**CiberAmigo: Plataforma de Protección y Asistencia en Ciberseguridad para Adultos Mayores**

*Equipo:*

*\* Alan Gomez \** *Iker Fernandez*

*\* Regina Montesinos \* Víctor Villafáñez*

*\* Ximena De Jesus Romero*

*PITUFOS*

**Resumen** – CiberAmigo es una solución innovadora diseñada para proteger a los adultos mayores de ciberataques y fraudes en línea mediante el uso de inteligencia artificial. Esta plataforma incluye monitoreo de red, análisis de correos electrónicos y redes sociales, y un asistente en forma de chatbot que proporciona recomendaciones de seguridad. La aplicación alerta a los usuarios sobre actividades sospechosas y les ofrece asistencia personalizada para mejorar su seguridad en línea. CiberAmigo busca promover la seguridad digital y la confianza en la tecnología para un sector vulnerable, ayudando a prevenir riesgos cibernéticos de manera accesible y efectiva.

**Palabras clave** – Ciberseguridad, Adultos mayores, inteligencia artificial, Monitoreo de red, Chatbot, Prevención de fraudes, Seguridad digital, Asistencia en línea .

## 1. Introducción

Al cierre de 2023, las quejas por fraudes cibernéticos aumentaron en 20.1% respecto al mismo periodo de 2022 y representan cada año una mayor proporción al pasar de 59% en 2018 al 71% en 2023.[1]

Tabla

Descripción generada automáticamente.[1]

La Secretaría del Bienestar ha alertado a los beneficiarios del Programa de Pensión del Bienestar para las Personas Adultas Mayores,**sobre estafas que están ocurriendo en WhatsApp relacionadas con las pensiones de los cuentahabientes.**

A través de un comunicado, la Secretaría aclaró que **no "ofrece préstamos a través de llamadas telefónicas, mensajes de texto ni WhatsApp". [2]**

Por lo que convocó a los usuarios a no dejarse engañar e instó a evitar compartir cualquier tipo de información que pudiera poner en riesgo la seguridad del usuario, **tales como datos personales, número o PIN de su tarjeta, etc.** **Uno de los grupos más vulnerables para caer en una estafa son los adultos mayores.**En este sentido es importante mantenerse al tanto de sus actividades digitales para evitar que sean víctimas de los ciberdelincuentes. .[2]

## México está entre los 10 países con más cibercrímenes en el mundo

De acuerdo con datos de la empresa de ciberseguridad Surfshark, 801.000 usuarios de internet fueron víctimas de crímenes cibernéticos a nivel mundial en 2022. El delito más común fue el fraude financiero

En la era digital, los adultos mayores representan un grupo vulnerable a ciberataques y fraudes en línea debido a la falta de familiaridad con tecnologías de seguridad y prácticas de protección de datos. El aumento de la digitalización ha dado lugar a un incremento en el número de estafas que se dirigen específicamente a esta población, que suele carecer de alfabetización digital necesaria para protegerse de manera efectiva.

CiberAmigo se presenta como una plataforma integral de ciberseguridad enfocada en proteger a los adultos mayores mediante el uso de inteligencia artificial y tecnologías de monitoreo. Esta solución innovadora ofrece alertas en tiempo real sobre actividades sospechosas, así como un asistente de chatbot que ayuda a los usuarios a identificar y comprender los riesgos cibernéticos. CiberAmigo no solo tiene un impacto ético al mejorar la seguridad de este sector, sino que también fortalece su confianza en el uso de la tecnología para una vida digital más segura.

## Objetivo

## Desarrollar una plataforma de ciberseguridad accesible y efectiva, diseñada para proteger a los adultos mayores de ciberataques y fraudes en línea, mediante el uso de inteligencia artificial y tecnologías de monitoreo, brindándoles asistencia personalizada y recomendaciones de seguridad.

## Objetivos Específicos

1. Implementar un sistema de monitoreo de red que detecte actividades sospechosas y potenciales riesgos cibernéticos para alertar al usuario de forma proactiva.
2. Integrar un chatbot que, mediante inteligencia artificial, proporcione asesoramiento en temas de ciberseguridad y respuesta a las dudas frecuentes de los adultos mayores, en un lenguaje claro y accesible.
3. Diseñar un sistema de alertas por correo electrónico que informe al usuario sobre cualquier actividad sospechosa detectada en su red, facilitando la toma de acciones preventivas.
4. Fomentar la confianza y el uso seguro de la tecnología en adultos mayores, a través de recomendaciones y herramientas prácticas que les permitan protegerse en línea.

**Justificación**

El uso creciente de tecnologías digitales por parte de los adultos mayores, especialmente en la comunicación, el entretenimiento y las transacciones en línea, ha incrementado su exposición a riesgos cibernéticos como fraudes, estafas de phishing y accesos no autorizados. Sin embargo, esta población suele carecer de conocimientos en ciberseguridad, lo que los convierte en un blanco fácil para los ciberatacantes.

**CiberAmigo** responde a esta problemática proporcionando una solución accesible y adaptada a las necesidades de seguridad de los adultos mayores. A través de un monitoreo proactivo de su red y correo electrónico, junto con un chatbot asistente que responde en términos claros y sencillos, CiberAmigo no solo previene incidentes de ciberseguridad, sino que también educa y empodera a los usuarios, fomentando una mayor confianza en el uso de tecnologías digitales.

Esta plataforma se justifica no solo por su impacto en la protección individual de los adultos mayores, sino también por el beneficio social y ético de reducir la vulnerabilidad de un sector que, en muchos casos, depende cada vez más de la tecnología para sus actividades cotidianas. Además, CiberAmigo ofrece una solución innovadora que aprovecha la inteligencia artificial y las herramientas de monitoreo para crear un ambiente digital más seguro para esta población.

Para justificar la importancia de **CiberAmigo** y el impacto de los ciberataques en adultos mayores, se pueden considerar estadísticas recientes:

1. **Aumento en el número de ataques dirigidos a adultos mayores**: En 2023, los adultos mayores (mayores de 60 años) representaron uno de los grupos más afectados por delitos cibernéticos. De hecho, en Estados Unidos, este grupo mostró un alto número de víctimas de estafas y fraudes digitales. Esta situación se agrava debido a que los adultos mayores, en general, presentan una menor familiaridad con las prácticas de ciberseguridad, lo cual los convierte en blancos atractivos para los ciberdelincuentes​

.

1. **Frecuencia y costos de los ciberataques**: A nivel mundial, el costo de los ciberataques continúa en aumento. Tan solo en el primer semestre de 2023, el número de ataques de ransomware creció un 42% en comparación con el año anterior, afectando gravemente a las personas y empresas, y destacando la necesidad de protección contra estos riesgos​
2. **Vulnerabilidad a los ataques de phishing**: El phishing sigue siendo uno de los métodos más comunes para distribuir malware, siendo responsable de hasta el 92% de los ataques de malware a través del correo electrónico. Este tipo de ataques puede dirigirse fácilmente a adultos mayores, especialmente si estos no cuentan con las habilidades digitales para identificar mensajes fraudulentos​
3. **Impacto de la falta de alfabetización digital**: Muchos adultos mayores no están acostumbrados a identificar enlaces sospechosos o prácticas fraudulentas en redes sociales, lo cual incrementa su riesgo de ser víctimas de ataques. La educación y el soporte en ciberseguridad, como el que ofrece CiberAmigo, se vuelven esenciales para mitigar estos riesgos y proporcionar un entorno digital más seguro para este grupo.

## Problemática

La problemática abordada del proyecto se centra en las dificultades que enfrentan los dueños de mascotas para

Con el avance de la tecnología y la digitalización de la vida cotidiana, los adultos mayores se enfrentan a riesgos crecientes de ciberataques, fraudes, y estafas en línea. Muchos de ellos no poseen los conocimientos necesarios en ciberseguridad para protegerse adecuadamente, lo cual los convierte en un blanco fácil para los ciberdelincuentes. Esta falta de alfabetización digital puede llevar a situaciones en las que los adultos mayores sean víctimas de phishing, robo de identidad, o incluso engaños en redes sociales.

A nivel mundial, los ataques a personas y pequeñas organizaciones han incrementado su frecuencia y sofisticación, destacándose el phishing como uno de los métodos de ataque más comunes, debido a que hasta el 92% de los ataques de malware se distribuyen a través del correo electrónico. Estos riesgos aumentan para los adultos mayores, quienes a menudo son menos capaces de reconocer señales de peligro en línea, como enlaces sospechosos o mensajes fraudulentos​

Además, la pandemia de COVID-19 aceleró la adopción de tecnologías digitales, lo que obligó a muchos adultos mayores a utilizar servicios en línea sin la capacitación adecuada. Esto expuso aún más a este grupo a ciberataques y fraudes en momentos críticos. Sin un soporte adecuado, los adultos mayores no solo corren el riesgo de perder datos personales y financieros, sino también de ver afectada su confianza en el uso de la tecnología.

**CiberAmigo** surge como una respuesta a esta problemática, buscando ofrecer una solución accesible y educativa que brinde apoyo en tiempo real, ayude a identificar riesgos, y proporcione recomendaciones de seguridad en un lenguaje claro y adaptado a las necesidades de esta población vulnerable.

## Propuesta de solución

## Para abordar el problema de la alimentación de mascotas, se CiberAmigo es una plataforma integral de ciberseguridad diseñada específicamente para proteger a los adultos mayores de amenazas en línea, utilizando inteligencia artificial y tecnologías de monitoreo. La solución se compone de tres componentes principales:

## Monitoreo de red: CiberAmigo cuenta con un sistema que analiza el tráfico de red en tiempo real para detectar actividades sospechosas, como accesos no autorizados o intentos de ataque. Este componente permite identificar patrones de riesgo en los protocolos HTTP, HTTPS y SSH, así como prevenir ataques de tipo ping o intentos de fuerza bruta.

## Análisis de correos electrónicos y redes sociales: La plataforma incluye un sistema de análisis de correos electrónicos que examina el contenido de los mensajes en busca de enlaces y mensajes potencialmente maliciosos. Esto ayuda a proteger a los usuarios de ataques de phishing y fraudes que suelen distribuirse por estos medios. Además, se analiza la actividad en redes sociales para identificar intentos de fraude o mensajes engañosos.

## Asistente de seguridad mediante chatbot: El sistema incorpora un chatbot basado en inteligencia artificial, que ofrece recomendaciones y resuelve dudas de los adultos mayores en temas de seguridad digital. El chatbot utiliza un lenguaje sencillo y está entrenado para responder a preguntas frecuentes sobre cómo prevenir riesgos, identificar enlaces sospechosos y proteger sus cuentas en línea.

## Alertas por correo electrónico y acciones correctivas: Ante cualquier actividad sospechosa, CiberAmigo envía una alerta por correo electrónico al usuario. El mensaje incluye un resumen de las amenazas detectadas y un botón de "Más información" que dirige al usuario a la interfaz del chatbot, donde recibe recomendaciones personalizadas y aclaraciones sobre los riesgos identificados.

## Objetivo de la Solución: Esta propuesta no solo busca proteger a los adultos mayores de posibles ataques, sino también fomentar su educación y confianza en el uso de tecnologías digitales. Mediante un monitoreo constante, alertas proactivas y asistencia adaptada, CiberAmigo actúa como un escudo preventivo que mejora la seguridad digital de esta población vulnerable y les brinda herramientas prácticas para enfrentar los riesgos en línea.

## Diseño y Arquitectura del sistema

iberAmigo está diseñado como una plataforma de múltiples componentes que integran monitoreo de red, análisis de correos electrónicos y redes sociales, y un chatbot interactivo para proporcionar asistencia en tiempo real a los usuarios. La arquitectura del sistema incluye los siguientes módulos clave:

1. Módulo de Monitoreo de Red

Descripción: Este módulo utiliza Python y la biblioteca Scapy para capturar y analizar el tráfico de red en tiempo real.

Funcionalidad: Se encarga de monitorear los protocolos HTTP, HTTPS, SSH y los intentos de ping. Detecta patrones sospechosos, como solicitudes frecuentes a páginas inseguras o accesos no autorizados, generando una alerta cuando se superan ciertos umbrales de actividad.

Implementación: Este módulo se despliega en una máquina virtual en Azure, que actúa como servidor de monitoreo, y está configurado para iniciar automáticamente en cada reinicio de la máquina.

2. Módulo de Análisis de Correos Electrónicos y Redes Sociales

Descripción: Este componente analiza los correos electrónicos del usuario en busca de patrones de phishing, enlaces sospechosos y mensajes no reconocidos.

Funcionalidad: Utilizando IMAP y expresiones regulares, el sistema detecta signos de contenido malicioso en los correos electrónicos, tales como enlaces desconocidos o idiomas distintos al del usuario.

Implementación: Al identificar actividades sospechosas, envía alertas que permiten al usuario tomar acciones preventivas. Este módulo también se ejecuta en el servidor de Azure junto con el monitoreo de red.

3. Chatbot de Asistencia en Ciberseguridad

Descripción: Este módulo es un chatbot basado en Dialogflow (de Google Cloud) que ofrece asistencia personalizada en temas de ciberseguridad.

Funcionalidad: Responde a las dudas del usuario sobre protección en línea, phishing, contraseñas seguras, y medidas contra el fraude. Además, proporciona recomendaciones automáticas cuando el usuario hace clic en "Más información" tras recibir una alerta de seguridad.

Implementación: El chatbot se integra en la interfaz web del frontend y está configurado para recibir un mensaje inicial basado en el contexto de la alerta detectada.

4. Módulo de Alerta y Notificación por Correo Electrónico

Descripción: Este módulo se encarga de enviar alertas al usuario cuando se detectan actividades sospechosas.

Funcionalidad: Utiliza el servicio SMTP de Gmail para enviar correos electrónicos que contienen un resumen de los riesgos detectados y un enlace "Más información" que redirige al chatbot para obtener ayuda adicional.

Implementación: Este módulo se activa cada vez que el sistema de monitoreo o el análisis de correos detecta actividades fuera de lo común.

Arquitectura del Sistema

1. Arquitectura de N-capas:

Capa de Presentación (Frontend): La interfaz de usuario está desarrollada en React y permite la interacción con el chatbot, así como el acceso a las alertas y recomendaciones de seguridad. Este frontend se despliega en Azure para acceso en línea.

Capa de Lógica de Negocios (Backend): Esta capa incluye los módulos de monitoreo de red, análisis de correos y notificaciones, todos desarrollados en Python. Los scripts se ejecutan en una máquina virtual de Azure, lo que permite un monitoreo constante y el envío de alertas en tiempo real.

Capa de Datos: Utiliza variables de entorno almacenadas con dotenv para la configuración segura de credenciales. Además, Dialogflow y Gmail actúan como fuentes de datos para el chatbot y el sistema de notificaciones.

2. Diagrama de Flujo del Sistema:

Inicio de Monitoreo: El módulo de monitoreo analiza el tráfico de red y el contenido de correos electrónicos de manera continua.

Detección de Amenazas: Cuando se detecta una actividad sospechosa, el sistema genera una alerta y activa el módulo de notificación por correo.

Interacción con el Usuario: El usuario recibe la alerta con un enlace "Más información" que abre el chatbot en el frontend, con el mensaje predefinido.

Asesoramiento del Chatbot: El chatbot, al recibir el mensaje de contexto, inicia una conversación y brinda recomendaciones adaptadas a la situación detectada.

*Imagen que contiene Escala de tiempo

Descripción generada automáticamente*

y

## 10. Referencias

[1] Cota, I., Cota, I., & Cota, I. (2023, 12 mayo). México está entre los 10 países con más cibercrímenes en el mundo. *El País México*. https://elpais.com/mexico/2023-05-12/mexico-esta-entre-los-10-paises-con-mas-cibercrimenes-en-el-mundo.html

[2] FRAUDES CIBERNÉTICOS Y TRADICIONALES. (s. f.). *La Hacienda*.

Sun. (2024, 18 agosto). WhatsApp: Alertan a adultos mayores por mensajes de estafa. *El Informador :: Noticias de Jalisco, México, Deportes & Entretenimiento*.

[3] https://www.informador.mx/tecnologia/WhatsApp-Alertan-a-adultos-mayores-por-mensajes-de-estafa-20240815-0095.html