MEDIDAS PREVENTIVAS DE CIBERSEGURIDAD QUE DEBE TENER EL ADULTO MAYOR EN COLOMBIA PARA ACCEDER A INTERNET Y SUS SERVICIOS.

CHRISTIAN CAMILO MONTAÑEZ RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

MEDIDAS PREVENTIVAS DE CIBERSEGURIDAD QUE DEBE TENER EL ADULTO MAYOR EN COLOMBIA PARA ACCEDER A INTERNET Y SUS SERVICIOS.

CHRISTIAN CAMILO MONTAÑEZ RAMIREZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

DIRECTOR DE TRABAJO DE GRADO
EDUARD MANTILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., Fecha sustentación

DEDICATORIA

Mi reconocimiento total a Dios Todopoderoso arquitecto y constructor de mi vida. Quién ha sido el artífice directo en obtener este reconocimiento brindándome las estrategias necesarias como iniciativa habilidades productividad y responsabilidad colocando en mi camino adultos mayores idóneas como ustedes porque sin él nada hubiese sido posible gracias

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Quiénes con su trabajo y dedicación continuas nos brindan la oportunidad de estudiar y elaborar al mismo tiempo de igual manera a cada uno de Los tutores y asesores que me acompañaron en el proceso le Reconozco que sin su apoyo y colaboración este logró no hubiese sido posible humanamente.

CONTENIDO

pág.

LISTA DE ILUSTRACIONES

Pág.

GLOSARIO

ACTIVO (asset): Cualquier cosa que tenga valor para un individuo, organización o gobierno.

AMENAZA (threat): Posible causa de falla inesperada, que puede provocar daños para un sistema, individuo u organización.

ATAQUE (attack): Intento de deshabilitar, alterar, exponer, destruir, robar u obtener acceso no autorizado o también de hacer uso no autorizado de algún activo.

CIBERDELITO (cybercrimen): La actividad delictiva en la que se prestan los servicios o algunas aplicaciones en el ciberespacio o en la red o que son el objetivo de algún crimen o donde el ciberespacio es el blanco, herramienta, fuente o el lugar de un delito.

CONTENIDOS MALICIOSOS (malicious contents): Documentos, archivos, aplicaciones datos u otros recursos con características o capacidades dañinas incrustadas, disfrazadas u ocultas.

ESTAFA (scam): Fraude o engaño.

INTERNET (internet / internetwork): Interconexión de las redes o una recopilación de redes que están interconectadas

ORGANIZACIÓN (organization): Grupo de instalaciones y adultos mayores con una destreza de responsabilidades, autoridades y relaciones.

PIRATERÍA INFORMÁTICA (hacking): Acceso intencional a algún sistema informático sin la previa autorización del adulto mayor o del adulto mayor.

SOFTWARE PUBLICITARIO (adware): Aplicación que mientras se ejecuta, despliega publicidad a los adultos mayores o recopilan información de los movimientos o conducta en línea de los
adultos mayores.

SUPLANTACIÓN DE IDENTIDAD (phishing): Operación fraudulenta, donde se intentar adquirir información confidencial o privada de manera sigilosa, haciéndose pasar por alguna entidad de confianza como por ejemplo un banco.

TROYANO (trojan / trojan horse): Software malintencionado que aparenta restar haciendo una función deseable. [1]

[1] ICONTEC, ICONTEC e-Collection, {En Línea}, accedido 9 de mayo de 2022, https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/.

RESUMEN

La elaboración de un estado de arte desempeña un papel fundamental al proporcionar un análisis detallado del panorama actual en relación con las amenazas que enfrentan los adultos mayores al utilizar servicios en línea, así como resaltar la crucial importancia de la ciberseguridad en Colombia. En este contexto, esta monografía se convierte en un faro que ilumina la necesidad apremiante de establecer un manual de recomendaciones específicas dirigido a prevenir el robo de datos personales en este segmento demográfico vulnerable.

El auge de Internet ha transformado la sociedad, pero también ha llevado consigo un incremento en las amenazas cibernéticas, lo cual afecta de manera especial a los adultos mayores debido a sus brechas digitales y falta de familiaridad con las herramientas tecnológicas. Esta vulnerabilidad pone en riesgo sus datos personales y recursos financieros. La ciberseguridad se convierte en un foco prioritario para garantizar su independencia y seguridad en línea.

La normativa en Colombia reconoce la necesidad de proteger a los adultos mayores de los ciberdelitos y promueve medidas para su inclusión digital. La conectividad a Internet es esencial para acceder a servicios esenciales. Sin embargo, la seguridad en línea es fundamental, y es aquí donde entra en juego un manual de recomendaciones de ciberseguridad específicas.

Este manual ofrece directrices clave para prevenir el robo de datos personales y estafas a los adultos mayores colombianos. Las sugerencias, que abordan desde la ingeniería social hasta las amenazas y ataques en línea, son diseñadas para salvaguardar sus datos personales. Adicionalmente, se destaca la importancia de capacitar a un miembro de la familia o amigo cercano en las prácticas de seguridad digital, lo que fomentará una adopción más segura de la tecnología y contribuirá a incrementar el número de adultos mayores en la era digital.

El manual no solo provee medidas de seguridad, sino que también aborda la necesidad de una educación continua en ciberseguridad. Con un enfoque en la inclusión y el desarrollo, este recurso se convierte en un paso crucial para cerrar la brecha digital que los adultos mayores han enfrentado durante años. Al empoderarlos con las herramientas para navegar el mundo en línea de manera segura, se promueve su participación en la sociedad moderna.

PALABRAS CLAVES: Adulto mayor, Amenaza, Ciberataque, Manual de funciones, Recomendaciones.

ABSTRACT

The development of a state-of-the-art report plays a fundamental role in providing a detailed analysis of the current landscape in relation to the threats that older adults face when using online services, as well as highlighting the crucial importance of cybersecurity in Colombia. In this context, this monograph becomes a beacon that illuminates the urgent need to establish a manual of specific recommendations aimed at preventing the theft of personal data in this vulnerable demographic segment.

The rise of the internet has transformed society, but it has also led to an increase in cyber threats, which particularly affects older adults due to their digital gaps and lack of familiarity with technological tools. This vulnerability puts their personal data and financial resources at risk. Cybersecurity becomes a priority focus to ensure their independence and security online.

Colombian regulations recognize the need to protect older adults from cybercrime and promote measures for their digital inclusion. Internet connectivity is essential to access essential services. However, online security is essential, and this is where a manual of specific cybersecurity recommendations comes into play.

This manual provides key guidelines to prevent the theft of personal data and scams to Colombian older adults. The suggestions, which address from social engineering to online threats and attacks, are designed to safeguard their personal data. Additionally, the importance of training a family member or close friend in digital security practices is highlighted, which will encourage safer adoption of technology and help to increase the number of older adults in the digital age.

The manual not only provides security measures, but also addresses the need for ongoing cybersecurity education. With a focus on inclusion and development, this resource becomes a crucial step towards closing the digital gap that older adults have faced for years. By empowering them with the tools to navigate the online world safely, their participation in modern society is promoted.

KEYWORDS: Cyberattack, Elderly, Recommendations, Threat.

INTRODUCCIÓN

El acceso a internet ha revolucionado la vida de las personas de todas las edades, pero los adultos mayores se han beneficiado especialmente de este avance tecnológico. Internet ha permitido a los adultos mayores mantenerse en contacto con sus seres queridos, aprender cosas nuevas, participar en actividades sociales y acceder a servicios gubernamentales y de atención médica.

Sin embargo, el acceso a internet también ha expuesto a los adultos mayores a nuevos riesgos, como los delitos cibernéticos. Los delitos cibernéticos son un tipo de delito que se comete utilizando las tecnologías de la información y la comunicación. Estos delitos pueden incluir el robo de identidad, el fraude financiero, el chantaje y la suplantación de identidad.

Los adultos mayores son más vulnerables a los delitos cibernéticos que otros grupos de edad por varias razones. En primer lugar, los adultos mayores suelen tener menos conocimientos sobre las tecnologías de la información y la comunicación. Esto los hace más susceptibles a las estafas y engaños perpetrados por los ciberdelincuentes. En segundo lugar, los adultos mayores suelen tener más información personal y financiera disponible en línea. Esta información es un objetivo atractivo para los ciberdelincuentes, que pueden utilizarla para cometer fraude o robar dinero.

Para ayudar a los adultos mayores a protegerse de los delitos cibernéticos, es importante que ellos conozcan los riesgos y que tomen medidas para protegerse. Algunas de las cosas que los adultos mayores pueden hacer para protegerse de los delitos cibernéticos incluyen:

- Usar contraseñas seguras y únicas para cada sitio web.
- No compartir su información personal con desconocidos.
- Ser escéptico sobre los correos electrónicos y los mensajes de texto que le piden información personal.
- Mantener sus dispositivos actualizados con el software de seguridad más reciente.
- Instalar un antivirus en sus dispositivos.
- Ser consciente de las señales de alerta de los delitos cibernéticos.
- Si sospecha que ha sido víctima de un delito cibernético, debe denunciarlo a las autoridades.

Los delitos cibernéticos son un problema grave, pero hay medidas que los adultos mayores pueden tomar para protegerse. Al conocer los riesgos y tomar medidas para protegerse, los adultos mayores pueden ayudar a mantener sus datos personales y financieros seguros.

Además de las medidas de seguridad mencionadas anteriormente, los adultos mayores también pueden protegerse de los delitos cibernéticos participando en programas de educación y capacitación sobre seguridad cibernética. Estos programas pueden enseñar

a los adultos mayores sobre los riesgos de los delitos cibernéticos, cómo identificar los fraudes y cómo proteger sus datos personales y financieros.

Los adultos mayores también cuentan con recursos disponibles para resguardarse de los delitos cibernéticos provenientes de sus seres queridos y amistades. Estos individuos cercanos tienen la posibilidad de asistir a los adultos mayores en la selección de contraseñas robustas, en la actualización constante de sus dispositivos con las más recientes herramientas de seguridad, así como en la instalación de programas antivirus y firewalls. Adicionalmente, tienen la capacidad de orientar a los adultos mayores en la identificación de las señales de alerta asociadas a los crímenes cibernéticos y en la ejecución de denuncias ante las autoridades pertinentes.

Mediante la colaboración de los adultos mayores, sus familiares y amigos, es plausible reducir significativamente el riesgo vinculado a los delitos cibernéticos. Resulta esencial proporcionar los medios necesarios para garantizar la seguridad en el acceso. Por ello, esta monografía se fundamenta en un análisis exhaustivo de diversas fuentes bibliográficas de índole científica y periodística, con el propósito de arrojar claridad sobre el panorama actual de los delitos cibernéticos que impactan en la integridad de los datos personales de este segmento poblacional.

Para llevar a cabo esta labor, resulta imperativo contar con información proveniente de fuentes confiables, las cuales aborden de manera integral los delitos cibernéticos y sus múltiples facetas, incluyendo estrategias para su prevención, tal y como se delinean en las recomendaciones presentes en esta monografía.

1. DEFINICIÓN DEL PROBLEMA

1.1.1 ANTECEDENTES DEL PROBLEMA

El acceso a internet ha evolucionado con el transcurso de los años, por lo que ha aumentado el número de usuarios que utilizan la red y sus servicios, entre ellos aquellas generaciones que en su momento no tenían acceso al mundo digital, como lo es la población del adulto mayor que en su generalidad son personas que no crecieron con la tecnología, por lo cual el manejo de este tipo de herramientas se les dificulta, al ser algo totalmente nuevo y al cual se han venido adaptando paulatinamente.

En razón a lo anterior, podemos encontrar diferentes estadísticas que revelan que los adultos mayores en los últimos años han incrementado el uso de las nuevas tecnologías y con ello el acceso a internet, tal como lo ha señalado el DANE en un conversatorio realizado por la subdirección para la vejez de la secretaria distrital de integración social, para el año 2021 el 40,9% de las personas que tienen edades superiores a los 60 años, utilizan dispositivos electrónicos para acceder a internet.[2]

Aunado a lo anterior, se evidencio con la pandemia causado por el virus COVID – 19, y por el aislamiento que esta conllevo a que los adultos mayores se vieron obligados a usar este tipo de herramientas tecnológicas, por lo que se aumentó el acceso a internet por parte de esta población, encontrándose que, en la actualidad, la gran mayoría usan a diario estos recursos.

Considerando el vertiginoso aumento en la adopción de Internet entre los adultos mayores, diversos expertos en seguridad informática anticipan los desafíos emergentes en el ámbito de la ciberseguridad para este año, así como las tendencias que se perfilan para abordarlos, donde se destaca la aparición inminente de nuevos modelos de extorsión y una reinvención del ransomware. Estas amenazas afectarán a cualquier individuo que haga uso de dispositivos electrónicos con conectividad a Internet. Además, es previsible que los servicios de datos móviles expandan su alcance más allá de las redes locales y conexiones Wi-Fi, brindando así cobertura constante en cualquier momento.[3]

1.1.2 PLANTEAMIENTO

El aumento permanente en las amenazas informáticas es un fenómeno que se ha venido observando en los últimos años. Este crecimiento está relacionado con el aumento del acceso al internet y sus servicios, lo que ha hecho que un mayor número de personas y sobre todo los adultos mayores estén expuestas a estas amenazas.

---

[2] DANE, Encuesta de Tecnologías de la Información y las Comunicaciones en Hogares (ENTIC Hogares), accedido 10 de diciembre de 2022, https://www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/tecnologias-de-la-informacion-y-las-comunicaciones-tic/encuesta-de-tecnologias-de-la-informacion-y-las-comunicaciones-en-hogares-entic-hogares.

[3] BUENO. Laura, Ciberseguridad en Colombia, avances y retos, 2022, 20 p.

En este contexto, los especialistas señalan dos nuevas tendencias que representan desafíos importantes para la ciberseguridad: la reinvención del ransomware y el aumento del campo de acción de las amenazas.

El ransomware es un tipo de malware que bloquea el acceso a los datos de una computadora o sistema informático. Los atacantes luego exigen un rescate a cambio de desbloquear los datos. En los últimos años, el ransomware ha evolucionado para volverse más sofisticado y difícil de detectar. Los atacantes ahora utilizan técnicas como el phishing y el malware para infectar a las víctimas.[4]

¿Qué medidas de ciberseguridad deben tomar los adultos mayores colombianos cuando utilizan el internet y sus servicios?

[4] ROJAS VILLALOBOS. Bernal, Aprendizaje por defensa reactiva: el nuevo modelo de entrenamiento contra malware, 2021, 16 p.

2 JUSTIFICACIÓN

Los ciberataques son una amenaza creciente para todas las personas, independientemente de su edad, condición social o ubicación. Compañías, instituciones públicas, hospitales, entidades financieras y adultos mayores son todos vulnerables a estos ataques.

En los últimos años, se han producido varios casos de filtración de datos de adultos mayores, lo que ha dejado expuesta su información personal, como números de tarjetas de crédito, direcciones de correo electrónico y contraseñas. Esta información puede ser utilizada para extorsionar a las víctimas, robar sus cuentas bancarias o incluso secuestrarlas.

Los adultos mayores son un grupo vulnerable a los ciberataques. Por ello, es necesario tomar medidas para protegerlos. Esta monografía propone recomendaciones para mejorar el tratamiento de los datos personales de los adultos mayores en internet. Estas recomendaciones buscan minimizar los errores cometidos al proporcionar información personal, como contraseñas y datos financieros.

En mi rol como estudiante de seguridad informática, subrayo la vitalidad de salvaguardar a los adultos mayores. Con ese propósito, ofrezco recomendaciones que robustecen su ciberseguridad, enriqueciendo la visión de las estrategias, planes y buenas prácticas que se deben implementar los adultos mayores con acceso a internet en Colombia.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar las amenazas a las que se encuentra expuesto el adulto mayor en Colombia al utilizar internet y sus servicios, por medio de una revisión sistemática de literatura para proponer medidas preventivas de ciberseguridad en esta población.

3.2 OBJETIVOS ESPECÍFICOS

- Construir el estado del arte sobre las amenazas a las que se encuentra expuesto el adulto mayor al utilizar los servicios del internet.

- Examinar la normatividad vigente en Colombia referente a los lineamientos de seguridad digital de los ciudadanos.

- Proponer un manual de recomendaciones y medidas de ciberseguridad para prevenir el hurto de datos personales a los adultos mayores en Colombia.

4 MARCO REFERENCIAL

En este capítulo, se abarcarán los conceptos básicos para tener en cuenta en el desarrollo de la monografía. Donde se busca esclarecer los conceptos relevantes de la seguridad informática centrada en la protección de Información, vulnerabilidades, amenazas comunes de seguridad informática y medidas preventivas de ciberseguridad de los adultos mayores que acceden a internet y sus servicios.

4.1 MARCO TEÓRICO

El DANE, realizo una proyección del crecimiento de la población adulto mayor, analizando los años de 1985 a 2020 y en los resultados publicados se encontró que en Bogotá el porcentaje de personas con edad de 59 años se encontraba en el año 1985 en el 7% y paso al 10% en 2010, proyectando que en el año 2020 esta alcanzará un total del 13%, adicionalmente revelo que para el año 2011 en Bogotá hay 743.572 personas mayores de 59 años.

La ONU en recientes estudios ha determinado que el mundo se encuentra envejeciendo toda vez que el 22% de los habitantes para el año 2050 tendrán más de 60 años, lo que trae consigo modificaciones importantes a nivel social, cultural y económicas, en todo el mundo, encontrándose Colombia en la misma situación, tal como lo revelo el DANE, puesto que las edades de primera infancia, adolescentes, edades productivas, están presentando un porcentaje menor de crecimiento, frente a la población de la tercera edad.

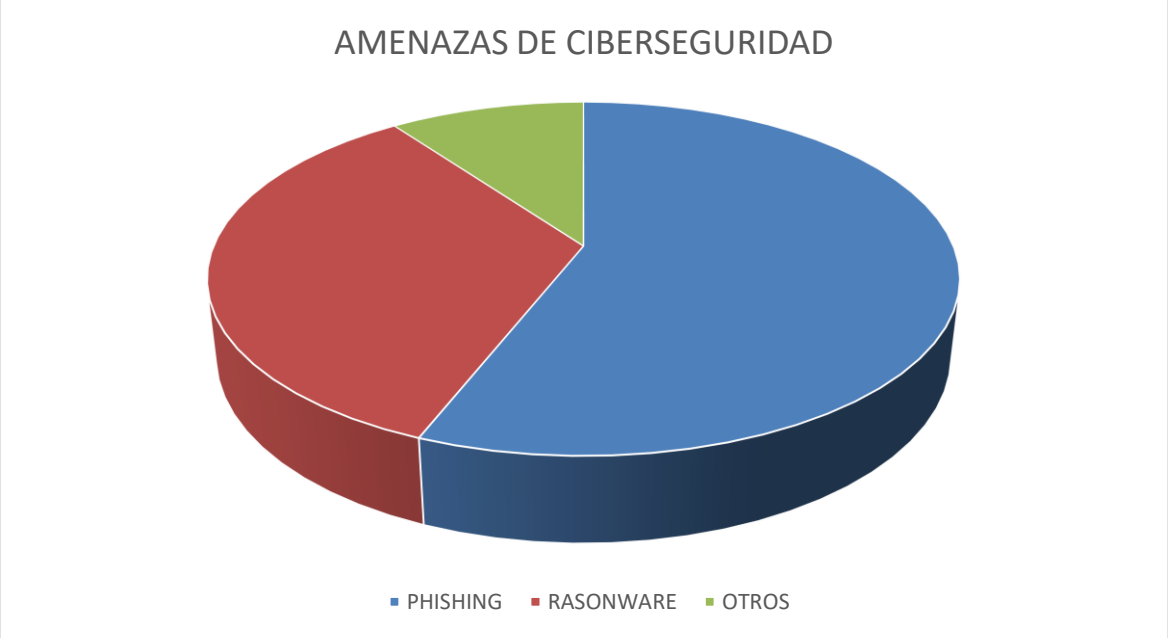
En el año 2019 el MINISTERIO DE LA TELECOMUNICACIONES implemento un programa piloto denominado alfabetización digital al adulto mayor, en el cual buscaba capacitar a dicha población en el acceso a internet, herramientas digitales y sus diferentes servicios, con lo cual logro certificar a 100 personas, generando con esto un incremento en la población que actualmente utiliza estas redes en su diario vivir, con los beneficios y riesgos que esto conlleva.[5]

Para el 2021 se presentaron más de 41 mil millones de intentos de ciberataques a nivel mundial, 7 mil millones de ellos en Colombia. A medida que el delito cibernético genera ganancias cada vez mayores para los atacantes, la curva de ataques cibernéticos para los usuarios como lo son los adultos mayores seguirá creciendo sin las herramientas para contrarrestarlos y defenderse de ellos. Según el último informe presentado por la Fiscalía General de la Nación, el número de ciberataques en Colombia aumentará un 30% en 2021 con respecto al año anterior. Si bien las empresas y organismos oficiales han trabajado arduamente para desarrollar estrategias para fortalecer las medidas de ciberseguridad, no es suficiente, y menos para la población del adulto mayor, quienes no tienen las herramientas ni el conocimiento necesario para protegerse.

[5] MINTIC, Adultos mayores salieron del analfabetismo digital y entraron al mundo de las TIC, accedido 11 de diciembre de 2022, http://www.mintic.gov.co/portal/715/w3-article-124707.html.

Según un informe del portal web de grupo semana sobre las tendencias de seguridad, para los colombianos las principales preocupaciones también incluyen amenazas de ingeniería social, llamadas phishing, con un 56%, a través del cual el adulto mayor es engañado al hacerle creer que ingresa a un sitio seguro cuando no lo es. Con este mismo porcentaje (56%), las empresas temen los ataques de negación del servicio (dos), que atacan directamente un sistema informático o una red, lo que lo hace inaccesible para sus empleados. Y los peligros asociados con el Ransomware, mejor conocido como "secuestro de datos" con un (34%).[6]

Figura 1 Amenazas De Ciberseguridad



Fuente: https://www.semana.com/tecnologia/articulo/como-evitar-los-ataques-ciberneticos-y-el-secuestro-de-datos/202238/.

En razón a lo expuesto, es evidente que la población de los adultos mayores va tomando un incremento importante, al igual que los ciberataques, por lo que se incrementa la necesidad de garantizar un acceso correcto y sin amenazas a internet y sus servicios.

4.2 MARCO CONCEPTUAL

4.2.1 ATAQUE INFORMÁTICO

Método que aprovecha a un individuo para explotar las debilidades o las vulnerabilidades en sistemas informáticos para tratar de tomar el control, causar daños o simplemente desestabilizar un sistema informático, causando efectos negativos en la seguridad del sistema.[7]

[6] BENAVIDES. Blackwood, El fraude electrónico, 2022, 22 p.
[7] GONZÁLEZ. Edwin Mauricio, Actualidad de Colombia en seguridad de la información, 2014, 6 p.

Figura 2. Fases de un Ataque Informático.

Fuente: Elaboración propia.

4.2.1.1 RECONOCIMIENTO

En esta fase, se obtiene toda la información necesaria del objetivo y/o la víctima que puede ser un adulto mayor, antes de lanzar un ataque. Consiste en 2 tipos de reconocimiento pasivo y activo.

El reconocimiento pasivo es cuando la información se adquiere sin tener una interacción directa al objetivo, Se puede utilizar la piratería de Google, la ingeniería social, el monitoreo de las redes de datos. Por ejemplo, sniffing, etc.

El reconocimiento activo se da cuando se tiene una interacción directa con el posible objetivo, es decir que el atacante envía un tipo de acción en busca de una respuesta que por lo general lo logra. La red se prueba para detectar hosts accesibles, la ubicación de los enrutadores, puertos abiertos, los detalles de los sistemas operativos y de los servicios. Esta fase puede llevar mucho tiempo, porque se analiza toda la información obtenida y se crea una estrategia para lanzar el ataque con mayor precisión.

4.2.1.2 EXPLORACIÓN

En esta fase, se emplea la información obtenida en la fase anterior, identifica debilidades específicas. Un ejemplo muy claro es que si en la Fase 1. El atacante descubre que su objetivo usa Windows 7 como sistema operativo, buscará vulnerabilidades para dicho sistema y saber dónde atacarlo.

4.2.1.3 OBTENER ACCESO

Esta fase es la más importante porque el ataque comienza a materializarse gracias a la explotación de las debilidades y las deficiencias del sistema descubierto en las fases señaladas con antelación de reconocimiento y exploración. La explotación de

vulnerabilidades suele generarse localmente, esto es sin estar conectado, a una red local en internet. Para hacer esto, las herramientas especialmente diseñadas para este propósito generalmente se conocen como exploit.

4.2.1.4 MANTENER ACCESO

El atácate en esta fase ya obtuvo acceso al sistema y su prioridad es mantenerlo el máximo tiempo posible, donde buscará mecanismos que le permitan continuar accediendo en un futuro cercano, en el momento que tenga acceso a Internet. Para hacer esto, generalmente usan técnicas como las backdoors (puertas traseras), rootkits (encubridor) y trojans (troyanos) para acceder a cuentas de adultos mayores con privilegios administrativos que facilitan el acceso al atacante posterior al sistema afectado. Para causar más daños a la víctima, controlando el sistema que ya ha logrado acceder.

4.2.1.5 BORRAR HUELLAS

En esta fase, el atacante intentará borrar toda la evidencia de cualquier posible rastro de sus actividades realizadas durante la intrusión para evitar ser detectados por el profesional de seguridad o los administradores de la red, para continuar accediendo al sistema atacado cuando tú deseas. Además, es importante borrar las huellas para cancelar la posibilidad de ser capturado.[8]

4.2.1.6 TIPOS DE ATAQUES

Un ataque es una acción que intenta aprovechar una vulnerabilidad de un sistema informático para tener alguna clase de impacto e incluso tomar el control, estas son acciones intencionales y fortuitas que pueden poner en peligro a un sistema.

ATAQUES PASIVOS: En este tipo de ataques, el atacante en lugar de modificar la conexión, simplemente la escucha o monitorea, con el fin de esta forma recolectar la información transmitida.

- **Sniffing:** Consiste en recopilar el tráfico de la red para posteriormente obtener datos, tales como la dirección IP, la dirección MAC, la cuenta de correo electrónico, la contraseña, e información importante del adulto mayor, etc.

- **Análisis de tráfico** Incluye recopilar los datos que la red genera, mediante el análisis del tráfico y sus patrones, por ejemplo, al ser encendidos ciertos dispositivos, qué tráfico se envía, cuándo hay más tráfico disponible, etc.

ATAQUES ACTIVOS: Estos ataques generan un tipo de modificación en el flujo de información trasmitida o la creación de un flujo de datos falso

[8] CONDORI. José Luis, Fases de un ataque a un Sistema Informático, 2020, 52-55 p.

- **Suplantación:** un intruso que se hace pasar por otra entidad.

- **Reproducción:** Uno o más mensajes legítimos se graban y repiten para producir efectos no deseados.

- **Modificación:** Se modifica parte del aviso legal, se retrasan o reprograman los avisos.

- **Degradación del servicio:** Impidiendo o restringiendo la utilización de los medios informáticos y de comunicaciones.

4.2.2 SEGURIDAD DE LA INFORMACIÓN

Se basa en el resguardo de la información con el fin de mantener la disponibilidad, integridad y confidencialidad, de la misma forma que el tratamiento de los sistemas dentro de una entidad. Para asegurarse de que se administre adecuadamente, se debe llevar a cabo un procedimiento documentado, confiable, conocido y sistemático en toda la entidad, este proceso que constituye un SGSI.

4.2.2.1 INTEGRIDAD

Este principio garantiza que la información sea correcta, completa, sin modificaciones o modificaciones de su contenido, Se protege frente a vulnerabilidades externas o posibles errores humanos.

4.2.2.2 CONFIDENCIALIDAD

Su objetivo es evitar el uso no autorizado de la información, por personas que no están facultadas para este propósito. Esto significa que estos datos solo deben ser conocidos solo por un grupo o usuario individual, definidos por la persona responsable de la información.

4.2.2.3 DISPONIBILIDAD

Este principio garantiza que los adultos mayores tengan acceso oportuno y confiable a sus recursos de información, lo que permite la continuidad de las actividades.[9]

[9] GUAÑA. Javier, Ataques informáticos más comunes en el mundo digitalizado, 2022, No. E54, 87-100 p.

4.3 MARCO HISTÓRICO

4.3.1 HISTORIA DEL CIBERCRIMEN

La historia del cibercrimen se remonta al siglo XX, cuando se comenzaron a desarrollar los primeros sistemas informáticos. Los primeros delitos informáticos fueron relativamente simples, como el uso de teléfonos públicos sin pagar o el acceso no autorizado a sistemas informáticos. Sin embargo, a medida que la tecnología informática se ha desarrollado, también lo han hecho los delitos informáticos.[10]

Las siguientes son algunas fechas importantes en la historia del cibercrimen:

- 1958: Joseph Carl Robnett Licklider, un científico informático estadounidense, acuñó el término "cibernauta" para referirse a una persona que navega por el ciberespacio.
- 1969: Se crea la ARPANET, la primera red informática de área amplia.
- 1971: El estudiante de la Universidad de California, Berkeley, John Draper, conocido como "Captain Crunch", descubre cómo hacer llamadas telefónicas gratuitas usando un dispositivo llamado "caja de cereal".
- 1973: El grupo de piratería informática conocido como "The 414s" comienza a operar.
- 1978: El gobierno de Estados Unidos aprueba la Ley de Fraude y Abuso Informático (CFAA).
- 1981: El estudiante de la Universidad de California, Irvine, Ian Murphy, es condenado por el primer delito cibernético de la historia.
- 1983: El virus informático Creeper se propaga por la ARPANET.
- 1988: El gusano informático Morris se propaga por Internet, causando daños por valor de millones de dólares.
- 1995: Los hermanos Kevin, Dennis y Ronald Mitnick son condenados por una serie de delitos cibernéticos, incluido el acceso no autorizado a sistemas informáticos y el robo de información confidencial.
- 1996: Se crea la Organización Internacional de Policía Criminal (Interpol) la División de Cibercrimen.

[10] RUIZ. Claudia Bibiana, Los ciberdelito y la ciberseguridad: una cuestión de género, 2023, No. 13, 73-84 p.

- 1998: Se crea la Comisión Europea la Oficina Europea de Policía (Europol) la Unidad de Cibercrimen (EC3).
- 2000: Se crea el Centro Nacional de Coordinación para la Prevención, Detección e Investigación de Delitos Informáticos (INCIBE) en España.
- 2001: El ataque terrorista del 11 de septiembre de 2001 lleva a un aumento de la preocupación por la seguridad cibernética.
- 2003: Se crea el Departamento de Seguridad Nacional de Estados Unidos (DHS).
- 2005: Se crea la Agencia de Ciberseguridad de Estados Unidos (CISA).
- 2007: El virus informático Stuxnet se propaga por Internet, causando daños a las instalaciones nucleares de Irán.
- 2010: El ataque cibernético de los Estados Unidos a Irán, conocido como Operación Olympic Games, es descubierto.
- 2013: Edward Snowden revela el programa de vigilancia global de la Agencia de Seguridad Nacional de Estados Unidos (NSA).
- 2014: El ataque cibernético a Sony Pictures Entertainment es llevado a cabo por el grupo de hackers Guardians of Peace.
- 2015: El ataque cibernético a Target, una cadena de tiendas de descuento, roba información personal de 110 millones de clientes.
- 2016: El ataque cibernético a las elecciones presidenciales de Estados Unidos es llevado a cabo por el grupo de hackers Fancy Bear.
- 2017: El ransomware WannaCry se propaga por Internet, infectando más de 200.000 computadoras en 150 países.
- 2018: El ataque cibernético a Equifax, una agencia de crédito, roba información personal de más de 145 millones de personas.
- 2020: La pandemia de COVID-19 lleva a un aumento de los ataques cibernéticos dirigidos a empresas y organizaciones sanitarias.

4.3.2 CIBERATAQUES EN COLOMBIA.

- 2008: Un ciberataque al Ministerio de Hacienda de Colombia roba información sobre impuestos y recaudación.
- 2011: Un grupo de piratas informáticos conocidos como "Los Rastrojos" hackean el sitio web del Banco de la República de Colombia y roban información sobre cuentas bancarias.

- 2014: Un equipo de hackers consiguieron transferir alrededor de $160.000 millones a unas 360 cuentas vinculadas a Bancolombia. Sin embargo, debido a las sólidas medidas de seguridad interna del banco, los delincuentes únicamente pudieron acceder al 4% de los fondos que tenían como objetivo sustraer.

- 2016: Un ciberataque a la empresa de telecomunicaciones Claro roba información personal de más de 10 millones de clientes.

- 2017: Un ciberataque a la empresa de energía Electricaribe roba información personal de más de 2 millones de clientes.

- 2020: Un ciberataque al Ministerio de Salud de Colombia roba información personal de más de 50 millones de colombianos.

- 2021: En noviembre, el Departamento Nacional de Estadísticas de Estadísticas de Colombia fue comprometido por un ataque informático. Los atacantes continuaron eliminando los sistemas de procesamiento estadístico y las bases de datos con información reservada y con "información confidencial".

- 2022: Un ciberataque a la empresa de servicios públicos Emcali roba información personal de más de 1 millón de clientes.

4.4 ANTECEDENTES O ESTADO ACTUAL

Ciberseguridad en Colombia: un desafío creciente la ciberseguridad es un tema de gran relevancia en Colombia, ya que el país ha sido víctima de numerosos ciberataques en los últimos años. En 2022, Colombia recibió 20.000 millones de intentos de ciberataques, un aumento del 80% con respecto al año anterior.

Estos ataques buscan explotar las vulnerabilidades de los sistemas informáticos para robar información sensible, extorsionar a las víctimas o causar daños en la infraestructura crítica.

La ciberseguridad es un desafío creciente para Colombia, ya que el país es cada vez más dependiente de la tecnología. Es importante que las empresas, organizaciones y ciudadanos tomen medidas para proteger sus sistemas y datos de los ciberataques.[11]

[11] CASTAÑEDA. Marlon Stiven, Panorama de Ciberataques más Recurrentes en Colombia 2021 y 2022, 2022, 6 p.

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

La pandemia de COVID 19 ha acelerado la transformación digital. Internet se ha convertido en un gran aliado para quienes quieren desarrollar su negocio. Un perfil activo en el sitio web y las redes sociales nos ayuda a aumentar la visibilidad y atraer a más clientes potenciales, lo que a su vez genera nuevas oportunidades de negocio. Además, la conexión a Internet y la transformación digital te permiten llevar tu catálogo contigo a cualquier parte del mundo. La generación de nuevas ideas debe ser una rutina, ya que los cambios tecnológicos constantes requieren mantenerse al día con los últimos desarrollos y la comunicación entre ambos se vuelve más fluida.[12]

La transformación digital no se basa solo de tecnología, si no que se trata de adultos mayores, cultura y cambio. Es importante empoderar a esta población por medio de estrategias de capacitación, motivación, formación, apoyo, trabajo en red y equipos de alto rendimiento que se alineen con la visión y la misión de la transformación digital. Seguir esta nueva cultura aumentará su productividad y que mantengan en contacto con sus familiares y amigos, al igual que lo hace la población joven, obteniendo una mejor calidad de vida.[13]

4.6 MARCO LEGAL

Con la nueva Constitución de Colombia de 1991, se incluyó en el artículo 46: “El Estado, la sociedad y la familia concurrirán para la protección y la asistencia de las personas de la tercera edad y promoverán su integración a la vida activa y comunitaria”[14].

Para el año 1995 por parte del Departamento Nacional de Planeación se promulgo el Copes 2793 Envejecimiento y vejez, mediante el cual se establecen medidas para la atención a la vejez y a las condiciones básicas que se le deben garantizar a las personas de la tercera edad en Colombia. Desde dicho momento los proyectos, planes y políticas se refieren a las personas de mayor edad como “Tercera Edad” o “Adulto Mayor”.

En el 2001 se realizaron tres foros en los cuales se tocaron los temas de vejez y envejecimiento, por parte de la Agencia Colombiana de Cooperación Internacional y la Fundación Santillana para Iberoamérica realizando la “Agenda sobre Envejecimiento. Colombia Siglo XIX” donde destaca como necesidad construir una sociedad para todos, esto es sin discriminar las edades

[12] DIAZ CANCECO. Terry, Transformación digital en la educación en tiempos del covid-19, 2020, 36 p.
[13] BAYONA ACEVEDO. Leydis, La transformación digital de las empresas colombianas en los últimos 5 años, 2022, 24 p.
[14] COLOMBIA. CONGRESO DE LA REPUBLICA. Constitución Política de Colombia 1991. (6, julio, 1991). Gaceta Constitucional. Bogotá DC. No. 116. Art. 46.

En el 2007 se publicó la Política Nacional de envejecimiento y Vejez (2007-2019) encaminado al propender por una vejez activa y la protección integral de esta población, de sus derechos humanos, elaborada por el Ministerio de la Protección Social.

En el año 2008 el Congreso de la República de Colombia aprobó la Ley 1251 “por el cual se dictan normas tendientes a procurar la protección, promoción y defensa de los derechos de los adultos mayores”.

En el 2012, Colombia participo en la tercera conferencia sobre envejecimiento, llevada a cabo en Costa Rica, en la cual se definieron acciones para proteger los derechos humanos de los adultos mayores y su inclusión y desarrollo en el mundo actual, esto se denominó la Carta de San José sobre los derechos de las personas mayores de américa latina y el caribe.

Las leyes más recientes sobre ciberseguridad y adultos mayores en Colombia son las de 2022 por la cual se establece la Política Nacional de Ciberseguridad para la protección de la población adulta mayor y la del presente año 2023 bajo resolución 000214 de 2023 por la cual se adopta el Plan Nacional de Acción para la Protección de la Población Adulta Mayor en el Ciberespacio. Esta resolución fue expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) el 22 de febrero de 2023.

5 DESARROLLO DE LOS OBJETIVOS

5.1 DESARROLLO DE OBJETIVO 1

- Construir el estado del arte sobre las amenazas a las que se encuentra expuesto el adulto mayor al utilizar los servicios del internet.

5.1.1 AMENAZAS

5.1.1.1 GUSANOS

Los adultos mayores deben de tener cuidado con los gusanos informáticos por que se propagan con facilidad como por ejemplo en archivos adjuntos, en enlaces web, a través de redes compartidas P2P como lo que era la aplicación de ARES en su época.

Este es un programa que hace una copia de sí mismo y se propaga por la red cuando una computadora se infecta. A diferencia de los virus, puede distribuirse a través de una red o correo electrónico, por lo que no se requiere la intervención del Adulto mayor. Están diseñados para irradiar e infectar otros equipos y en principio, no afectan al funcionamiento normal del sistema y son difíciles de detectar, su uso principal es crear una red zombi (botnet) que se utiliza para realizar operaciones de forma remota, como ataques de denegación de servicio (DoS).[15]

Figura 3. Gusano

Fuente: https://www.laopinion.com.co/tecnologia/que-es-un-gusano-informatico

[15] GONZÁLEZ. Jesús Audelo, Gusanos informáticos, 2015, 8 p.

5.1.1.2 TROYANO

En la mayoría de los casos, los adultos mayores generalmente no pueden detectar infecciones en sus computadoras por sí mismos a menos que usen una solución como la que es un buen antivirus. Al parecer, los gusanos y troyanos no suelen revelar su existencia, es muy raro que algunos troyanos informen a los usuarios de que su ordenador o dispositivo está infectado. De hecho, los troyanos suelen instalarse sigilosamente en el sistema y utilizan técnicas especiales para ocultarse y llevar a cabo sus actividades sin ser detectados. Por lo tanto, la infección solo puede probarse mediante pruebas circunstanciales.[16]

Este último es tan autodestructivo como un virus, pero los troyanos intentan abrir puertas traseras para facilitar la intrusión de otros programas maliciosos. Con el fin de infiltrarte en el sistema sin que te detecten como lo que es una amenaza potencial. Este no se propaga por sí solo y a menudo, se suelen incluir en ejecutables supuestamente inofensivos.[17]

Figura 4. Troyano

Fuente: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/recomendaciones-ante-evolucion-del-malware-troyano-emotet

[16] CALDERON OJEDA. Andrea Carolina, Prototipo de software de administración remota, 2020, 68 p.
[17] HERRERA RODRÍGUEZ. Marcel, Desarrollo de análisis de riesgos aplicado a los troyanos backdoor en un equipo windows simulado, 2021, 52 p.

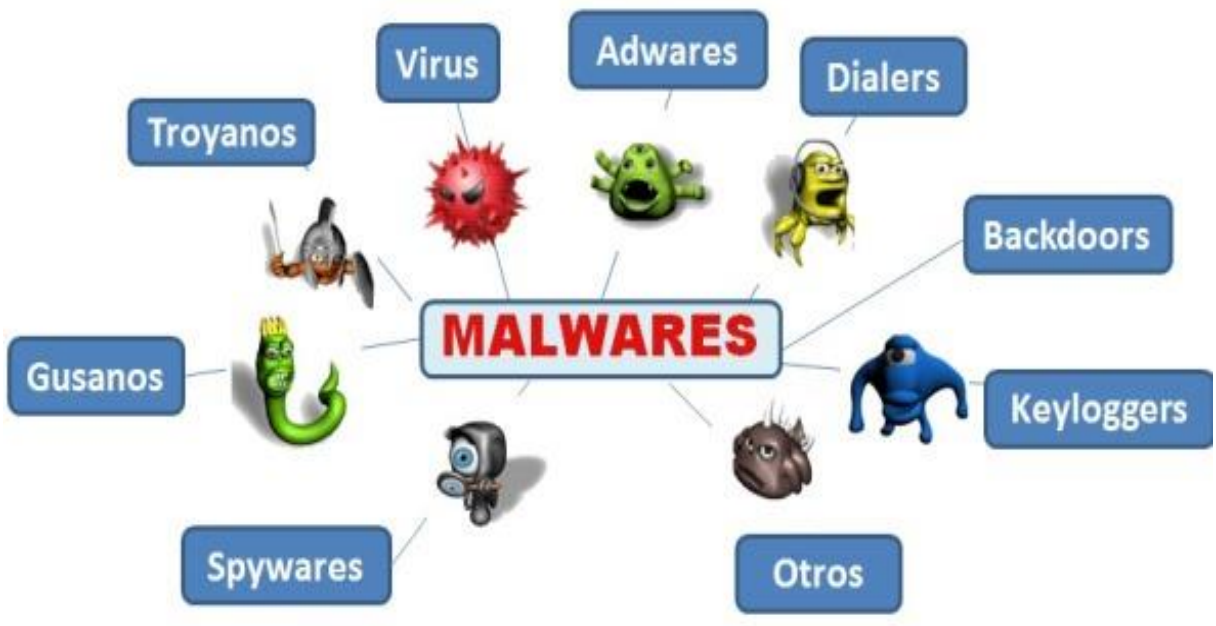
5.1.1.3 MALWARE

El término "malware" se puede decir que es la combinación de la palabra software con la palabra malware este término es usado para describir cualquier programa malicioso instalado en algún dispositivo móvil o PC, dicho malware se instala sin el consentimiento del adulto mayor algunos de los efectos negativos pueden variar, como lo que sería una disminución del rendimiento de algún dispositivo, obtener algunos datos personales de los sistema, también pueden eliminar algún dato o información, incluso afectar negativamente el funcionamiento del hardware indispensable para el uso normal de algún dispositivo.

El mercado del malware está explotando a medida que los piratas informáticos desarrollan métodos cada vez más sofisticados para infiltrarse en los sistemas de los adultos mayores.[18]

El término generalmente se refiere al software malicioso destinado a entrar en un sistema para dañarlo. Los virus, gusanos y troyanos son tipos de programa maligno comúnmente asociados.[19]

Figura 5. Malware



Fuente: https://haitamh.wordpress.com/3-malware/

[18] TAMAYO ARIAS. Johnny Alexander, Mitos y realidades de los virus informáticos, 2002, 8 p.
[19] GUILABERT. Natalia, Actividades cotidianas de los jóvenes en Internet y victimización por malware, 2016, No. 22, 48-61 p.

5.1.1.4 VIRUS

Uno de los clásicos ciberataques que la mayoría de los adultos mayores han sufrido de una forma u otra es un virus informático, un software malicioso diseñado para cambiar el comportamiento de cualquier dispositivo sin el permiso del Adulto mayor y que tiene el potencial de causar estragos, el primer registro fue en 1971 a pesar de ser una de las amenazas más antiguas sus cifras van en aumento.[20]

Este es un código que suele infectar los archivos del sistema a través de programas maliciosos que los Adultos mayores necesitan ejecutar directamente. Una vez habilitado, se extiende a todo lo que puede acceder una computadora o una cuenta de correo, desde los dispositivos de hardware hasta las unidades virtuales y las ubicaciones remotas en la red. [21]

Figura 6. Virus

Fuente: https://sites.google.com/site/seguridadinformaticatamaranr/seguridad-en-la-maquina/virus

[20] YANSENIS LÓPEZ. Matachana, Los virus informáticos: una amenaza para la sociedad, 2020, 33 p.
[21] ARANGO GOMEZ. Oscar Dario, El ABC de la seguridad informática: guía práctica para entender la seguridad digital, 2023, 93 p.

5.1.1.5 SPYWARE

Es un software espía o software malicioso que intenta ocultarse mientras registra información en secreto y rastrea sus actividades en línea en computadoras y dispositivos móviles pertenecientes a los adultos mayores. Los Spyware pueden monitorear y copiar todo lo que escribes, subes, descargas y guardas. Algunos spyware también pueden activar cámaras y micrófonos para verlo y escucharlo sin su conocimiento.[22]

Los spyware tienen como objetivo reunir la información de su computadora y enviarla a una entidad externa sin la aprobación del adulto mayor. Por lo general, funciona de manera silenciosa sin síntomas operativos, e incluso puede instalar otros programas sin que se dé cuenta. Los resultados de la infección también incluyen una degradación significativa del rendimiento de los sistemas dificultando la conexión a Internet.[23]

Figura 7. Spyware

Fuente: https://www.tecnologia-informatica.com/wp-content/uploads/2018/03/que-es-y-como-eliminar-spyware-1.jpg

[22] LLAC SEMOERE David, Delitos informáticos. Delitos contra la intimidad, 2022, 29 p.
[23] LYSENKO Sergii, Spyware Detection Technique Based on Reinforcement Learning, 2020, 12 p.

5.1.1.6 ADWARE

Son los anuncios en línea y por lo general contienen adware que es malware, por ejemplo, cuando entramos a una página web y nos bombardea constantemente con anuncios emergentes. El adware no solo es molesto, sino que puede recopilar su información personal, registrar los sitios web que visita e incluso registrar todo lo que escribe. Por eso hay que tener cuidado con los anuncios llamativos o esos que dicen “Haga clic aquí” o que digan que se ganó algo, se podría decir que adware es muy similar al spyware, spyware malicioso.[24]

Su principal función es mostrar anuncios. Aunque no tiene la intención de dañar su computadora, algunos lo consideran un tipo de spyware porque puede recopilar y enviar datos, investigar el comportamiento del Adulto mayor y orientar mejor los tipos de anuncios.[25]

Figura 8. Adware

Fuente: https://es.malwarebytes.com/images/adware/adware_graphics_2.jpg

[24] SÁNCHEZ BAUTISTA. Gabriel, Amenazas de seguridad a considerar en el desarrollo de software, 2022, Vol. 10, No 19, 31-37 p.
[25] DOMÍNGUEZ. Víctor, Backdoor de los antivirus, 2018, 114 p.

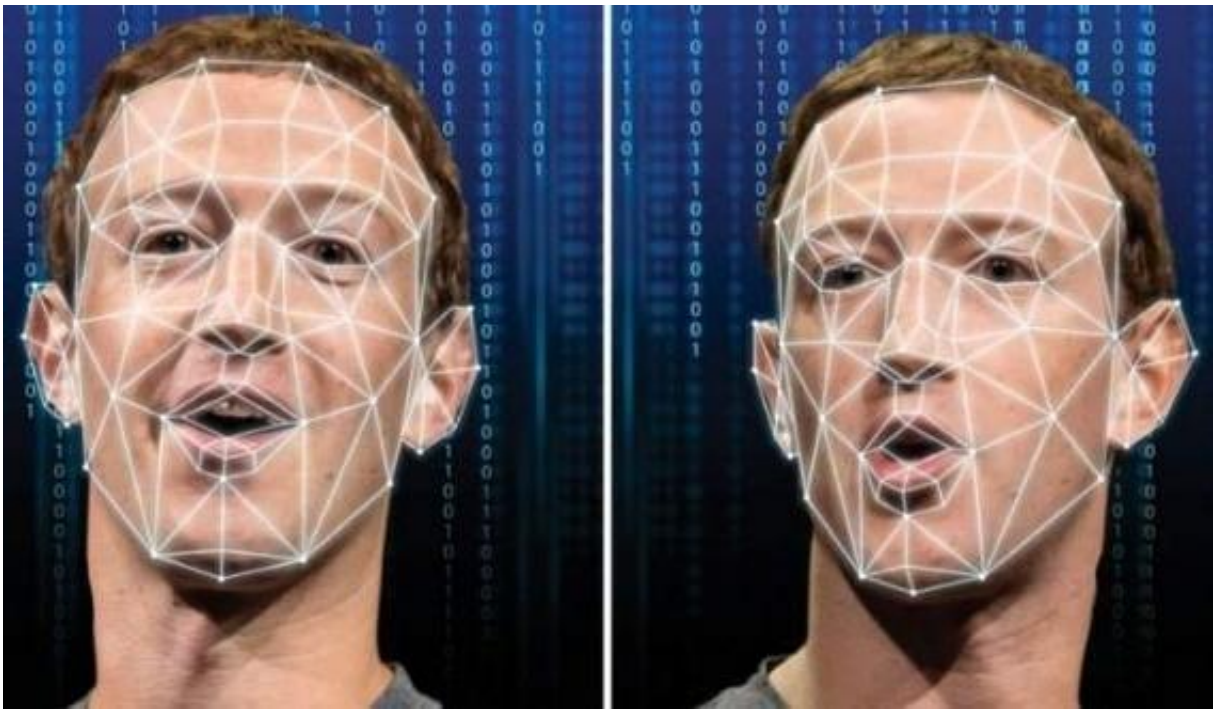
5.1.1.7 DEEPFAKES

Las falsificaciones profundas o "falsificaciones profundas" son archivos de video, imagen o voz que son manipulados por un software de inteligencia artificial para que parezcan originales, genuinos y auténticos.

Deepfakes usa inteligencia artificial para aprender, por lo que estos archivos pueden engañarnos fácilmente. Las falsificaciones profundas se utilizan para engañar a los adultos mayores, por lo que representan una gran amenaza para la sociedad actual, con la capacidad de promover la desinformación y generar algún tipo de desconfianza pública hacia cualquier fuente de información.[26]

También por medio de la inteligencia artificial en conjunto con programas de edición de video, manipulan el rostro de un adulto mayor logrando que realice gestos para que digan con su propia voz algo que no es y nos puede acarrear muchos problemas al realizar este tipo de suplantación de identidad.[27]

Figura 9. Deepfakes



Fuente: https://seguridad.cicese.mx/uploads/noticia/not1651-620e8e7af17f1.jpeg

[26] GARCIA. Jose, Deepfakes: the next challenge in fake news detection, 2021, 18 p.
[27] MORENO. Milagros, Regulación global para evitar la suplantación de identidad digital, 2022, Vol 14, No. 6, 690-696 p.

5.1.1.8 RANSOMWARE

Una de las principales formas en que el ransomware infecta las computadoras es mediante el envío de correos electrónicos que contienen malware, generalmente de manera inteligente, se puede decir que están escondidos o disfrazados .

El nombre Ransomware es una palabra compuesta, una combinación de las palabras rescate y software. Ransom en inglés significa rescate, de hecho, la función de este tipo de malware es robar los datos de tu ordenador y exigir un rescate económico a cambio de liberar los datos.[28]

Este es uno de los ataques más sofisticados y actualizados porque al obtener acceso a su computadora a través de un gusano informático u otro tipo de malware secuestra (cifra) los datos, bloquea la computadora y muestra una pantalla de advertencia que le indica que ha sido víctima de un ataque. la pantalla también muestra el monto a pagar y el método de pago, por eso se suele decir que se exige un rescate para recuperar estos. Por lo general se suele solicitar una transferencia en dinero electrónico (bitcoin) para evitar localización o evitar el rastreo del dinero. Este tipo de ciberataque va en aumento y por tanto es uno de los más temidos en la actualidad.[29]

Figura 10. Ransomware

Fuente: https://www.muyseguridad.net/wp-content/uploads/2019/11/ransomware_2.png

[28] MORENO. Jóse, Revisión sobre propagación de ransomware en sistemas operativos Windows, 2020, Vol 16, No. 1, 39-45 p.
[29] BELTRAN. Cristian, Estudio de Seguridad en Dispositivos Móviles con Sistema Operativo Android, 2021, 81 p.

5.1.1.9 PHISHING

El termino phishing hace referencia a que los ciberdelincuentes "pescan" con "cebos" ósea están al pendiente de ver si una víctima muerde el anzuelo, los phishers quieren robar sus datos y usarlos en su contra. Todos los ataques de phishing suelen realizar las mismas acciones, ya sea que se realicen a través de correo electrónico, redes sociales, mensajes de texto u otros sistemas, en los adultos mayores es muy usual utilizar los mensajes de texto, puesto que es el mecanismo que más usan y entienden. Los atacantes envían notificaciones específicas para engañar a las víctimas para que hagan clic en enlaces, descarguen archivos adjuntos, envíen la información solicitada o realicen pagos, cayendo muy fácilmente este tipo de personas adultas, puesto que por su edad no han conocido aun este tipo de delitos cibernéticos, confiando en el internet y sus servicios sin advertencia alguna.[30]

No es un software, sino diferentes técnicas de robo de privacidad para obtener información del adulto mayor, como contraseñas y datos bancarios. Los medios más comunes son correos electrónicos, mensajes o llamadas telefónicas donde se hacen pasar por una entidad u organización conocida y luego solicitan datos confidenciales que un tercero puede usar para su propio beneficio, siendo esta población muy vulnerable por su falta de conocimiento y de habilidad a la hora de usar el internet y sus servicios.[31]

Figura 11. Phishing

Fuente: https://www.valoradata.com/files/uploads/2019/09/phishing.jpg

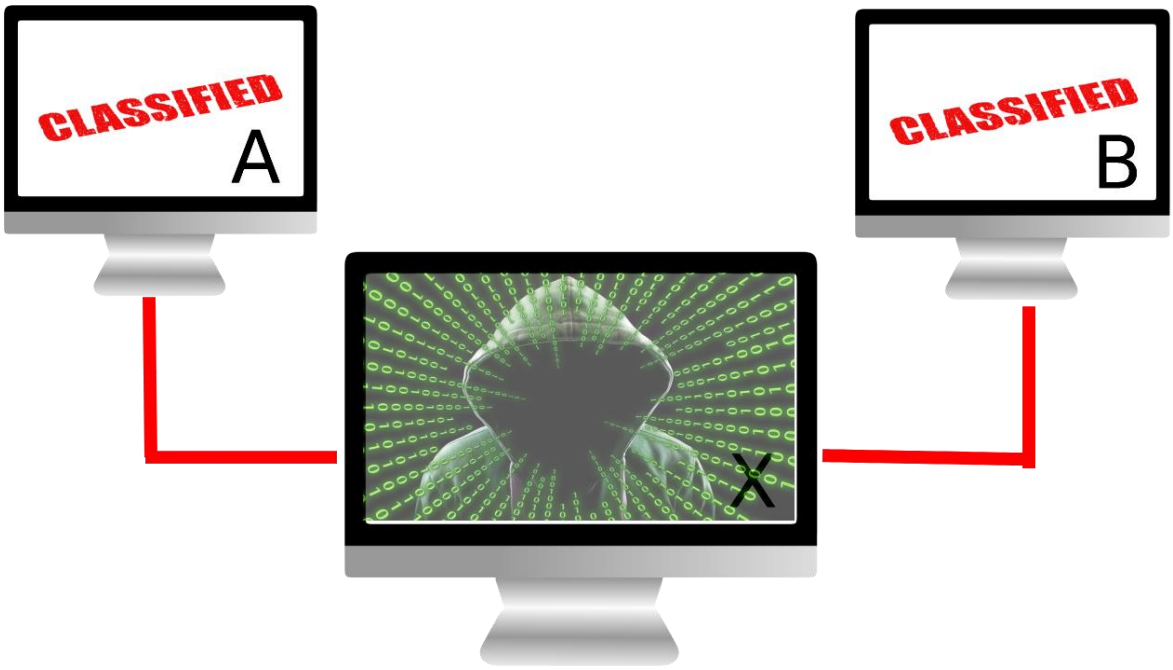
[30] LEGUIZAMÓN. Mayra Sheila Mariana, El phishing, 2015, 47 p.
[31] QUIRUMBAY YAGUAL. Daniel Iván, Una revisión del aprendizaje profundo aplicado a la ciberseguridad, 2022, Vol. 9, No. 1, 57-65 p.

5.1.1.10 ATAQUE MITM (MAN-IN-THE-MIDDLE)

Un ataque informático man-in-the-middle ocurre cuando un hacker interfiere con la transmisión de datos entre dos partes que se comunican electrónicamente. Los ciberdelincuentes se hacen pasar por una o ambas partes, ellos interceptan o secuestran datos de los adultos mayores y hacen creer a este y su receptor que se están comunicando entre sí, cuando en realidad no es así, y el hacker actúa como intermediario de esa comunicación.

Este ocurre cuando un ciberdelincuente intercepta la comunicación entre dos sistemas utilizando una identificación falsa. En este sentido, un atacante tiene control total sobre la información intercambiada y es libre de manipular la información de los adultos mayores sin que estos lo noten de inmediato. Debido a que normalmente se hace a través de una red WIFI pública abierta, se puede obtener información sensible del adulto mayor (la víctima) y es difícil de identificar por parte de la víctima sin un conocimiento mínimo del tema, es muy peligroso. sumado a que esta población ante su poco conocimiento accede a cualquier red, sin identificar si es segura o no, por lo que son quienes más se encuentran expuestos.[32]

Figura 12. man-in-the-middle.



Fuente: https://www.incibe.es/sites/default/files/contenidos/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo/mitm.png

[32] MEDINA PÉREZ. Victor, Seguridad adicional frente a ciber ataques Man-In-The-Middle, 2022, 85 p.

5.1.2 ATAQUES INFORMÁTICOS DONDE SE EVIDENCIA EL USO DE INGENIERÍA SOCIAL

5.1.2.1 Phishing por e-mail

Sin duda, este es el ataque de ingeniería social más común en la actualidad. Esto no es nada nuevo, ni mucho menos. Pero con el tiempo han perfeccionado su técnica. Básicamente, recibe un correo electrónico que le indica que inicie sesión o descargue un archivo a través de un enlace. El caso es que, cuando iniciamos sesión, le damos nuestros datos a los ciberdelincuentes.[33]

Figura 13. Phishing por email

Fuente: https://www.lisot.com/wp-content/uploads/2020/02/detectar-emails-fraudulentos.png

[33] VILCHEZ. Jose, Ciberseguridad y robo de información: Una revisión sistemática de la literatura, 2022, 20 p.

5.1.2.2 Mensajes de texto

La ingeniería social también se utiliza para realizar ataques mediante mensajes de texto. Pueden llevar a las víctimas a un sitio web malicioso o enviar datos de los adultos mayores con un simple mensaje de texto. Por ejemplo, pueden pretender ser organizaciones legítimas. Muchas veces nos invitan a un enlace donde podemos solucionar un problema u obtener algún beneficio que puede animar a la víctima a entrar.

Figura 14. Phishing por mensaje de texto

Fuente: https://www.barranquilla.gov.co/intranet/fraude-por-mensaje-de-texto-o-smishing

5.1.2.3 Estafas por redes sociales

Las redes sociales también son una fuente importante de ataques de ingeniería social. En muchos casos, los atacantes agregan a sus víctimas y fingen ser Adultos mayores legítimos, a veces miembros de organizaciones.[34]

Figura 15. Estafas en redes sociales

Fuente: https://img.freepik.com/vector-premium/ladrones-ciberneticos-piratas-informaticos-roban-informacion-personal-estafa-internet-phishing-delincuentes-web-delincuencia-linea-fraude-digital-contrasena-seguridad-informatica-ladron-datos-esplendido-vector_81894-8107.jpg?w=2000

[34] GAMBOA SUAREZ. Jose, Importancia de la seguridad informática y ciberseguridad en el mundo actual, 2020, 12 p.

5.1.2.4 Producto gratis

El anzuelo más tradicional. Esto le da al atacante la oportunidad de obtener algo gratis. Puede ser un software, un producto físico o un beneficio de firmar un contrato de servicio. Una vez más, intentan ganarse la confianza de sus víctimas antes de llevar a cabo sus ataques.

Figura 16. Phishing por mensaje de texto

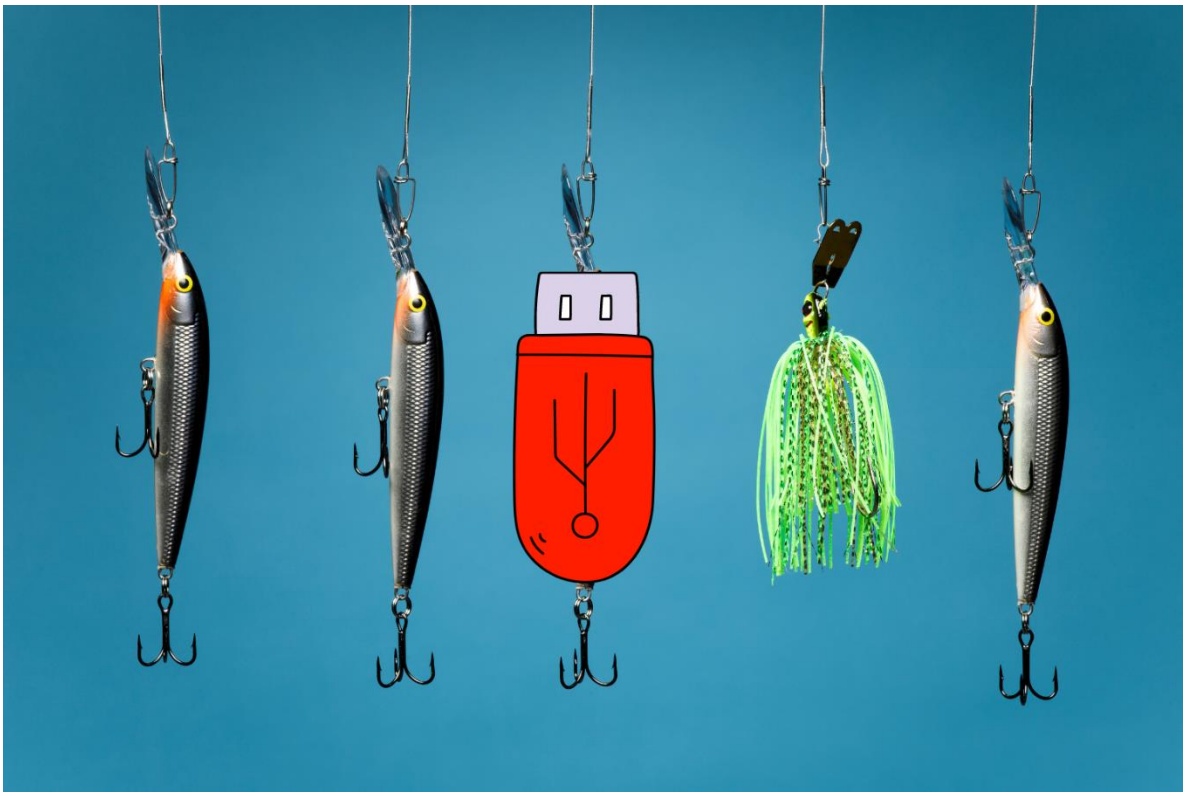
Fuente: https://imagenes.t13.cl/images/original/2021/03/1616440290-fraude-banco-estado.jpg?width=1200&height=675&position=top

5.1.2.5 Baiting

Es un tipo de ataque de ingeniería social en el que el atacante deja una USB infectada en un lugar público, como un parque, una biblioteca o una oficina. La víctima, al encontrar la unidad flash, es atraída por ella, ya que puede contener información interesante o útil. Al insertar la unidad flash en su ordenador, la víctima permite al atacante acceder al dispositivo y robar información personal o instalar malware.[35]

[35] UGARTE ESPADA. Paola, Métodos Orientados a Reducir Ataques de Ingeniería Social en Organizaciones, 2020, 76-79 p.

Figura 17. Baiting



Fuente: https://www.redseguridad.com/wp-content/uploads/sites/2/2021/06/baiting.png

5.1.3 APLICACIONES MALICIOSAS

Las aplicaciones maliciosas son aplicaciones móviles que no cumplen lo que prometen y simplemente nos bombardean con anuncios, o son aplicaciones que inyectan algún tipo de malware o virus en nuestros teléfonos inteligentes Android para robar datos, información de cuentas o controlar su teléfono móvil. dispositivo de forma remota.

En pocas palabras, las aplicaciones maliciosas son vías de entrada que utilizan diferentes tipos de malware para acceder a nuestros teléfonos. ¿Por qué son peligrosas las aplicaciones maliciosas? Las aplicaciones maliciosas se consideran peligrosas porque infectan nuestros teléfonos con algún tipo de malware sin nuestro conocimiento e instalan el malware más avanzado en el terminal que lo mantiene funcionando en segundo plano. Dependiendo de sus creadores o de lo que busquen sus creadores, las aplicaciones maliciosas contendrán malware para diferentes propósitos, por ejemplo, pueden contener algún tipo de spyware para espiar nuestros teléfonos y robarnos mientras usamos nuestros datos bancarios de aplicaciones bancarias, o pueden descargar un gusano informático que se propaga a través de nuestras listas de contactos, o controlar remotamente el terminal, grabar la pantalla del teléfono o usar su cámara, o incluso secuestrarlo y bloquearlo con Ransomware.

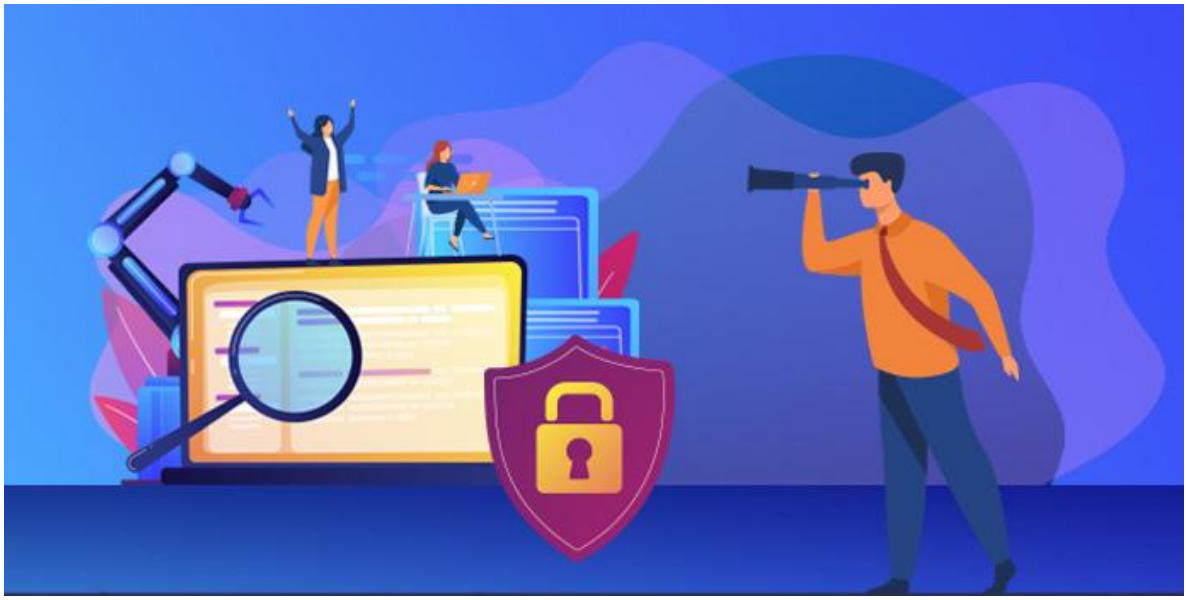
Como puede ver, descargar e instalar aplicaciones maliciosas puede tener graves consecuencias para su teléfono, datos personales, cuentas de usuario e incluso su dinero.[36]

5.1.4 VULNERABILIDADES EN APLICACIONES

Son debilidades o fallas de un sistema de información que abre la puerta para que los atacantes o circunstancias imprevistas puedan comprometen la integridad, disponibilidad o confidencialidad de los datos.

Las vulnerabilidades provienen de una variedad de fuentes, como errores de configuración, errores de diseño o errores de programa.[37]

Figura 18. Vulnerabilidades en aplicaciones.



Fuente: https://saynet.com.mx/wp-content/uploads/2021/01/vulnerabilidades.jpg

Algunas de las vulnerabilidades por las cuales no debemos instalar aplicaciones de fuentes desconocidas son las siguientes:

[36] MEJÍA. Jazreel, Detectando aplicaciones maliciosas en Smartphone con sistema Android a través del uso de una aplicación, 2019, No. 31, 82-93 p.
[37] QUIROZ ZAMBRANO. Silvia, Seguridad en informática: consideraciones, 2017, Vol. 3, 676-688 p.

5.1.4.1 VULNERABILIDADES DE USO

Hace referencia a deficiencias en el uso que los adultos mayores dan a sus equipos, presentando ausencia de actualizaciones, o dispositivos los cuales ya no tienen soporte por su antigüedad, y al igual softwares que ya no reciben este tipo de actualizaciones.

Esta suele tener mayor impacto que todas las anteriores porque son las menos consideradas. Están relacionadas con la falta de capacitación o desconocimiento de las prácticas de seguridad entre los Adultos mayores.

Sumado a ello, también se presentan vulnerabilidades en su falta de conocimiento, por ejemplo, es donde se le miente al Adulto mayor diciéndole que es ganador de un algún premio, cosa que no es cierta, siendo su objetivo que el Adulto mayor de su información confidencial, al hacer clic en esas ventanas recuperan datos de la computadora ahí es donde proceden a realizar un ataque.[38]

5.1.5 CUIDADOS CON HACKERS

Al adulto mayor le suelen robar grandes sumas de dinero en todo el mundo esto tal vez por su ingenuidad o desconocimiento de las nuevas herramientas digitales. Lo cual simplemente sucede porque las personas mayores contestaron el teléfono y creyeron lo que dijo el estafador o hicieron clic en un enlace que recibieron en un correo electrónico o en Facebook. Las personas mayores también suelen desconocer la mayoría de las complejidades de la tecnología, por lo que es vital que tomemos medidas para protegerlos de este tipo de estafas.

Los hackers buscan estafar a los adultos mayores utilizando las siguientes estrategias: ofreciendo la oportunidad de comprar un seguro a precios inmejorables, con anuncios de lotería falsos que debe ganar, increíbles descuentos en viajes para personas mayores y más, llamadas telefónicas donde brindan información de bancos o entidades con las cuales tienen un producto haciéndoles entregar información personal y mediante redes sociales. En otros casos, pueden secuestrar las cuentas de familiares y hacerse pasar por ellos para pedirles dinero para ayudarlos en situaciones difíciles.

Los tres principales tipos de hackers que debemos de tener en cuenta:

5.1.5.1 White hats

La piratería de sombrero blanco, en el sentido informático, se refiere a la ética de los piratas informáticos que se centra en la seguridad y protección de los sistemas de digitales. Estos suelen trabajar para empresas de seguridad informática.

[38] MOLINA. Yeison, Vulnerabilidades de los Sistemas de Información: una revisión, 2020, 11 p.

5.1.5.2 Black hats

Los sombreros negros son villanos o malos, por lo que los sombreros negros se usan en tales roles en lugar de los heroicos sombreros blancos. También conocidos como "crackers", demuestran sus habilidades informáticas al descifrar los sistemas de seguridad informática, colapsar servidores, ingresar a áreas restringidas, infectar o apoderarse de redes y muchas otras cosas utilizando sus habilidades de piratería. Disfrutan del desafío intelectual de superar o eludir las limitaciones de forma creativa.

5.1.5.3 Gray hats

Se puede decir que es una mezcla o hibrido entre ciberdelincuentes y un hacker de sombrero blanco, este no pretende tener malas intenciones, pero si tiene que obviar las legalidades lo va a hacer.[39]

Figura 19. Hacker

Fuente: https://www.campusciberseguridad.com/media/k2/items/cache/9267284e7733f4bec00d2e114d3f3ba1_L.jpg

[39] SALINAS PINEDA. Denis Neptalí, Análisis de un mecanismo de seguridad informática mediante el manual de la metodología abierta de testeo de seguridad, 2017, 17 p.

5.2 DESARROLLO DE OBJETIVO 2

- Examinar la normatividad vigente en Colombia referente a los lineamientos de seguridad digital de los ciudadanos.

5.2.1 Normatividad seguridad informática en Colombia

Según la legislación colombiana va desde multas desde 10 hasta 1.000 salarios mínimos legales mensuales vigentes, dependiendo de la gravedad del asusto puede incurrir en cárcel que va desde 36 hasta 96 meses de prisión las leyes más referentes en Colombia son:

5.2.1.1 Ley 1273 de 2009

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

La ley está conformada por artículos de las cuales describe cada uno de los diferentes delitos informáticos que son sancionados según la legislación colombiana, estipulando las diferentes multas de 100 a 1000 salarios mínimos vigentes mensuales y penas de prisión contemplados que pueden ir de cuarenta y ocho (48) a noventa y seis meses (96).[40]

5.2.1.2 Ley 1581 De 2012

"Por la cual se dictan disposiciones generales para la protección de datos personales". Esta ley cubre todos los datos recolectados en las entidades públicas y privada la cual puede ser datos públicos, semiprivados, privados, sensibles, biométricos, de niños, niñas y adolescentes. Las entidades deben tener claro el uso de los datos dependiente de su clasificación ya que de ellos depende también su uso indebido genera sanciones impuesto por la superintendencia de industria y comercio. Las sanciones al incumplimiento de la norma ocasiones sanciones que pueden ser multas, cese de actividades, cierre de la empresa o entidad proporcional al grado de la infracción.[41]

[40] CONGRESO DE COLOMBIA, Ley 1273 2009, {En Línea}, accedido 9 de julio de 2022, https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf.
[41] SECRETARIA SENADO, Leyes desde 1992 [LEY_1581_2012], {En Línea}, 10 de julio de 2022, http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

5.2.1.3 Ley 527 de 1999

Regula y define el acceso y uso de mensajes de datos, comercio electrónico, firmas digitales y autoridades de certificación, y promulga otras regulaciones.[42]

5.2.1.4 Ley 1712 de 2014

Esta ley establece el derecho de acceso a la información pública y la transparencia en la gestión pública. También establece la obligación de las entidades públicas de garantizar la seguridad de la información que manejan.

5.2.1.5 Resolución 3067 de 2019

Esta resolución establece los requisitos mínimos de seguridad que deben cumplir las entidades públicas en Colombia para proteger su información y prevenir ataques cibernéticos.

5.2.1.6 Resolución 1007 de 2020

Esta resolución establece los lineamientos para la identificación y gestión de riesgos de ciberseguridad en las entidades públicas.

5.2.1.7 Ley 2068 de 2022

Establece la Política Nacional de Ciberseguridad para la protección de la población adulta mayor, fue sancionada por el presidente Iván Duque el 20 de julio de 2022.

5.2.1.8 Resolución 000214 de 2023

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) adoptó el Plan Nacional de Acción para la Protección de la Población Adulta Mayor en el Ciberespacio el 22 de febrero de 2023.

5.2.2 EL INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE)

el INCIBE es una entidad española gracias a su experiencia y recursos podrían ser de utilidad como modelo para otros países, incluyendo Colombia, en la mejora de la ciberseguridad y protección de los ciudadanos y empresas de los riesgos en línea, Sin embargo, los adultos mayores en Colombia son una población especialmente vulnerable en cuanto a la protección de sus datos en línea, ya que el país ha experimentado un aumento significativo de los ciberataques en los últimos años. Los recursos y servicios

[42] FUNCION REPUBLICA, Ley 527 de 1999, 10 de julio de 2022, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276.

del INCIBE podrían adaptarse y utilizarse en Colombia para mejorar la formación y concienciación en ciberseguridad, y para proporcionar apoyo y asesoramiento a las empresas y ciudadanos colombianos en la protección de sus sistemas y datos.

5.2.2.1 Ley Orgánica 3/2018

Menciona la Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) esta ley regula la protección de datos personales y los derechos de los ciudadanos en relación con los mismos.

5.2.2.2 Reglamento General de Protección de Datos (RGPD)

Esta normativa europea establece las obligaciones para la protección de datos personales en la Unión Europea y se aplica a todas las empresas que manejan datos personales de ciudadanos europeos.

5.2.2.3 Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE)

Esta ley regula el comercio electrónico en España y establece obligaciones para las empresas que ofrecen servicios en línea.

5.2.3 CONSTITUCIÓN POLÍTICA DE COLOMBIA

La vejez es una categoría de rango especial de protección en cabeza del estado, por lo que deberá asegurar todas las condiciones básicas para vivir así lo establece la carta política en el artículo 46 por ello deberán propender para que las personas de la tercera edad tengan una integración a la vida activa y comunitaria.

5.2.3.1 Ley 1251 de 2008

Esta norma establece el deber de procurar por la implementación de planes y programas que tengan en cuenta el proceso de envejecimiento, y que se garanticen por parte de la familia, el estado y la sociedad, conforme lo ordena el artículo 46 de la constitución política de Colombia.

Como podemos ver esta variedad de normas, van estrictamente ligadas con la carta política y los pactos internacionales (bloque de constitucionalidad), para abarcar el tema desde todos los aspectos sociales, culturales, económicos y políticos que rigen el entorno internacional y nacional.

Podríamos considerar esta ley como la fuente de toda la normatividad que se desprende en pro del adulto mayor y su bienestar.

En su Artículo 17° habla las áreas que deberá intervenir el estado para velar por los derechos del adulto mayor, entre los que nos conciernen en el presente estudio, están la educación, recreación, cultura, participación en la equidad, mejoramiento continuo, mejorar calidad y expectativas de vida familiar, social y personal, acciones educativas, productivas con el fin de generar su desarrollo económico y productivo, y la capacitación para que se facilite y promueva el acceso a las nuevas tecnologías y al teletrabajo.

5.3 DESARROLLO DE OBJETIVO 3

- Proponer un manual de recomendaciones y medidas de ciberseguridad para prevenir el hurto de datos personales a los adultos mayores en Colombia.

MANUAL DE MEDIDAS DE PRECAUCIÓN:

El objetivo de esta guía es abordar los peligros comunes que enfrentan los adultos mayores en la actualidad, por tanto, se menciona las siguientes pautas para que los adultos mayores sepan qué hacer y que no hacer, además, este guía es totalmente útil para todos los Adultos mayores que hagan uso de los medios digitales. ya que las amenazas como los virus no discriminan ninguna situación y nos afectan a todos.

5.3.1 SENTIDO COMUN

Sea critico al leer los correos electrónicos, mensajes y publicaciones, en redes sociales, si algo parece demasiado bueno para ser verdad, probablemente no lo sea.

5.3.2 CONTRASEÑAS

Las contraseñas son la clave para acceder a nuestros servicios e información personal, por lo que, si alguien se apodera de ellas, puede comprometer nuestra privacidad y, entre otras cosas, poder: publicar en nuestro nombre en las redes sociales, leer y responder a nuestros correos electrónicos, visite nuestro banco de internet, etc.

Procurar usar contraseñas robustas y seguras, evitar usar la misma contraseña en todas las cuentas, una contraseña segura debe incluir números, caracteres especiales, letras minúsculas con mayúsculas procurando de que no sean fáciles de adivinar o usar la autenticación de dos pasos como lo que podría ser un toquen por medio de un mensaje de texto.

Como no se deben usar las contraseñas o que no deben contener las contraseñas: Nombres propios, algún lugar de residencia, combinaciones cortas o palabras sencillas, fechas de nacimiento y por último no compartir sus contraseñas con nadie

Figura 20. Contraseñas seguras

Fuente: https://blog.udlap.mx/wp-content/uploads/2020/08/contrasena-.jpg

5.3.3 CORREOS

Evitar abrir correos electrónicos desconocidos o que no esté esperando, correos que no están autenticados, correos de dudosa procedencia, mensajes con demasiadas imágenes o referencias de asuntos engañosos, ya que estos mensajes son enviados por oportunistas con el fin de engañar a algún adulto mayor desprevenido buscando obtener algún tipo de información de interés como la que podría ser información financiera (datos de cuentas de bancos o datos de una tarjeta de crédito)

Por eso es importante nunca confiar en los archivos adjuntos de correo electrónico no solicitados. Si recibe un correo electrónico inesperado con un archivo adjunto de un extraño, nunca abra el archivo adjunto y no elimine el correo electrónico, no intente abrirlo.

Figura 21. Cuidado con los correos electrónicos

Fuente: https://www.muyseguridad.net/wp-content/uploads/2020/08/malware-por-correo-electr%C3%B3nico.jpg

5.3.4 MENSAJES DE TEXTO

Es muy importante que siempre leamos correctamente los encabezados de los correos electrónicos para verificar realmente quién recibe la respuesta del correo electrónico.
Como puede ver en la imagen a continuación, el campo DE muestra el nombre de la empresa que lo envió (legítimo, por supuesto), pero podemos confirmar que no pertenece al dominio SMTP de esa empresa. También podemos revisar la ortografía y revisar las expresiones que se utilizan para dirigirse a nosotros. Si hay errores tipográficos o inconsistencias en el informe, dude de su autenticidad. En muchos casos, los atacantes usan programas automatizados para traducir los mensajes, y aquí es donde ocurre el error.

5.3.5 REDES PÚBLICAS

Evitar usar redes WIFI no confiables o redes WIFI públicas con la finalidad de ahorrar los datos móviles del celular, al momento de acceder a algún sitio donde pueda intercambiar información sensible o financiera donde se puedan ver comprometidos datos o tarjetas de crédito.

Tener en cuenta estas recomendaciones: Mantener siempre el navegador web actualizado, usar contraseñas robustas, realizar como mínimo 1 vez a la semana una copia de seguridad y no descargar contenido pirata.

Figura 22. Cuidado con el WIFI gratis

Fuente: https://tuxiaomi.es/wp-content/uploads/2019/02/cafeteria_wifi_publica_x210.jpg

5.3.6 SITIOS WEB SEGUROS

Procurar ingresar a sitios web que sean seguros, por ejemplo que la página web que se está visitando coincida con la URL, que contengan la letra “s” después de “http” y buscar el icono del candado de color verde, evitar abrir links que te llegaron por mensaje de texto o correo electrónico por que estos no pueden redirigir a sitios web falsos, de la misma manera tener mucho cuidado con las ofertas que se ven tan tentadoras o que dicen ser que expiran pronto y que solo tú puedes aprovechar de esta oferta, porque no lo son.

Figura 23.Sitios web seguros

Fuente: https://signal.avg.com/hubfs/Blog_Content/Avg/Signal/AVG%20Signal%20Images/How%20to%20Check%20if%20a%20Website%20is%20Safe/How_to_Check_if_a_Website_is_Safe-Thumb.jpg#keepProtocol

5.3.7 REDES SOCIALES

Hacer buen uso de las redes sociales significa: no ingresar a grupos, páginas que no conozca, no agregar a gente desconocida, usar contraseñas robustas, fijarse que la URL de la red social sea segura que el http contenga la “s” (https), no compartir información sensible o financiera, mantener el antivirus actualizado, cuidado con lo que se publica para no dar a entender de que estamos de viaje y que nuestro hogar está solo.

Figura 24. Cuidado con las redes sociales

Fuente: https://www.iberdrola.com/documents/20125/40411/746x419.jpg/a9f90420-f107-c3a2-256f-d378757ac699?t=1627362831670

5.3.8 CERRAR SIEMPRE SESIÓN

Es muy importante que siempre cierres sesión, porque uno nunca sabe quién pueda coger nuestros dispositivos electrónicos, por más contraseña robusta que tengamos o segundo factor para autenticación es mejor siempre cerrar sesión para evitar que hagan uso de nuestros perfiles, hagan compras, nos roben nuestros datos o nos descarguen malware.

Figura 25. Cerrar siempre sesión

Fuente: https://www.redseguridad.com/wp-content/uploads/sites/2/2020/03/914788014-gi.jpg

5.3.9 MANTENER LOS SISTEMAS SIEMPRE ACTUALIZADOS

Hay que tener cuidado porque los ciberdelincuentes siempre están buscando vulnerabilidades en los sistemas, la finalidad de actualizar todos los sistemas es para conseguir los parches de las vulnerabilidades que pudieron haber ocurrido tiempo atrás y así siempre proteger nuestra información del hurto o daño.[43]

Figura 26. Actualizaciones constantes

Fuente: https://www.cronup.com/alerta-de-seguridad-por-nuevas-actualizaciones-de-seguridad-para-microsoft-windows-noviembre-2022/

5.3.10 DISPOSITIVOS SIEMPRE BLOQUEADOS

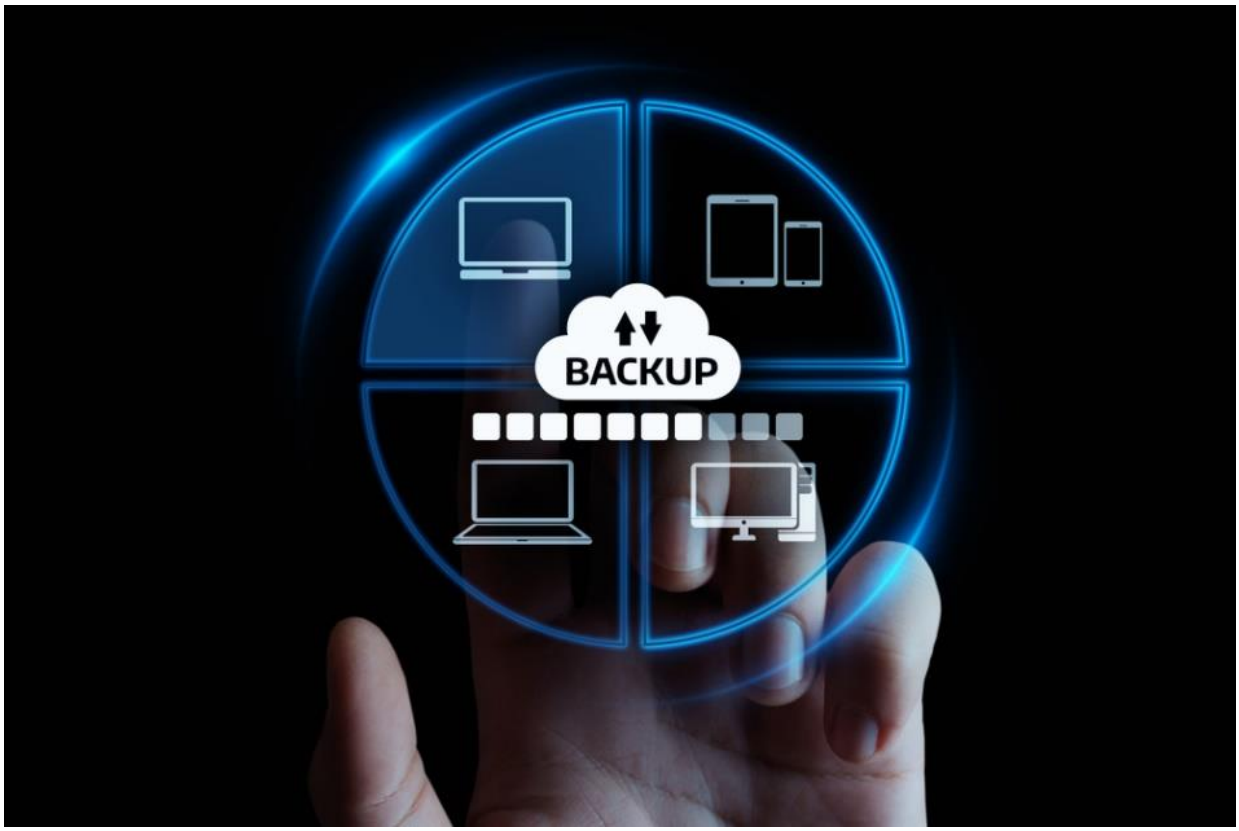
[43] MONSALVE MENDEZ. Jaime Yesid, Ciberseguridad: principales amenazas en Colombia (ingeniería social, Phishing y Dos), 2018, 10 p.

Configura tu teléfono inteligente para que permanezca bloqueado hasta que proporciones datos biométricos, como una huella dactilar o un escaneo facial.

5.3.11 COPIA DE SEGURIDAD

Uno siempre debe de realizar copias de seguridad al menos una vez al mes, porque uno no sabe en qué momento algún dispositivo llegue a fallar o algún virus llegue a dañar algún dato conllevándonos a la perdida de lo más valioso que es la información.

Figura 27. Copias de seguridad



Fuente: https://cuadernosdeseguridad.com/wp-content/uploads/2019/07/backup.jpg

5.3.12 NO INSTALAR APLICACIONES QUE NO SEAN NECESARIAS

Evitar usar aplicaciones que piden audios, videos o fotos, especialmente si son de procedencia desconocida, ya que estas aplicaciones se suelen usar para la suplantación de identidad, también hay que tener cuidado con aplicaciones que piden permisos de accesos ya sea a la ubicación al micrófono o la cámara, procurar siempre descargar aplicaciones de tiendas oficiales como la Playstore y la reputación de estas apps.

Figura 28. Aplicaciones dañinas o innecesarias

Fuente: https://cronicaglobal.elespanol.com/uploads/s1/25/36/32/5/movil-virus-alerta.jpeg

5.3.13 MANTENERSE SIEMPRE INFORMADO DE NUEVOS CASOS DE CIBERSEGURIDAD Y APRENDER DE LOS ERRORES

Procurar siempre mantenerse al día e informado de las novedades sobre ciberseguridad con la finalidad de minimizar los riesgos a los que estamos expuestos al momento de hacer uso de la gran red de informa que es el internet, teniendo claro cómo hacerle frente, en pocas palabras a cualquiera lo puede afectar alguna amenaza de ciberseguridad y en cualquier momento, por eso la finalidad de esta guía de brindar unas pautas mínimas para no correr riesgos de ciberseguridad, y de que llegase a suceder aprender de los errores y poner sobre aviso a nuestros allegados para procurar evitar a que ellos nos les llegue a pasar también.

Figura 29: Cuidados de ciberseguridad

Fuente: https://niubox.legal/wp-content/uploads/2021/04/ciberseguridad.png

5.3.14 BLOQUEAR LLAMADAS NO SOLICITADA

Recibir llamadas de números que no se encuentran almacenados en nuestros contactos es una práctica que se presenta con más frecuencia de lo que creemos, toda vez que los ciberdelincuentes están buscando víctimas potenciales como lo son los adultos mayores, es por ello que ante por eso ante cualquier llamada que evidenciemos provenga de un contacto desconocido, proceder a bloquearla para evitar las amenazas y riesgos que estas pueden conllevar.

5.3.15 REVISAR REGISTROS DE INICIO DE SESIÓN

Al iniciar sesión en los diferentes sitios web, se debe siempre tratar de revisar regularmente la fecha y la hora que nos registra del "último inicio de sesión" que los adultos mayores usan, con la finalidad de corroborar que la información arrojada, como lo son los horarios de acceso coinciden con las actividades que se han ejecutado con dichas herramientas y se verifique que efectivamente corresponden a los inicios de sesiones que se han hecho por parte de los propietarios de las cuentas.

5.3.16 TENER CUIDADO CON FRAUDES O ESTAFAS EN INTERNET

5.3.16.1 TIENDAS ONLINE

Mediante esta modalidad los ciberdelincuentes crean páginas web falsas, las cuales ofrecen productos a valores atractivos debido a que son a bajo costo en comparación al mercado, o prometiendo beneficios tales como entrega rápida o gratis, generando al adulto mayor un interés, pero una vez realizan el cobro del producto y obtiene el pago, la victima nunca recibe el producto y la pagina suele desaparecer, siendo imposible localizarlos, toda vez que los servidores utilizados para estos sitios web, se encuentran generalmente en países fuera de la jurisdicción policial o legal, siendo imposible ejecutar alguna acciona legal en su contra.

5.3.16.2 FALSOS ARRIENDOS O ALQUILERES

Al igual que en el punto anterior, actualmente las ofertas de productos y servicios se han incrementado, como lo es el alquiler online, de hospedaje turístico, temporal o de larga duración, en propiedades con precios muy atractivos por estar en bajo costo y aparentar tratarse de una ganga, por lo que se requiere dinero como pago inicial, depósito o reserva. Empero a ello, sucede que, en muchos casos, la propiedad no existe o no está disponible para ser arrendada, por lo que el adulto mayor cancela y posteriormente quien le ofreció el servicio desaparece y no responde por ello, siendo una estafa.

5.3.16.3 TÉCNICO FALSO

Al acceder a determinadas páginas, se generan avisos indicando que el ordenador presenta una infección con un virus que generara la eliminación de los datos, archivos e impedirá utilizar el dispositivo, por ello solicitara se indique un número de contacto para que se le otorgue soporte técnico para eliminar dicha amenaza, pero generalmente al obtener contacto con el presunto técnico, este le solicitara descargar una aplicación que le permita acceder de manera remota al dispositivo, pero es allí que el ciberdelincuente obtiene el control del equipo y exigir un pago. La cantidad requerida suele ser siempre demasiado alta. A veces, las fallas de los dispositivos son reales porque estos delincuentes descargan malware antes de brindar soporte técnico.

5.3.16.4 FALSOS EMPLEOS

Recibir ofertas para vacantes mediante el correo electrónico o publicaciones de redes sociales en las cuales se señales unas condiciones muy atractivas y favorables, donde el salario, beneficios económicos y salarios, sea superiores a los que normalmente se oferten en las empresas, para llamar la atención, sobre todo de los adultos mayores que son una población que por su edad presentan una dificultad en ser empeladas, por lo tanto aprovechan esta situación y se les exigen pagos anticipados para participar en los procesos de selección, pero una vez que se obtuvo el dinero, no hubo más mención de

esta oferta. En otros casos, es necesario abrir una cuenta bancaria para recibir fondos junto con contraseñas y firmas electrónicas. Este enfoque permitió la creación de las llamadas cuentas mula, que luego se utilizaron para transferir fondos de otras actividades ilegales sin el conocimiento de los adultos mayores que aparecían como propietarios.

5.3.16.5 SIM SWAPPING

Esta amenaza consiste en utilizar documentos de adultos mayores para adquirir tarjetas SIM, con su información, esto permite que los ciberdelincuentes tomen el control de su teléfono y acceder a todos los datos almacenados. Esto se hace falsificando sus documentos de identidad o entregando fotocopias de estos. De esta forma, les activan la tarjeta SIM obtenida fraudulentamente y se invalida la tarjeta SIM original, con lo cual lograron la misión y con esta pueden ingresar a cuentas bancarias y transferir dinero desde ellas.

5.3.16.6 FRAUDES EN INVERSIONES

En la actualidad las redes sociales y el uso de las nuevas tecnologías han creado una tendencia de nuevos negocios y formas de inversión, como lo son las criptomonedas, los diamantes o el oro, este fraude consiste en engañar a las víctimas para que transfieran dinero a otras cuentas, vendiendo la idea de dinero fácil, haciendo creer que se enriquecerán en cuestión de horas o días, generalmente este tipo de negocios o inversiones prometen retornos financieros exorbitantes, y, como prueba, estas víctimas son dirigidas a sitios web donde se suben falsos testimonios que muestran las grandes ganancias que recibirían. Sin embargo, después de sus inversiones desaparecen y nunca reciben nada de lo que se les prometió inicialmente.

5.3.16.7 ESTAFAS CON TARJETAS DE VACUNACIÓN CONTRA LA COVID-19

Debido a la pandemia del COVID-19, y el incentivo que se generó para la vacunación, muchos de los adultos mayores, publicaron sus carnets de vacunación, donde revelaron su información personal, situación que fue aprovechada por los ciberdelincuentes, y de esta manera al tener su nombre completo, fecha de nacimiento y documento, obtener acceso a tarjeta de crédito o cuentas de correo electrónico donde se almacenan contraseñas importantes, robando así su identidad.

5.3.16.8 CITAS POR INTERNET

Con el desarrollo de las herramientas tecnológicas se han creado aplicaciones de citas por internet, las cuales tienen un gran acceso por parte de los adultos mayores, los cuales están buscando nuevos relacionamientos, por lo que ante una necesidad de conocer personas, no se percatan de la veracidad o la existencia de la persona con la que se están conociendo, cayendo en trampas de estafadores que a menudo atraen a sus víctimas románticas desde sitios web que pueden monitorear a Google Meet, WhatsApp o Facebook Messenger, donde nadie los ve, y terminan solicitando dinero o datos personales que permiten que suplante su identidad e ingresen a sus cuentas y posterior robo de dinero.

5.3.16.9 FALSOS FAMILIARES

Esta amenaza se dirige generalmente a personas de la tercera edad, donde buscan estafarlos mediante llamadas donde suplantan a familiares muy cercanos tales como nietos o hijos, quienes son suplantados por los estafadores que se ponen en contacto con las víctimas afirmando encontrarse en una emergencia tal como haber sufrido un accidente o ser capturado por alguna autoridad, situación que genera se les exija una transferencia de dinero fácil y rápida ante la necesidad en la que se encuentra, los estafadores obtienen información de dichos familiares en los perfiles de las redes sociales a fin de generar confianza al momento de tener la comunicación, y lograr su cometido.

5.3.16.10 CONTRATISTAS A DOMICILIO

Dentro de las amenazas más comunes y que se han presentado a lo largo de los años, son los falsos funcionarios de entidades de servicio público u otras empresas que prestan servicios en los domicilios, quienes mediante identificaciones falsas, logran ingresar a los predios de los adultos mayores y acceder a información relevante o equipos que permiten que posteriormente estos estafadores accedan a cuentas donde puedan robar sus cuentas, o a personas cercanas y familiares, por lo que es importante si se necesita de estos servicios siempre contactar alguien de confianza o corroborar con las empresas la identidad de las personas que se permiten ingresar al hogar, oficinas o empresas.

6 CONCLUSIONES

Basado en el primer objetivo, que aborda el estado del arte sobre las amenazas que enfrentan los adultos mayores al utilizar servicios de internet, es importante considerar el profundo impacto que el auge de Internet ha tenido en la sociedad actual. Este fenómeno ha revolucionado la accesibilidad a la información, coincidiendo con un aumento en la expectativa de vida y en la población de adultos mayores. Sin embargo, esta transformación acelerada ha planteado un desafío crucial: la gestión de los riesgos de seguridad asociados con la creciente dependencia de dispositivos electrónicos, como teléfonos móviles y computadoras, las amenazas cibernéticas han aumentado exponencialmente. Este grupo demográfico, debido a su edad y a las brechas digitales existentes, se encuentra particularmente vulnerable, ya que a menudo carecen de la educación necesaria en el uso de herramientas tecnológicas e internet. En este contexto, la ciberseguridad ha adquirido una relevancia global, en vista de la necesidad de salvaguardar los activos de información accesibles a través de la red de los ciberdelincuentes.

El análisis exhaustivo de las distintas amenazas de ciberseguridad que enfrentan los adultos mayores que se conectan a internet revela que esta población es objeto de robo de información y diversas estafas que impactan negativamente en sus recursos económicos. Esta problemática genera un sentimiento de inseguridad en el uso de esta herramienta valiosa y sitúa a los adultos mayores en una posición de desventaja social. Aunque los virus y programas maliciosos también constituyen amenazas, los adultos mayores, debido a su condición de vulnerabilidad social y digital, se convierten en blancos más fáciles para los delincuentes cibernéticos. Esta situación agrava las desigualdades existentes y subraya la urgente necesidad de abordar la ciberseguridad desde una perspectiva inclusiva y educativa, con el fin de empoderar a esta población y permitirles beneficiarse plenamente de los avances tecnológicos sin comprometer su seguridad financiera y personal.

Siguiendo el segundo objetivo, que se enfoca en la normativa actual en Colombia relacionada con las directrices de seguridad digital para los ciudadanos, es crucial considerar el marco legal y regulatorio que ampara la protección de los ciberdelitos en el país. En este contexto, se establecen sanciones y penalidades específicas para estos delitos, donde los adultos mayores son reconocidos como una población que merece una atención y protección especiales. Como respuesta, se han promulgado diversas normas destinadas a fomentar su inclusión social y su educación digital. La ciberseguridad emerge como un pilar fundamental, permitiendo que esta demografía pueda acceder a la tecnología de manera segura y sin enfrentar obstáculos o desigualdades sociales que limiten su independencia en el ejercicio de sus derechos y su calidad de vida. Esta es una preocupación relevante, ya que la conectividad a Internet es esencial para acceder a servicios vitales como empleo, educación y otros aspectos necesarios en la vida moderna.

Por último en base el tercer objetivo hace referencia al enfoque de como la ciberseguridad se convierte en un elemento esencial al proponer un manual de recomendaciones y medidas específicas para prevenir el robo de datos personales entre los adultos mayores en Colombia. Las sugerencias que abarcan aspectos como la ingeniería social, amenazas y ataques, se establecen como herramientas preventivas cruciales, diseñadas para salvaguardar la información personal de los adultos mayores durante su actividad en línea. Cada una de estas recomendaciones está alineada con un enfoque central: asegurar que los adultos mayores puedan disfrutar de los beneficios de Internet sin poner en riesgo su privacidad.

Además, es fundamental que cada adulto mayor considere compartir sus conocimientos o capacitar a un miembro cercano de la familia o amigos, generando así conciencia sobre las amenazas y riesgos que pueden surgir al navegar por la web. Este enfoque no solo promueve la adopción segura de herramientas digitales, sino que también contribuye a ampliar el número de personas de edad avanzada que se aventuran en las plataformas en línea, fomentando su crecimiento y desarrollo en la era digital actual.

En este contexto, resulta imperativo reconocer la importancia de este manual de recomendaciones de ciberseguridad. Basado en fuentes bibliográficas cuidadosamente revisadas, el estudio subraya el progresivo aumento de la población adulta y su creciente participación en el entorno digital. Este incremento destaca la necesidad de priorizar medidas preventivas de ciberseguridad, con el propósito de salvaguardar sus derechos y cumplir con las normativas nacionales e internacionales. Esto no solo promueve la inclusión y desarrollo de las personas mayores en la sociedad actual, sino que también contribuye a cerrar la brecha digital que ha persistido durante años. Si no se brinda seguridad en el ámbito digital y no se protege a los adultos mayores de los ciberdelitos, existe el riesgo de que se vean excluidos de las oportunidades en línea y detengan su avance en la era digital. Por ende, la promoción de buenas prácticas en seguridad informática no solo garantiza la seguridad en línea de los adultos mayores, sino que también impulsa su participación y su desarrollo continuo en la sociedad moderna.

7 RECOMENDACIONES

- Para protegerse de los riesgos de seguridad en línea, como virus, fraudes y phishing, es importante que los adultos mayores sigan algunos consejos prácticos. En primer lugar, se recomienda instalar software antivirus en todos los dispositivos y mantenerlos actualizados. Además, es importante realizar escaneos frecuentes y ejecutar parches de seguridad en el sistema operativo. También se recomienda hacer copias de seguridad de los datos importantes y configurar adecuadamente la seguridad del navegador. Es importante no descargar aplicaciones o archivos de fuentes desconocidas y utilizar contraseñas seguras y diferentes para cada servicio.

- Además, se recomienda a los adultos mayores que se tomen el tiempo necesario para investigar y confirmar cualquier comunicación no solicitada o desconocida, sin importar cuán urgente parezca. Nunca deben proporcionar información confidencial, como contraseñas o información de tarjetas de crédito, en respuesta a una solicitud no solicitada. Tampoco deben descargar o ejecutar archivos adjuntos de desconocidos. Siguiendo estas medidas, los adultos mayores pueden proteger su seguridad en línea y disfrutar de Internet con mayor tranquilidad.

- Para proteger a los adultos mayores de las amenazas cibernéticas, es importante que las autoridades implementen leyes y sanciones más severas para los delincuentes cibernéticos que ataquen a esta población vulnerable. Además, es crucial que se ofrezcan programas educativos eficaces que no solo enseñen cómo utilizar las herramientas digitales, sino también cómo mantenerse seguro en línea y evitar amenazas de seguridad informática. Al aumentar la conciencia y educación sobre la ciberseguridad, podemos ayudar a prevenir que los adultos mayores sean víctimas de delitos cibernéticos.

- En virtud del estudio realizado, se ha destacado la urgente necesidad de que las entidades gubernamentales implementen medidas adicionales para proteger a la población adulta mayor de los delitos informáticos. Además de la implementación de normas más estrictas, es importante que se desarrollen manuales y programas educativos específicos para los adultos mayores, que les enseñen medidas efectivas de ciberseguridad para evitar ser víctimas de estos delitos. Al proteger a los adultos mayores de la discriminación y la vulnerabilidad que resulta de los delitos informáticos, tendrán la capacidad de disfrutar de las herramientas digitales sin limitaciones y aprovechar todos sus beneficios en la actualidad.

- La ciberseguridad es un tema crítico que aún no se ha abordado adecuadamente en nuestro país, lo que ha llevado a un desconocimiento generalizado tanto entre la población adulta mayor como entre los legisladores. Para enfrentar esta situación, es esencial implementar programas efectivos que permitan capacitar y educar a todos los niveles académicos sobre los riesgos y las consecuencias negativas de estas amenazas. Esto ayudará a combatir a los ciberdelincuentes y promover un acceso responsable a Internet y sus servicios.

BIBLIOGRAFÍA

ARANGO GOMEZ. Oscar Dario, El ABC de la seguridad informática: guía práctica para entender la seguridad digital, 2023, 93 p.

BAYONA ACEVEDO. Leydis, La transformación digital de las empresas colombianas en los últimos 5 años, 2022, 24 p.

BELTRAN. Cristian, Estudio de Seguridad en Dispositivos Móviles con Sistema Operativo Android, 2021, 81 p.

BENAVIDES. Blackwood, El fraude electrónico, 2022, 22 p.

BUENO. Laura, Ciberseguridad en Colombia, avances y retos, 2022, 20 p.

CALDERON OJEDA. Andrea Carolina, Prototipo de software de administración remota, 2020, 68 p.

CASTAÑEDA. Marlon Stiven, Panorama de Ciberataques más Recurrentes en Colombia 2021 y 2022, 2022, 6 p.

CONDORI. José Luis, Fases de un ataque a un Sistema Informático, 2020, 52-55 p.

CONGRESO DE COLOMBIA. Ley 1273 2009, {En Línea}. Accedido 9 de julio de 2022. https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf.

DANE. Encuesta de Tecnologías de la Información y las Comunicaciones en Hogares (ENTIC Hogares). Accedido 10 de diciembre de 2022. https://www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/tecnologias-de-la-informacion-y-las-comunicaciones-tic/encuesta-de-tecnologias-de-la-informacion-y-las-comunicaciones-en-hogares-entic-hogares.

DIAZ CANCECO. Terry, Transformación digital en la educación en tiempos del covid-19, 2020, 36 p.

DOMÍNGUEZ. Víctor, Backdoor de los antivirus, 2018, 114 p.

FUNCION REPUBLICA. Ley 527 de 1999, 10 de julio de 2022. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276.

GAMBOA SUAREZ. Jose, Importancia de la seguridad informática y ciberseguridad en el mundo actual, 2020, 12 p.

GARCIA. Jose, Deepfakes: the next challenge in fake news detection, 2021, 18 p.

GONZÁLEZ. Edwin Mauricio, Actualidad de Colombia en seguridad de la información, 2014, 6 p.

GONZÁLEZ. Jesús Audelo, Gusanos informáticos, 2015, 8 p.

GUAÑA. Javier, Ataques informáticos más comunes en el mundo digitalizado, 2022, No. E54, 87-100 p.

GUILABERT. Natalia, Actividades cotidianas de los jóvenes en Internet y victimización por malware, 2016, No. 22, 48-61 p.

HERRERA RODRÍGUEZ. Marcel, Desarrollo de análisis de riesgos aplicado a los troyanos backdoor en un equipo windows simulado, 2021, 52 p.

ICONTEC. ICONTEC e-Collection, {En Línea}. Accedido 9 de mayo de 2022. https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/.

LEGUIZAMÓN. Mayra Sheila Mariana, El phishing, 2015, 47 p.

LLAC SEMOERE David, Delitos informáticos. Delitos contra la intimidad, 2022, 29 p.

LYSENKO Sergii, Spyware Detection Technique Based on Reinforcement Learning, 2020, 12 p.

MEDINA PÉREZ. Victor, Seguridad adicional frente a ciber ataques Man-In-The-Middle, 2022, 85 p.
MEJÍA. Jazreel, Detectando aplicaciones maliciosas en Smartphone con sistema Android a través del uso de una aplicación, 2019, No. 31, 82-93 p.
MINTIC. Adultos mayores salieron del analfabetismo digital y entraron al mundo de las TIC. Accedido 11 de diciembre de 2022. http://www.mintic.gov.co/portal/715/w3-article-124707.html.
MOLINA. Yeison, Vulnerabilidades de los Sistemas de Información: una revisión, 2020, 11 p.
MONSALVE MENDEZ. Jaime Yesid, Ciberseguridad: principales amenazas en Colombia (ingeniería social, Phishing y Dos), 2018, 10 p.
MORENO. Jóse, Revisión sobre propagación de ransomware en sistemas operativos Windows, 2020, Vol 16, No. 1, 39-45 p.
MORENO. Milagros, Regulación global para evitar la suplantación de identidad digital, 2022, Vol 14, No. 6, 690-696 p.
QUIROZ ZAMBRANO. Silvia, Seguridad en informática: consideraciones, 2017, Vol. 3, 676-688 p.
QUIRUMBAY YAGUAL. Daniel Iván, Una revisión del aprendizaje profundo aplicado a la ciberseguridad, 2022, Vol. 9, No. 1, 57-65 p.
ROJAS VILLALOBOS. Bernal, Aprendizaje por defensa reactiva: el nuevo modelo de entrenamiento contra malware, 2021, 16 p.
RUIZ. Claudia Bibiana, Los ciberdelito y la ciberseguridad: una cuestión de género, 2023, No. 13, 73-84 p.
SALINAS PINEDA. Denis Neptalí, Análisis de un mecanismo de seguridad informática mediante el manual de la metodología abierta de testeo de seguridad, 2017, 17 p.
SÁNCHEZ BAUTISTA. Gabriel, Amenazas de seguridad a considerar en el desarrollo de software, 2022, Vol. 10, No 19, 31-37 p.
SECRETARIA SENADO. Leyes desde 1992 [LEY_1581_2012], {En Línea}, 10 de julio de 2022. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.
TAMAYO ARIAS. Johnny Alexander, Mitos y realidades de los virus informáticos, 2002, 8 p.
UGARTE ESPADA. Paola, Métodos Orientados a Reducir Ataques de Ingeniería Social en Organizaciones, 2020, 76-79 p.
VILCHEZ. Jose, Ciberseguridad y robo de información: Una revisión sistemática de la literatura, 2022, 20 p.
YANSENIS LÓPEZ. Matachana, Los virus informáticos: una amenaza para la sociedad, 2020, 33 p.