anteriores
6/7/2025 19:35:11	Entre 65 años o más	África	Soy nativo (Lengua materna)	Educación Secundaria Obligatoria (ESO)	Ninguna de las anteriores
6/7/2025 19:44:49	Entre 65 años o más	África	Competente (Buen nivel de fluidez y compresión an	Educación Secundaria Obligatoria (ESO)	SÍ, curso estudios/trabajo relacionados con la ciber
6/7/2025 22:49:11	Entre 45 y 54 años	África	Soy nativo (Lengua materna)	Bachillerato	Ninguna de las anteriores
6/7/2025 22:54:13	Entre 25 y 34 años	Centroamérica y América del Sur	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/7/2025 23:02:44	Entre 25 y 34 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/8/2025 16:00:18	Entre 25 y 34 años	América del Norte	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/8/2025 16:49:16	Entre 25 y 34 años	América del Norte	Soy nativo (Lengua materna)	Formación Profesional (FP)	Ninguna de las anteriores
6/10/2025 11:51:39	Entre 45 y 54 años	España (Europa)	Soy nativo (Lengua materna)	Enseñanzas universitarias	Ninguna de las anteriores
6/10/2025 12:51:46	Entre 55 y 64 años	España (Europa)	Soy nativo (Lengua materna)	Bachillerato	Ninguna de las anteriores
6/16/2025 12:45:19	Entre 19 y 24 años	África	Intermedio (Domino perfectamente la lectura y escr	Enseñanzas universitarias	SÍ, curso estudios/trabajo relacionados con las TI
6/19/2025 20:40:36	Entre 19 y 24 años	España (Europa)	Soy nativo (Lengua materna)	Educación Secundaria Obligatoria (ESO)	Ninguna de las anteriores
6/20/2025 13:22:24	Entre 45 y 54 años	España (Europa)	Soy nativo (Lengua materna)	Formación Profesional (FP)	Ninguna de las anteriores

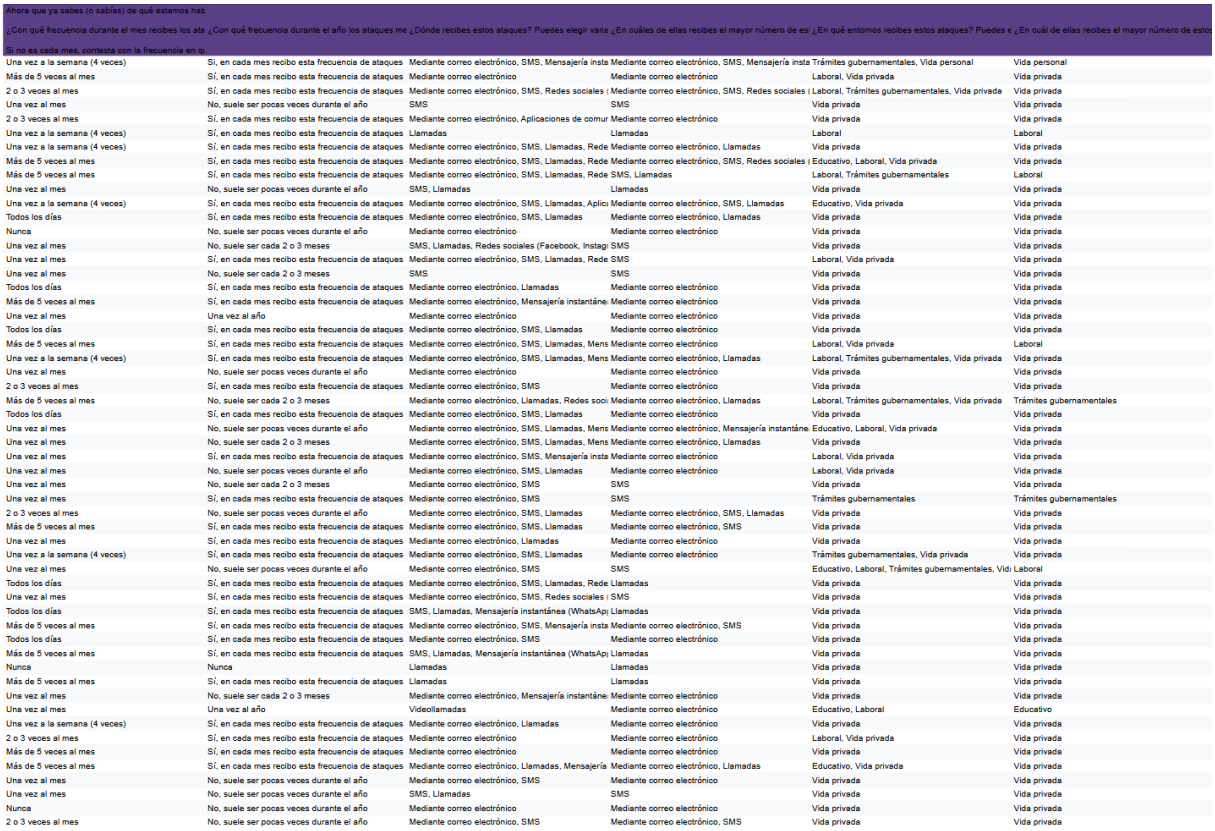
Figura A.2.1. Respuesta a las preguntas formuladas en la encuesta desde la pregunta 1 hasta la pregunta 7 hasta la pregunta 10

Sobre la tecnología 1. ¿Con qué frecuencia usas tus dispositivos? (sien	2. ¿Cuántos dispositivos tienes?	3. ¿Conoces todas las funcionalidades que ofrecen	¿Sabes lo que significa la palabra "phishing"?	¿Has recibido algún correo similar al adjuntado en e Fuente: INCIBE - OSI (Blog para la ciudadanía)
A diario		3 Si, conozco todo el potencial de mis dispositivos	Si, sé perfectamente lo que significa	Sí
A diario	4 o más	Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		3 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		2 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		2 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		3 Poco	Creo haber escuchado/leído el término por algún la	No
A diario		3 Me defiendo	Creo haber escuchado/leído el término por algún la	Sí
A diario		3 Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario		3 Me defiendo	Creo haber escuchado/leído el término por algún la	Sí
A diario		3 Me defiendo	No, no lo había escuchado o leído nunca	No
A diario	4 o más	Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario	4 o más	Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario		3 Sí, conozco todo el potencial de mis dispositivos	No, no lo había escuchado o leído nunca	No
A diario		3 Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario		3 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		2 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		3 Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario	4 o más	Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		2 Me defiendo	Creo haber escuchado/leído el término por algún la	Sí
A diario	4 o más	Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario	4 o más	Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario	4 o más	Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario	4 o más	Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	No
A diario	4 o más	Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		3 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		2 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		2 Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario	4 o más	Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario		3 Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario		3 Poco	No, no lo había escuchado o leído nunca	Sí
A diario		3 Me defiendo	Creo haber escuchado/leído el término por algún la	Sí
A diario		2 Poco	No, no lo había escuchado o leído nunca	Sí
A diario		3 Me defiendo	Creo haber escuchado/leído el término por algún la	No
A diario		1 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		2 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		2 Me defiendo	Creo haber escuchado/leído el término por algún la	Sí
A diario		1 Poco	Sí, sé perfectamente lo que significa	Sí
A diario		3 Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario		3 Sí, conozco todo el potencial de mis dispositivos	No, no lo había escuchado o leído nunca	Sí
A diario		1 Poco	Creo haber escuchado/leído el término por algún la	No
A diario	4 o más	Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		3 Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario		1 Me defiendo	No, no lo había escuchado o leído nunca	No
A diario		2 Me defiendo	No, no lo había escuchado o leído nunca	No
A diario		2 Poco	No, no lo había escuchado o leído nunca	No
A diario		2 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario	4 o más	Sí, conozco todo el potencial de mis dispositivos	Creo haber escuchado/leído el término por algún la	Sí
A diario		3 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		3 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario	4 o más	Me defiendo	Sí, sé perfectamente lo que significa	Sí
A diario		3 Me defiendo	Creo haber escuchado/leído el término por algún la	Sí
A diario		3 Me defiendo	Sí, sé perfectamente lo que significa	No
A diario		3 Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	No
A diario	4 o más	Sí, conozco todo el potencial de mis dispositivos	Sí, sé perfectamente lo que significa	Sí
A diario		2 Poco	No, no lo había escuchado o leído nunca	No

Figura A.2.2 Respuesta a las preguntas formuladas en la encuesta desde la pregunta 8.1 hasta la pregunta 8.1

"Durante estos días has realizado un pedido y recibes el correo indicado anteriormente en tu buzón.." ¿Que harías en esta situación?
Contactar directamente a la empresa de correos desde su sitio web oficial para clarificar el asunto.
No hacer caso y eliminar el correo
Verificar si los datos son correctos, en caso de que no lo sean informar del correo en la bandeja como phishing
No rellenar nada que no este verificado por la empresa de transporte
Revisar en la página o aplicación oficial donde hice el pedido para ver el estado del mismo y si es necesario o no realizar alguna acción adicional
No dar ninguna información, especialmente si sé que no he pedido ningún paquete
Reportar como spam e ignorarlo.
Compruebo si he hecho el pedido y si lo he hecho en que situacions de envio esta
Ignorar-lo. La dirección era correcta.
Llamar a la empresa
Corroborar los datos con la entidad, o empresa, verificar si he pedido un paquete el número de seguimiento y empresa de transporte, etc.
No entrar al enlace
No contestar
ignorar el mensaje
Comprobar dirección correo empresa, y consultar en pagina web oficial
No es necesario rellenar los datos tras completar una compra, ya deberían estar esos datos adjuntos a mi usuario de la página/app donde se hizo la compra
Marcarlo como para que a outlook le dé igual y me vuelva a llegar mañana.
Ignorarlo completamente.
Ignorarlo
Eliminar directamente y reportar como spam si no está marcado
No entiendo muy bien lo que dice, el contexto es raro
Comprobar en la tienda oficial si realmente he puesto mal la dirección o no para ver si es verdad aunque con ver el receptor del mensaje se suele saber si es fake o no
No hacer caso al correo
Borrarlo o denunciarlo por spam si se puede
Si no he pedido nada por internet o se que no me van a enviar nada paso de este correo y lo borro. Si he pedido o se que me tienen que enviar algo investigo la propia web o página del envío tipo Amazon, correos o lo que sea a ver si ahí me dice algo más de info, si veo que no tiene sentido/huele raro, hago lo mismo que antes
Ignoro el correo ya que los datos de dirección ya están rellenados cuando realicé el pedido
Ignorar el correo
Compruebo si los datos coinciden con mi pedido. En caso de que coincidan me pongo en contacto con la empresa de paquetería a través de canales oficiales, evitando así enviar mis datos a un correo sospechoso
Borrar el mensaje
Llamar
Denunciar
No hacerle caso al mensaje
Comprobar que es fiable. Si lo es, relleno los campos, si no, elimino
No pongo nada
eliminar correo
Soy muy desconfiada, no haría nada, lo marco como spam
Eliminar mensaje
Lo ignoraría y eliminaría
ignorar
Asegurarme si es verdad la información proporcionada
Mirar si en la aplicación del pedido hay realmente alguna incidencia
Reportar por phising
No voy hacer nada porque no me fío del correo
Completar la dirección para la entrega del paquete tal y como se indica en el correo
Rechazar los no conocidos
Marcarlo como spam
Completar la dirección para la entrega del paquete tal y como se indica en el correo
nada
Para empezar mi direccion siempre es la misma, no hay motivo para que sea otra. En la propia web oficial si hay error tambien lo pondria ahí. tambien ver el correo desde el que se envia el mensaje que siempre tienen algun error o sospechoso.
marcar al número de la compañía de envios que está en su pagina web y aclarar la situación, si es legítimo entonces hacerlo desde la llamada
Sospecho de fraude
Contactar con la empresa a la que he comprado
No contesto a ese correo
borrar el mail de pishing
No relleno nada

Figura A.2.3 Respuesta a las preguntas formuladas en la encuesta de la pregunta 11



Ahora que ya sabes (o sabías) de qué estamos hab					
¿Con qué frecuencia durante el mes recibes los ata	¿Con qué frecuencia durante el año los ataques me	¿Dónde recibes estos ataques? Puedes elegir varia	¿En cuáles de ellas recibes el mayor número de es	¿En qué entornos recibes estos ataques? Puedes e	¿En cuál de ellas recibes el mayor número de estos
Si no es cada mes, contesta con la frecuencia en qu					
Una vez a la semana (4 veces)	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Mensajería insta	Mediante correo electrónico, SMS, Mensajería insta	Trámites gubernamentales, Vida personal	Vida personal
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico	Mediante correo electrónico	Laboral, Vida privada	Vida privada
2 o 3 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Redes sociales (	Mediante correo electrónico, SMS, Redes sociales (	Laboral, Trámites gubernamentales, Vida privada	Vida privada
Una vez al mes	No, suele ser pocas veces durante el año	SMS	SMS	Vida privada	Vida privada
2 o 3 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, Aplicaciones de comur	Mediante correo electrónico	Vida privada	Vida privada
Una vez a la semana (4 veces)	Sí, en cada mes recibo esta frecuencia de ataques	Llamadas	Llamadas	Laboral	Laboral
Una vez a la semana (4 veces)	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas, Rede	Mediante correo electrónico, Llamadas	Vida privada	Vida privada
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas, Rede	Mediante correo electrónico, SMS, Redes sociales (	Educativo, Laboral, Vida privada	Vida privada
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas, Rede	SMS, Llamadas	Laboral, Trámites gubernamentales	Laboral
Una vez al mes	No, suele ser pocas veces durante el año	SMS, Llamadas	Llamadas	Vida privada	Vida privada
Una vez a la semana (4 veces)	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas, Aplica	Mediante correo electrónico, SMS, Llamadas	Educativo, Vida privada	Vida privada
Todos los días	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas	Mediante correo electrónico, Llamadas	Vida privada	Vida privada
Nunca	No, suele ser pocas veces durante el año	Mediante correo electrónico	Mediante correo electrónico	Vida privada	Vida privada
Una vez al mes	No, suele ser cada 2 o 3 meses	SMS, Llamadas, Redes sociales (Facebook, Instagr	SMS	Vida privada	Vida privada
Una vez al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas, Rede	SMS	Laboral, Vida privada	Vida privada
Una vez al mes	No, suele ser cada 2 o 3 meses	SMS	SMS	Vida privada	Vida privada
Todos los días	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, Llamadas	Mediante correo electrónico	Vida privada	Vida privada
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, Mensajería instantáne	Mediante correo electrónico	Vida privada	Vida privada
Una vez al mes	Una vez al año	Mediante correo electrónico	Mediante correo electrónico	Vida privada	Vida privada
Todos los días	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas	Mediante correo electrónico	Vida privada	Vida privada
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas, Mens	Mediante correo electrónico	Laboral, Vida privada	Laboral
Una vez a la semana (4 veces)	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas, Mens	Mediante correo electrónico, Llamadas	Laboral, Trámites gubernamentales, Vida privada	Vida privada
Una vez al mes	No, suele ser pocas veces durante el año	Mediante correo electrónico	Mediante correo electrónico	Vida privada	Vida privada
2 o 3 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS	Mediante correo electrónico	Vida privada	Vida privada
Más de 5 veces al mes	No, suele ser cada 2 o 3 meses	Mediante correo electrónico, Llamadas, Redes soci	Mediante correo electrónico, Llamadas	Laboral, Trámites gubernamentales, Vida privada	Trámites gubernamentales
Todos los días	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas	Mediante correo electrónico	Vida privada	Vida privada
Una vez al mes	No, suele ser pocas veces durante el año	Mediante correo electrónico, SMS, Llamadas, Mens	Mediante correo electrónico, Mensajería instantáne	Educativo, Laboral, Vida privada	Vida privada
Una vez al mes	No, suele ser cada 2 o 3 meses	Mediante correo electrónico, SMS, Llamadas, Mens	Mediante correo electrónico, Llamadas	Vida privada	Vida privada
Una vez al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Mensajería insta	Mediante correo electrónico	Laboral, Vida privada	Vida privada
Una vez al mes	No, suele ser pocas veces durante el año	Mediante correo electrónico, SMS, Llamadas	Mediante correo electrónico	Laboral, Vida privada	Vida privada
Una vez al mes	No, suele ser cada 2 o 3 meses	Mediante correo electrónico, SMS	SMS	Vida privada	Vida privada
Una vez al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS	SMS	Trámites gubernamentales	Trámites gubernamentales
2 o 3 veces al mes	No, suele ser pocas veces durante el año	Mediante correo electrónico, SMS, Llamadas	Mediante correo electrónico, SMS, Llamadas	Vida privada	Vida privada
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas	Mediante correo electrónico, SMS	Vida privada	Vida privada
Una vez al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, Llamadas	Mediante correo electrónico	Vida privada	Vida privada
Una vez a la semana (4 veces)	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas	Mediante correo electrónico	Trámites gubernamentales, Vida privada	Vida privada
Una vez al mes	No, suele ser pocas veces durante el año	Mediante correo electrónico, SMS	SMS	Educativo, Laboral, Trámites gubernamentales, Vida	Laboral
Todos los días	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Llamadas, Rede	Llamadas	Vida privada	Vida privada
Una vez al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Redes sociales (	SMS	Vida privada	Vida privada
Todos los días	Sí, en cada mes recibo esta frecuencia de ataques	SMS, Llamadas, Mensajería instantánea (WhatsAp	Llamadas	Vida privada	Vida privada
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS, Mensajería insta	Mediante correo electrónico, SMS	Vida privada	Vida privada
Todos los días	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, SMS	Mediante correo electrónico	Vida privada	Vida privada
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	SMS, Llamadas, Mensajería instantánea (WhatsAp	Llamadas	Vida privada	Vida privada
Nunca	Nunca	Llamadas	Llamadas	Vida privada	Vida privada
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Llamadas	Llamadas	Vida privada	Vida privada
Una vez al mes	No, suele ser cada 2 o 3 meses	Mediante correo electrónico, Mensajería instantáne	Mediante correo electrónico	Vida privada	Vida privada
Una vez al mes	Una vez al año	Videollamadas	Mediante correo electrónico	Educativo, Laboral	Educativo
Una vez a la semana (4 veces)	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, Llamadas	Mediante correo electrónico	Vida privada	Vida privada
2 o 3 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico	Mediante correo electrónico	Laboral, Vida privada	Vida privada
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico	Mediante correo electrónico	Vida privada	Vida privada
Más de 5 veces al mes	Sí, en cada mes recibo esta frecuencia de ataques	Mediante correo electrónico, Llamadas, Mensajería	Mediante correo electrónico, Llamadas	Educativo, Vida privada	Vida privada
Una vez al mes	No, suele ser pocas veces durante el año	Mediante correo electrónico, SMS	Mediante correo electrónico	Vida privada	Vida privada
Una vez al mes	No, suele ser pocas veces durante el año	SMS, Llamadas	SMS	Vida privada	Vida privada
Nunca	No, suele ser pocas veces durante el año	Mediante correo electrónico	Mediante correo electrónico	Vida privada	Vida privada
2 o 3 veces al mes	No, suele ser pocas veces durante el año	Mediante correo electrónico, SMS	Mediante correo electrónico, SMS	Vida privada	Vida privada

Figura A.2.4 Respuesta a las preguntas formuladas en la encuesta desde la pregunta 12 hasta la pregunta 16

¿Recibes más ataques en estos entornos con respe	¿Sabes detectar sin inconvenientes si es un ataque	¿Con el tiempo estás recibiendo ataques cada vez	¿Notas algún cambio en estos ataques con respect	¿Los ataques que has recibido suplantan ENTIDAD	¿Los ataques que has recibido suplantan PERSON
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mi	Sí, con respecto a la manera de comunicarse, es m	5	2
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, los datos que ofrecen son bastante similares a la	5	1
Sí, ahora recibo mucho más que antes	Con algunas sí con otras no	Sí, cada vez es más difícil	Todos los anteriores	4	2
No, ahora recibo mucho menos	Sí, no tengo mucho problema	No, es cada vez más fácil	Sí, con respecto a la manera de comunicarse, es m	2	1
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	4	2
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Todas las anteriores	3	1
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	4	1
Sí, ahora recibo mucho más que antes	Con algunas sí con otras no	Sí, cada vez es más difícil	Sí, con respecto a la manera de comunicarse, es m	4	4
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Todas las anteriores	4	1
Veo la misma cantidad que en años anteriores	No, no lo sé detectar la verdad	Sí, cada vez es más difícil	Sí, los datos que ofrecen son bastante similares a la	3	1
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	4	1
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	5	1
Sí, ahora recibo mucho más que antes	Con algunas sí con otras no	Sí, cada vez es más difícil	Sí, con respecto a la manera de comunicarse, es m	2	1
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sí, cada vez es más difícil	Todas las anteriores	4	2
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, los datos que ofrecen son bastante similares a la	4	2
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	3	1
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sí, cada vez es más difícil	Sí, los datos que ofrecen son bastante similares a la	5	1
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	3	1
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	3	3
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sí, cada vez es más difícil	Sí, los datos que ofrecen son bastante similares a la	5	1
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	5	4
Sí, ahora recibo mucho más que antes	Con algunas sí con otras no	Sí, cada vez es más difícil	Sí, los datos que ofrecen son bastante similares a la	5	1
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	3	1
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	5	3
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	En las llamadas se nota que usan una IA con voz, c	4	2
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, los datos que ofrecen son bastante similares a la	4	1
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	1	3
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	4	3
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	4	1
Sí, ahora recibo mucho más que antes	No, no lo sé detectar la verdad	Sí, cada vez es más difícil	Todas las anteriores	5	2
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, los datos que ofrecen son bastante similares a la	4	1
Sí, ahora recibo mucho más que antes	Con algunas sí con otras no	Sigue siendo igual para mí	No, no he notado ningún cambio	4	1
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	4	1
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sí, cada vez es más difícil	Sí, los datos que ofrecen son bastante similares a la	5	5
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sí, cada vez es más difícil	Sí, los datos que ofrecen son bastante similares a la	3	2
No, ahora recibo mucho menos	Sí, no tengo mucho problema	Sigue siendo igual para mí	Todas las anteriores	4	2
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Todas las anteriores	5	5
No, ahora recibo mucho menos	Con algunas sí con otras no	Sí, cada vez es más difícil	No, no he notado ningún cambio	1	2
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	5	3
Sí, ahora recibo mucho más que antes	Con algunas sí con otras no	Sí, cada vez es más difícil	Todas las anteriores	5	1
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	5	3
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sí, cada vez es más difícil	Sí, los datos que ofrecen son bastante similares a la	5	1
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	4	1
No, ahora recibo mucho menos	No, no lo sé detectar la verdad	No, es cada vez más fácil	No, no he notado ningún cambio	3	3
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sí, cada vez es más difícil	Sí, con respecto a la manera de comunicarse, es m	5	1
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sí, cada vez es más difícil	Sí, con respecto a la manera de comunicarse, es m	3	2
Sí, ahora recibo mucho más que antes	Con algunas sí con otras no	Sí, cada vez es más difícil	Todas las anteriores	2	2
Sí, ahora recibo mucho más que antes	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	5	1
No, ahora recibo mucho menos	Sí, no tengo mucho problema	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	3	3
Veo la misma cantidad que en años anteriores	Con algunas sí con otras no	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	4	2
Veo la misma cantidad que en años anteriores	Con algunas sí con otras no	Sí, cada vez es más difícil	Sí, los datos que ofrecen son bastante similares a la	3	3
No, ahora recibo mucho menos	Sí, no tengo mucho problema	Sigue siendo igual para mí	Todas las anteriores	1	1
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	1	5
Veo la misma cantidad que en años anteriores	Sí, no tengo mucho problema	Sigue siendo igual para mí	No, no he notado ningún cambio	2	1
No, ahora recibo mucho menos	Con algunas sí con otras no	Sigue siendo igual para mí	Sí, con respecto a la manera de comunicarse, es m	3	3

Figura A.2.5. Respuesta a las preguntas formuladas en la encuesta desde la pregunta 17 hasta la pregunta 22

¿Has caído en algún ataque que suplanten ENTIDA Si es así, indica si se pudo resolver a tiempo y de fc	¿Has caído en algún ataque que suplanten PERSO Si es así, indica si se pudo resolver en tiempo y forr	Si en las dos preguntas anteriores has indicado que ¿Podrías contar como era el ataque o ataques y las	Por último ¿Has recibido algún ataque en otro idion
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		Si, he recibido en Inglés
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	Ruso y zona sur de África
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
Si, se pudo resolver en tiempo y sastifactioramente,	No, no he caído ante ningún ataque	Nada	Si ingles
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
Si, se pudo resolver en tiempo y sastifactioramente,	No, no he caído ante ningún ataque		En inglés, francés y alemán.
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
Si, no se pudo resolver en tiempo y sastifactioramer	No, no he caído ante ningún ataque		Si
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		alguna vez he recibido un mensaje en un idioma de
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		Francés
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada.	Recibidos en inglés y en alguna lengua que GTrans
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No he caído en ninguno, pero hace un par de mese	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	nada	Árabe
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	En ingles y mandarin/chino
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
Si, se pudo resolver en tiempo y sastifactioramente,	No, no he caído ante ningún ataque		Ingles, frances, filipino, etc. No sabria nombrarlos t
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
Si, se pudo resolver en tiempo y sastifactioramente,	No, no he caído ante ningún ataque	No fue un ataque real, fue un entrenamiento de emp	No, los ataques son con el idioma o idiomas de mis
Si, se pudo resolver en tiempo y sastifactioramente,	Si, no se pudo resolver en tiempo y sastifactioramer	Llamándome para que diga " SI",	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Estaba vendiendo un móvil en wallapop, me pidiero	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	Ruso
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	Inglés
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No se si puede contar, en suplantacion de identidad	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		Inglés
Si, se pudo resolver en tiempo y sastifactioramente,	No, no he caído ante ningún ataque		
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		Francés
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		Africanos
Si, no se pudo resolver en tiempo y sastifactioramer	Si, se pudo resolver en tiempo y sastifactioramente,	me afectó mucho	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	nada	No, los ataques son con el idioma o idiomas de mis
Si, no se resolvió, pero me afectó poco	No, no he caído ante ningún ataque	fue phising con mi vieja cuenta de Apple que ya no	Inglés
Si, se pudo resolver en tiempo y sastifactioramente,	Si, se pudo resolver en tiempo y sastifactioramente,	Mi hijo socitaba ayuda x SMS y yo no tengo hijos.	No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		No, los ataques son con el idioma o idiomas de mis
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque		inglés y francés
No, no he caído ante ningún ataque	No, no he caído ante ningún ataque	Nada	No, los ataques son con el idioma o idiomas de mis

Figura A.2.6 Respuesta a las preguntas formuladas en la encuesta desde la pregunta 23 hasta la pregunta 26