



## DISEÑO E IMPLEMENTACIÓN DE CAPACITACIÓN EN ADULTOS MAYORES PARA PREVENIR TÉCNICAS DE ENGAÑO DIGITALES - JAC - VILLA ALSACIA / SAN LUIS BOGOTÁ

### DESIGN AND IMPLEMENTATION OF TRAINING FOR ELDERLY ADULTS TO PREVENT DIGITAL DECEIT TECHNIQUES - JAC - VILLA ALSACIA / SAN LUIS BOGOTÁ

Laura Valentina Sandoval Guarín  
[lsandovalg@libertadores.edu.co](mailto:lsandovalg@libertadores.edu.co)

Francy Milena Castillo Gamba  
[fmcastillog@libertadores.edu.co](mailto:fmcastillog@libertadores.edu.co)

Andrés Eduardo Guevara Amaya  
[aeguevaraa@libertadores.edu.co](mailto:aeguevaraa@libertadores.edu.co)

Héctor Manuel Herrera Herrera  
[hmherrerah@libertadores.edu.co](mailto:hmherrerah@libertadores.edu.co)

### RESUMEN

Para analizar el impacto de los ataques de fraude y robo a través de medios digitales en los adultos mayores, especialmente en los barrios San Luis y Villa Alsacia, es necesario elaborar una breve explicación de términos relacionados con ingeniería social, regulación, derecho y conceptos con el fin de determinar cuáles son las técnicas de ingeniería social más utilizadas para afectar a este grupo etario de la población colombiana.

Otro aspecto importante es determinar si existen políticas o campañas por parte de los entes gubernamentales para mitigar y prevenir la ocurrencia de incidentes relacionados o provocados. Gracias a los ejemplos del mundo real de cómo los ciudadanos, entes gubernamentales y las empresas se han visto perjudicados y conlleva a identificar los problemas y clasificarlos como problemas socioeconómicos que pueden afectar a las familias de las personas, los entornos laborales o las empresas en general. Por lo tanto, es posible implementar conceptos básicos de ingeniería social y ciberseguridad a nivel educativo para poder reducir la brecha entre la ignorancia y el miedo.



El propósito fundamental es generar un estudio basado en el conocimiento que demuestren la relevancia de la protección digital para los adultos mayores, compartir recomendaciones para mantener a estas personas a salvo de los ataques de ingeniería social y posteriormente las organizaciones privadas y públicas protejan a las personas mayores más adelante. Se utiliza para aumentar la conciencia del personal, y como estrategia preventiva.

La importancia de este artículo es que se ha compilado un conjunto de buenas prácticas y recomendaciones que pueden ayudar a crear conciencia sobre la seguridad digital. Esta es una gran iniciativa para desarrollar una guía que sea segura para las personas que la usen, esto para que se tomen medidas de protección contra tales ataques.

***Palabras Clave: Engaño, Concientización, Ataque Digital, Phishing, Estafa, Smishing, Vishing, Ingeniería Social.***

#### **ABSTRACT**

In order to analyze the impact of fraud and theft attacks through digital media on older adults, especially in the San Luis and Villa Alsacia neighborhoods, it is necessary to elaborate a brief explanation of terms related to social engineering, regulation, law and concepts in order to determine which are the most used social engineering techniques to affect this age group of the Colombian population.

Another important aspect is to determine if there are policies or campaigns by governmental entities to mitigate and prevent the occurrence of related or provoked incidents. Thanks to real-world examples of how citizens, governmental entities and companies have been harmed and leads to identify problems and classify them as socioeconomic problems that can affect people's families, work environments or companies in general. Therefore, it is possible to implement basic concepts of social engineering and cybersecurity at the educational level in order to reduce the gap between ignorance and fear.



The primary purpose is to generate a knowledge-based study that demonstrates the relevance of digital protection for seniors, share recommendations to keep seniors safe from social engineering attacks, and subsequently for private and public organizations to protect seniors at a later date. It is used to increase staff awareness, and as a preventative strategy.

The importance of this article is that it has compiled a set of best practices and recommendations that can help raise awareness about digital security. This is a great initiative to develop a guide that is safe for people to use, so that measures can be taken to protect against such attacks.

***Keywords: Deception, Awareness, Digital Attack, Phishing, Scam, Smishing, Vishing, Social Engineering.***

## INTRODUCCIÓN

La ingeniería social se entiende comúnmente como la manipulación del comportamiento de una persona en el ámbito psicológico para comportarse de una manera particular y conducir a la divulgación de información confidencial. “La ingeniería social se basa en un conjunto de técnicas destinadas a lograr que una persona específica proporcione información confidencial. (AVAST, 2023). Como en este caso se trata de un procedimiento que va más allá de los prejuicios intelectuales y de los instintos básicos y, lo que es más importante es el engaño con el fin de recabar información. Arraigada en el mundo de la tecnología y el cibercrimen, la ingeniería social se conoce como la piratería humana. Es una de las herramientas más populares utilizadas por los ciberdelincuentes en todo el mundo. Esto se puede hacer en persona, por teléfono o por escrito, pero la ingeniería social se puede hacer a escala en las plataformas con más auge de hoy en día gracias al INTERNET.

El desconocimiento de los vecinos de las zonas de San Luis y Villa Alsacia, localidades de Chapinero y Kennedy tiene serias implicaciones para la ciberseguridad entre los adultos mayores. La forma en que se eduque a los ciudadanos sobre las técnicas de fraude digital tendrá un impacto significativo en la reducción de los ataques de ingeniería social, lo que hará que las personas mayores sean objetivos menos atractivos para los ciberdelincuentes. El diseño de la educación en diversas formas relacionadas con los grupos objetivo incluye



estas amenazas. Estas amenazas forman parte del concepto de cultura de seguridad de la información, definida como un conjunto de patrones de comportamiento que contribuyen a la protección de la información del público.

## **PREGUNTA DE INVESTIGACIÓN**

¿Cómo generar hábitos de buenas prácticas de seguridad digital en los adultos mayores de los barrios Villa Alsacia y San Luis?

## **OBJETIVO GENERAL**

Aumentar las buenas prácticas digitales enfocado a los adultos mayores con énfasis en instruir temas de Ingeniería social para disminuir riesgos de engaños y fraudes en los habitantes de los barrios Villa Alsacia y San Luis.

## **OBJETIVOS ESPECIFICOS**

- Analizar las encuestas realizadas reuniendo los principales tipos de fraude que requieren mejoras en conocimiento, acordando las medidas que se deben tener en cuenta para minimizar los fraudes encontrados hacia los adultos mayores.
- Diseñar una guía y una página web con las estrategias y controles de capacitación y educación para disminuir los fraudes y robos encontrados y a su vez promover los cuidados de los adultos mayores al momento de utilizar aparatos inteligentes.
- Realizar una capacitación a adultos mayores para las JAC mitigando la ignorancia en temas de ciberseguridad.



## **ALCANCE**

El público objetivo de esta guía no son sólo los vecinos de la zona designada, sino también determinadas personas, especialmente las personas mayores, de las JAC (Junta de Acción Comunal) de dicha zona. Según entrevistas personales sobre testimonios propios, suelen ser personas que viven en dichas áreas. Estas zonas son las más afectadas por el engaño de los medios digitales.

Por esta razón, las personas mayores necesitan utilizar activamente los medios digitales y saber qué peligros y amenazas representan para proteger su integridad, honor y dinero.

## **MARCO TEÓRICO**

Para el desarrollo del artículo, se define como adulto mayor personas pertenecientes al grupo etario de 60 años en adelante según el DANE (DANE, 2021). También se tuvo en cuenta la normatividad legal vigente en Colombia como: Ley 1581 de 2012, la Ley 1273 del 2009 y el decreto 1377 del 2013.

Gracias a las encuestas realizadas a los adultos mayores, se conoce la desinformación que existe en los barrios San Luis y Villa Alsacia sobre técnicas de engaños digitales. Los ciberdelincuentes se aprovechan de este desconocimiento para atacar y cumplir su objetivo engañando a esta población. Por medio de esta iniciativa, se capacitará en conocer e identificar llamadas de fraude, correos y mensajes de texto teniendo en cuenta una serie de TIPS que serán otorgados para que esta desinformación disminuya y el atacante no alcance su objetivo criminal.



## ANTECEDENTES

Se necesita una definición clara de delito informático o delito cibernético. Esto suele ser ilegal y se considera una conducta delictiva mediante el acceso a computadoras con la intención de destruir, dañar y/o robar componentes digitales o económicos, medios electrónicos y redes de Internet. Sin embargo, las categorías que integran y componen los delitos informáticos son muy complejas y pueden dar lugar a la ejecución de delitos tradicionales como la estafa, el hurto, la extorsión y la falsificación. Con los avances en la tecnología digital y la creciente cantidad de información procesada de esta manera, los delitos informáticos se han vuelto más comunes y ocupan más titulares casi todos los días.

Las principales modalidades de delitos informáticos según expertos en informática forense, referencian que esta clase de crímenes se encuentran agrupados en el Código Penal colombiano, mencionando los siguientes; acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño Informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, hurto por medios informáticos y semejantes y transferencia no consentida de activos, delitos amparados por la Ley 1273 de 2009. (Buitrago, 2014).

A su vez, el Código Penal colombiano contempla delitos que pueden cometerse por medios informáticos. En este sentido, cobran relevancia delitos como los delitos contra la intimidad, la malversación y revelación de datos personales sensibles, los delitos contra el honor, la injuria, la estafa, la estafa, el fraude energético, y se incluye de forma explícita el fraude en las telecomunicaciones. Modificados maliciosamente para ello, exhibición o uso de medios secretos, delitos contra la propiedad intelectual, delitos contra la propiedad industrial, delitos contra el mercado y contra el consumidor, publicidad engañosa donde se realicen afirmaciones falsas, o presenten características inseguras sobre sí mismos y causen un daño grave y tangible al consumidor. (Buitrago, 2014).

Con respecto a lo anterior, los tipos de organizaciones e individuos que cometen delitos cibernéticos varían según su experiencia, capacitación y objetivos. En última instancia, lo mismo ocurre con los que tienen poca experiencia (principiantes) y los que delinquen de



forma privada y autónoma hasta llegar al crimen organizado a través de redes virtuales y reuniones secretas y estandarizar métodos rentables de ciberataque, como suele verse. para proporcionarles bienes. Los llamados sujetos activos se ofrecen en el mercado negro.

El advenimiento de los delitos informáticos en Colombia no tiene un origen preciso ni una fecha concreta. Para los expertos en la materia, se cree que la práctica se introducirá formalmente cuando la legislación colombiana incorpore a la regulación los delitos informáticos y establezca sanciones para su ocurrencia. Colombia fue el primer país en tipificar como delito los delitos informáticos con la ayuda de la Ley 1273 de 2009. Denominada Protección de Información y Datos, también está sujeta al más alto grado de sanciones económicas en el Código Penal colombiano, a diferencia de otros países. La sanción económica más baja es el salario mínimo legal vigente de 100 millones de pesos mensuales, o casi 60 millones de pesos. Por delitos informáticos, las multas pueden llegar hasta los 600 millones, dependiendo del delito cometido. Sin embargo, el poder judicial de Colombia no está de acuerdo con esta ley y pueden surgir diferencias desde la perspectiva de cada juez al analizar el caso. (Buitrago, 2014).

Este tipo de delitos se perpetran en Colombia desde hace más de una década bajo la apariencia de delitos cibernéticos, y a pesar de la promulgación de la Ley Colombiana de Lucha contra las Amenazas Informáticas, esta regulación se ha impuesto a algunas personas jurídicas. Sería interesante hablar aquí sobre el desarrollo de los delitos informáticos en Colombia. Un punto de partida es la Ley de Delitos Informáticos, que es equivalente a la Ley 1273 de 2009. Reforma el Código Penal colombiano para respetar las disposiciones sobre la sanción de este tipo de infracciones y establecer penas y multas para los infractores.



## ESTADO DEL ARTE

El primer antecedente jurídico en Colombia sobre delitos informáticos es el Decreto 1360 de 1989. En este se reglamenta la inscripción de software en el Registro Nacional del Derecho de Autor para regular las reclamaciones por la violación de tales derechos. (Función Pública, 1989).

Siendo así, entendiendo el software como un elemento informático, las conductas delictivas consagradas en los Artículos 51 y 52, capítulo De las Sanciones, de la Ley 44 de 1993 sobre Derechos de Autor, que indican: “Incurrirá en prisión de dos (2) a cinco (5) años y multa de cinco (5) a veinte (20) salarios legales mínimos mensuales” e “Incurrirá en prisión de uno (1) a cuatro (4) años y multa de tres (3) a diez (10) salarios legales mínimos mensuales”, respectivamente, se tienen como las primeras normas penalmente sancionatorias de dichos derechos de autor junto con las consagradas en la Ley 1360 de 1989.

Con la Ley 599 del 2000 se expide la reforma al Código Penal colombiano en cuyo Libro Segundo Capítulo séptimo Título III consagra los delitos contra la libertad individual y otras garantías, que trata sobre la reserva e interceptación de comunicaciones (art. 192, 193, 194, 194, 196, 197 del Código Penal). Posteriormente, llega la Ley 671 de 2001 que constituye un Estatuto para prevenir y contrarrestar la explotación y el turismo sexual con menores de edad. (Función Pública, 2000).

También incluye la prohibición de servidores y proveedores de redes de información global. Estas son simples prohibiciones y socavan la eficacia de la ley, ya que la ley no prevé sanciones penales, solo sanciones administrativas.

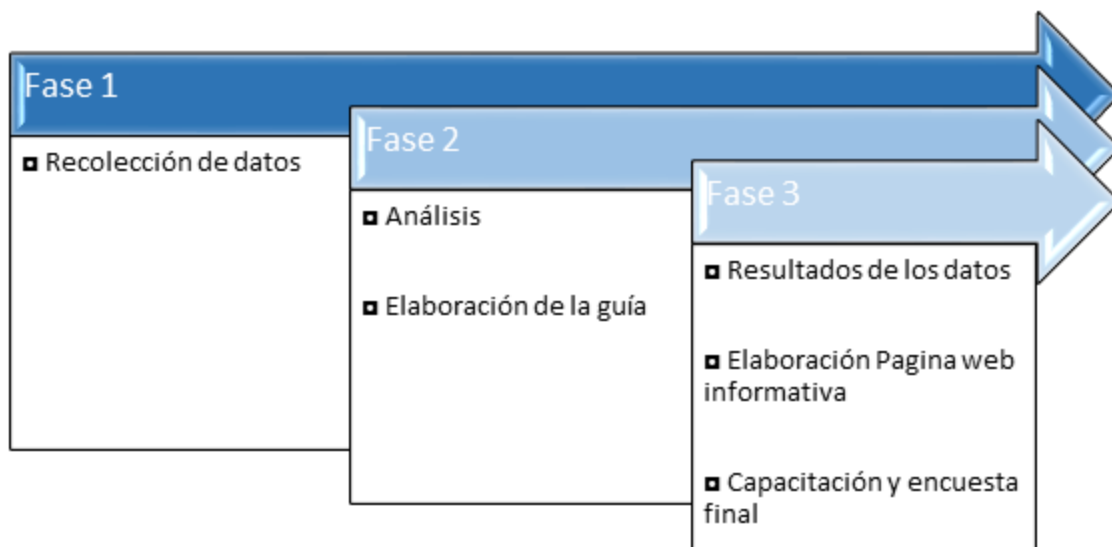
Con miras a remediar lo anterior, el 21 de julio de 2009 se sanciona la ley 1336 “por medio de la cual se adiciona y robustece le Ley 671 de 2001”. La Ley 1336 en su capítulo VI sanciona los tipos penales de turismo sexual y almacenamiento e intercambio de pornografía infantil.



Finalmente, la Ley 1273 de 2009 complementó el Código Penal y creó una nueva ley a través del concepto de “protección de información y datos”. Bajo esta ley, los delitos informáticos en Colombia están tipificados y tanto los organismos públicos como privados pueden atender estas violaciones antes de que se inicie un proceso penal en sus respectivos casos. Esto pone a Colombia a la par de los estados miembros de la Comunidad Económica Europea que han ratificado la Convención sobre Delitos Cibernéticos (la primera convención internacional sobre delitos cibernéticos firmada en Budapest, Hungría en 2001 y vigente desde julio de 2004). (MINTIC - Ministerio de Tecnologías de la Información y las Comunicaciones, 2021).

## METODOLOGÍA

Se extraerá una muestra de 50 habitantes en los barrios Villa Alsacia y San Luis en las cuales serán evaluados mediante una encuesta cualitativa los conocimientos que tienen en ciberseguridad y las diferentes situaciones a las que se han visto expuestos en las redes sociales o dispositivos móviles, para esto se plantearán diferentes situaciones comunes a los que habitantes se enfrentan en una plataforma digital con los resultados de dicho estudio se construirá una guía de buenas prácticas.



Gráfica 1 Fases de la Metodología. Fuente: Propia, adaptada de Word



Esta guía será llamativa ya que contendrá temáticas sencillas y de autoaprendizaje que sea de fácil entendimiento y facilitará a los habitantes de estos barrios y a su vez se pretende obtener atención instantánea para que ellos tengan un uso seguro de las redes sociales de las cuales hagan uso frecuentemente mediante sus dispositivos.

## RECOLECCIÓN DE DATOS

Se realiza encuesta creada para recolectar información relacionada con el nivel de conocimiento de los habitantes pertenecientes a la tercera edad, ubicado en las localidades de Kennedy y Teusaquillo, puntualmente en los barrios Villa Alsacia y San Luis, también tiene como fin recolectar diferentes testimonios de personas que han sido víctimas de este tipo de fraudes e identificar así, en estos barrios cuál es el método más usado por los ciberdelincuentes para instruir más a fondo en este tipo de engaños y como identificarlos.

**Encuesta de Ciberseguridad**

Fecha: \_\_\_\_\_ Grupo Etario (Edad): \_\_\_\_\_  
Barrio: \_\_\_\_\_ Nombre(Opcional): \_\_\_\_\_

¿Ha sido víctima de ataques por medio de correos electrónicos falsos, llamadas fraudulentas o páginas web engañosas? 

Si	No
----	----

**Si la respuesta anterior fue "Si", por favor brevemente describa el acontecimiento, de lo contrario coloque N/A:**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

¿Conoce el término "Phishing"? 

Si	No
----	----

¿Conoce el término "Smishing"? 

Si	No
----	----

¿Conoce el término "Vishing"? 

Si	No
----	----

¿Conoce el término "Ciberdelincuente"? 

Si	No
----	----

¿Conoce personas que han sido víctimas de fraudes por medio de llamadas, correos electrónicos, mensajes de texto o páginas web falsas? ¿Cuál? \_\_\_\_\_ 

Si	No
----	----

¿Conoce el alcance que puede tener caer en un ataque de fraude malintencionado digital? 

Si	No
----	----

¿Tiene en cuenta que **NINGUNA** entidad legal me solicitará datos con excusa de "Alta urgencia" sin dejar antes validar su proveniencia? 

Si	No
----	----

¿Cuida sus datos personales y conoce el alcance de compartirlos a un Ciberdelincuente? 

Si	No
----	----

¿Conoce métodos o TIPS de cuidados para no caer en estos ataques? 

Si	No
----	----

¿Le interesaría conocer más del tema para prevenir y compartir la información con familiares, amigos y compañeros? 

Si	No
----	----

¿Ha visto, conoce o ha sido parte de campañas y/o cursos en donde pueda capacitarse en Ciberseguridad? 

Si	No
----	----

Figura 1 Encuesta realizada. Fuente: Propia, adaptada desde Word



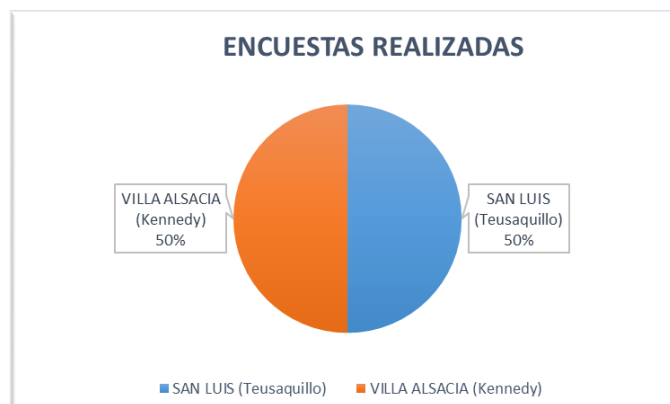
## ANÁLISIS Y RESULTADOS

Se evidencia que, en las localidades de Kennedy y Teusaquillo, puntualmente en los barrios Villa Alsacia y San Luis, respectivamente se encuentran varios antecedentes de delitos informáticos, en los cuales muchos de sus habitantes han sido víctimas, lucrando así a los Ciberdelincuentes.

En el entorno digital existen grandes riesgos y vulnerabilidades más cuando centramos nuestra vista en adultos mayores debemos tener muy en cuenta, que un gran porcentaje de adultos mayores no tienen conocimientos acerca de los peligros que se corren en la era digital, ya que el cambio de tecnologías y el abrupto avance de las telecomunicaciones ha logrado impactar en relación al manejo, entendimiento y uso de las mismas a una generación que venía acostumbrada a comunicarse de otras maneras menos invasivas, por dicha razón podemos ver como los Ciberdelincuente aprovechándose del desconocimiento engañan y manipulan para tener acceso a datos personales sensibles, dinero y hasta bienes.

Por estos motivos se realizan las encuestas para así tener más claro que temas se manejan y cuales se desconocen por esta población, para con esto crear una guía informativa y compartirla por medio de una capacitación con los temas de mayor desconocimiento, los riesgos y Tips para evitarlos o denunciarlos.

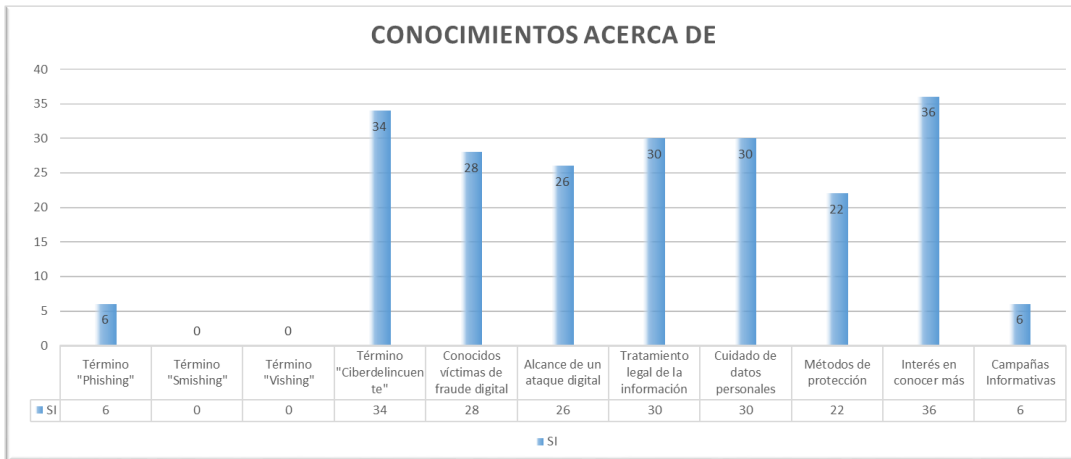
Después de realizar la encuesta en los dos barrios se evidencian los siguientes resultados



Gráfica 2 Personas encuestadas. Fuente: Propia, adaptada desde Excel



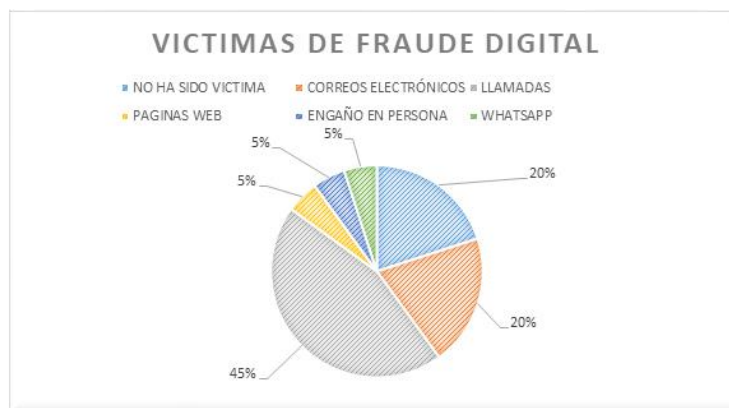
Se realizó un total de 25 encuestas por barrio, las cuales se evidencian las siguientes respuestas:



Gráfica 3 Respuestas de Encuestas. Fuente: Propia, adaptada desde Excel

Concluimos que el desconocimiento es amplio en los términos utilizados para nombrar estos tipos de fraudes, en donde curiosamente el 0% de los encuestados conocen el término "Vishing", más sin embargo es el tipo de fraude más común en los adultos mayores.

Se deja en evidencia que del 100% de los encuestados, el 90% manifiesta interés en conocer más acerca del tema de ciberseguridad y métodos para prevenir estos tipos de fraude, gracias a esto, se crea la necesidad de realizar una capacitación con los encuestados que aceptaron para ampliar sus conocimientos.



Gráfica 4 Encuestados Víctimas de ataques digitales. Fuente: Propia, adaptada desde Excel



Es claro que el ataque más común ha sido por medio de llamadas en un 45% y seguidamente los correos electrónicos en un 20%, por dicha razón se enfatizará en métodos para conocer cuando una llamada es verídica, y cuando puede ser hecha por un cibercriminal.

Únicamente el 20% de las personas no ha sido víctima de este tipo de ataques en primera persona, y más de la mitad, el 80% han tenido que pasar por este tipo de fraudes,

Se evidencia que un 5% de los encuestados fue víctima por medio de páginas web, los cuales comentan que fue a través de una página de pago en donde debitaron el valor de su cuenta pero nunca lograron obtener el producto, Cuando realizamos compras por internet debemos tener precauciones para poder identificar estafas más fácilmente, dentro de alguna de las precauciones como nos muestra en el artículo que debemos comprar solo en sitio Web seguros, evitar vendedores que utilicen tácticas para presionarlos a comprar, establecer alertas para cuentas bancarias como notificaciones por SMS cada vez que se realice cualquier tipo de movimiento, además de estar pendiente de que el número del que llega el mensaje solo tenga 5 dígitos.

Según está información obtenida, se genera la estructura para implementar en la capacitación de la mano con la Guía interactiva.



Figura 2 Estructura de la capacitación. Fuente: Propia, adaptada desde Canva



Se realiza la capacitación estructurada según la imagen (Figura 6), con el fin de mantener un orden de principio a fin y aplicar dinámicas en medio de las explicaciones teóricas para trabajar el conocimiento y mejorar la acogida de la información brindada hacía los asistentes.

## DISEÑO FLAYER PARA CAPACITACIÓN

Se realizaron diferentes métodos de difusión dentro de los cuales se encuentra el Flayer, el cual se comunicó a las diferentes personas y grupos pertenecientes a la junta de acción comunal, como también al coordinador del IDEPAC Teusaquillo (Jose Humberto Pedraza), quien difundió y resaltó la importancia al compartirlo en las redes sociales de Teusaquillo IDEPAC, para lograr así una mayor asistencia de personas interesadas en la seguridad digital.

**TALLER:  
PRÁCTICAS  
BÁSICAS EN  
CIBERSEGURIDAD**

Tips de prevención sobre ciberseguridad para adultos mayores

**Ingenieros de Sistemas  
Especialización en Seguridad de la  
Información**

Laura Sandoval Guarín  
Andrés Guevara      Francys Castillo

**LUGAR Y FECHA:**

- +57 30 435 60 362
- 5:30 pm. A 6:30 pm
- Martes 13 de junio
- TV 25 No 60 -10  
Restaurante Vegetariano Nirvana.  
Barrio San Luis  
Teusaquillo

Proyecto de Ciberseguridad para las JAC en CO.

Junta de Acción Comunal Barrio San Luis  
**JAC SAN LUIS**

GMLG

Nirvana  
Comida Saludable

Figura 3 Flayer Capacitación. Fuente: Propia, adaptado desde Canva

## DISEÑO DE GUÍA INTERACTIVA

La siguiente imagen es una muestra de la guía entregada en la capacitación a todos los adultos mayores asistentes para que puedan reforzar el conocimiento obtenido y también a su vez compartirlo con conocidos, familiares y vecinos.

**Phishing**  
Robo de identidad

Es una técnica que consiste en engañar al usuario para robarle información confidencial haciéndole creer que está en un sitio de total confianza. Esto se realiza a través de correos electrónicos o mensajes que incluyen un enlace que llevan al usuario al sitio web falso, el cual es una copia del original

**TIPO DE INFORMACIÓN ROBADA**

- Datos personales
- Información financiera
- Contraseñas

**RECOMENDACIONES**

1. Nunca hagas clic en enlaces contenidos en mensajes sospechosos
2. Nunca descargues archivos de mensajes sospechosos, estos pueden contener un programa malicioso
3. Con nuestro apoyo te ayudaremos a realizar copias de seguridad de tu información de manera periódica
4. Evita ingresar a sitios web de dudosa reputación o con contenido censurado
5. Utilizar contraseñas que sean complejas y cambiarlas periódicamente

**¿Qué es el Smishing?**

Es un ataque que usa mensajes de texto falsos para engañar a las personas para que descarguen malware, compartan información confidencial o envíen dinero a ciberdelincuentes

**RECOMENDACIONES**

1. Desconfiar de remitentes desconocidos.
2. No facilitar información que pide el mensaje, sobre todo si se trata de datos personales o bancarios. Ya que estas entidades nunca piden por SMS las claves de acceso ni datos de las tarjetas.
3. No hacer clic en los enlaces adjuntos.
4. Guardar las claves y la información bancaria mediante cifrado.
5. Evitar descargar aplicaciones desde mensajes de texto

**¡LO QUE SUBES A INTERNET, QUEDA AHÍ PARA SIEMPRE!**

Figura 4 Guía de la capacitación. Fuente: Propia, adaptada desde PowerPoint



## DISEÑO DE PÁGINA WEB INFORMATIVA

Se presenta una captura de pantalla de la página web creada por el grupo con el fin de compartir vídeos y textos explicativos acerca de los tipos de ataques, ejemplos y métodos para prevenir cualquier delito informático y como denunciarlos.



Figura 5 Página Web. Fuente: Propia. URL: <https://cuida-tu-informacion.web.app/>

## ENCUESTA POST CAPACITACIÓN

La siguiente imagen (Figura 10), representa la encuesta realizada al finalizar la capacitación, la cual tiene como objetivo analizar sus resultados y corroborar si se aumentó o no el conocimiento en seguridad digital en adultos mayores de los barrios aplicados.



## Pos-Encuesta de Ciberseguridad

Nombre: \_\_\_\_\_ Edad: \_\_\_\_\_

Barrio: \_\_\_\_\_

¿Conoce el término "Phishing"?

Si	No
----	----

¿Conoce el término "Smishing"?

Si	No
----	----

¿Conoce el término "Vishing"?

Si	No
----	----

¿Conoce el término "Ciberdelincuente"?

Si	No
----	----

¿Conoce el alcance que puede tener caer en un ataque de fraude malintencionado digital?

Si	No
----	----

¿Tiene en cuenta que **NINGUNA** entidad legal me solicitará datos con excusa de "Alta urgencia" sin dejar antes validar su proveniencia?

Si	No
----	----

¿Cuida sus datos personales y conoce el alcance de compartirlos a un Ciberdelincuente?

Si	No
----	----

¿Conoce métodos o TIPS de cuidados para no caer en estos ataques?

Si	No
----	----

¿Le interesaría conocer más del tema para prevenir y compartir la información con familiares, amigos y compañeros?

Si	No
----	----

¿Le pareció favorable y útil la capacitación sobre Ciberseguridad ?

Si	No
----	----

¿Conoce que tipo de detalles debe tener en cuenta para identificar una técnica de engaño?

Si	No
----	----

Califique la capacitación siendo 5 el más alto y 1 el más bajo.

--

¿Le parece importante que se repitan este tipo de eventos instructivos? ¿En qué Barrio?

Si	No
----	----

¿Existe algún sitio en Internet, correos oficiales para reportar la existencia de un ciberdelito? Si los conoce, por favor indicarlo \_\_\_\_\_

¿Qué mejoraría o aportaría a la capacitación presentada?

\_\_\_\_\_

\_\_\_\_\_

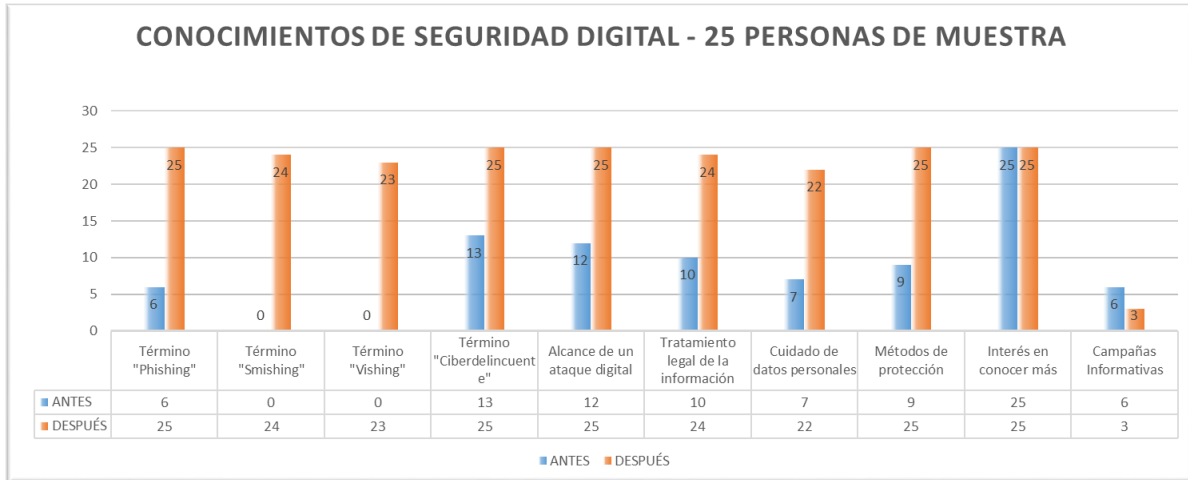
Figura 6 Post Encuesta. Fuente: Propia, adaptada desde Word

Se realiza la capacitación el día Martes 13 de Junio, en donde asistieron un total de 31 personas de las localidades de Teusaquillo y Kennedy, en donde se compartieron temas relacionados con Ingeniería social, los peligros y riesgos que corremos al momento de utilizar un computador o celular inteligente, también se les indicó el cómo se deben tratar, denunciar e identificar estos tipos de fraudes y se realizó un énfasis en continuar con la acogida a las nuevas tecnologías pero con conciencia clara y prevención.



Figura 7 Registro fotográfico capacitación. Fuente: Propia

Después de realizar la capacitación se aplicó esta encuesta (Figura 10), a todas las personas presentes, la cual deja en evidencia el siguiente análisis respecto a sus resultados:



*Gráfica 5 Comparación Post Conocimientos. Fuente: Propia, adaptada desde Excel*

Se generó una comparación entre el antes y el después de la capacitación aplicada con las mismas preguntas, en donde se refleja con una muestra de 25 personas, que efectivamente los conocimientos aumentaron notoriamente, por lo que se generó una buena acogida del tema explicado para los adultos mayores.

Varias personas colocaron sugerencias y puntos a incluir en las próximas capacitaciones, sin embargo, dejaron por escrito la favorabilidad y utilidad de los conocimientos compartidos durante el espacio, el cual fue del 100% de los asistentes, entre los puntos a mejorar están: "Muchos temas", escrito por una adulta mayor de 81 años, lo cual apunta a la importancia de generar capacitaciones separadas por rangos específicos de edad, ya que personas de 65 colocaron "Pueden hacer otra capacitación con más temas".



*Gráfica 6 Encuesta acerca de la capacitación. Fuente: Propia, adaptada desde Excel*



## CONCLUSIONES

Se aumentaron los conocimientos básicos en seguridad digital, como lo fueron términos, peligros, métodos y tips de prevención entre otros, logrando así disminuir los riesgos de engaño y fraude en los adultos mayores de los barrios Villa Alsacia, San Luis, y otros.

Se analizaron las encuestas realizadas, antes y después de la capacitación, la cual fue calificada por los asistentes quienes le colocaron una nota de 4.8 sobre 5.0, y en donde se evidencian la falta de conocimiento en los adultos mayores acerca de seguridad digital antes de, y el alto impacto reflejado después de la misma, dejando sobre la mesa la necesidad de que se realicen este y más espacios parecidos donde se les compartan distintos temas de tecnología, para que con ello, estas personas logren una acogida sin miedo y evitemos el rechazo al uso y apropiación de las nuevas tecnologías.

Con el fin de llevar a cabo la estrategia de aumentar el conocimiento y divulgarlo, se creó una guía, la cual fue entregada a cada uno de los asistentes a la capacitación con el fin de que fortalezcan lo aprendido y compartan esto con sus conocidos, vecinos, amigos y familiares, adicionalmente a esto, se les compartió la página creada por el grupo, en donde se apuntaron vídeos de enseñanza, entrevistas con personas de la tercera edad, y el botón en donde serán redirigidos a la página de la policía donde pueden hacer denuncias de todo tipo de fraude digital que noten en su diario vivir.

Se logró incentivar al adulto mayor al conocimiento y uso de la nueva era tecnológica, y con ello, sean parte de la Cibercultura sin que ningún ciberdelincuente pueda aprovecharse fácilmente de ellos.

Igualmente, desde el Ministerio de Educación Nacional, a partir de la plataforma de Colombia Aprende ([www.colombiaprende.edu.co](http://www.colombiaprende.edu.co)), programa que se establece como el principal punto de acceso y encuentro virtual de la comunidad educativa gratuita, en donde los adultos mayores pueden encontrar a cursos básicos de internet, biblioteca digital mundial de la UNESCO, guías para el uso responsable del internet, recomendaciones y catálogo de recursos para el aprendizaje.



## **AGRADECIMIENTOS**

- Junta de Acción Comunal San Luis
- Junta de Acción Comunal Campín
- Junta de Acción Comunal Villa Alsacia
- Leonardo Huertas Calle
- GMLG.ORG
- Restaurante Nirvana

A las Juntas de Acción Comunal, por fomentar en los adultos mayores pertenecientes no solo a estos barrios sino barrios aledaños la importancia de recibir esta capacitación y así poder aumentar sus conocimientos sobre estos inconvenientes que se presentan en el diario vivir de este grupo etario.

A GMLG y al Restaurante Nirvana por el apoyo y logística en los espacios suministrados.

Al ingeniero Leonardo Huertas Calle por la transmisión de su conocimiento a nosotros como ingenieros durante la especialización, ya que esto nos dio el punto de partida de nuestro proyecto de grado.



## GLOSARIO

### - **CIBERCULTURA**

La utilización de las nuevas tecnologías de la información y la comunicación de manera adecuada y responsable.

### - **ATAQUE DIGITAL**

Intentos maliciosos de acceder o dañar un sistema de computadoras o redes, donde pueden ocasionar pérdidas de dinero o robo de información personal.

### - **FRAUDE DIGITAL**

Estafa que sucede exclusivamente en el entorno digital.

### - **DELITO INFORMÁTICO**

Todas aquellas acciones ilegales, delictivas, antiéticas o no autorizadas que hacen uso de dispositivos electrónicos e internet, a fin de vulnerar, menoscabar o dañar los bienes, patrimoniales o no, de terceras personas o entidades.

### - **LEY 1581**

Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas.

### - **CIBERDELINCUENTES**

Es una persona cuyo conocimiento informático le permite realizar acciones delictivas en Internet

### - **CIBERSEGURIDAD**

Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual.



## REFERENCIAS

- AVAST. (25 de Enero de 2023). *¿Qué es la ingeniería social?* Obtenido de <https://www.avast.com/es-es/c-social-engineering>
- Buitrago, E. R. (19 de Noviembre de 2014). *Repositorio Unimilitar*. Obtenido de <https://repository.unimilitar.edu.co/bitstream/handle/10654/13452/Ensayo%20%20Edison%20Serrano%20EAS.pdf?sequence=1&isAllowed=y>
- DANE. (Enero de 2021). *Investigaciones*. Obtenido de <https://www.dane.gov.co/files/investigaciones/genero/presentacion-caracteristicas-generales-adulto-mayor-en-colombia.pdf>
- Función Pública. (23 de Junio de 1989). *Gestor normativo*. Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=10575>
- Función Pública. (24 de Julio de 2000). *Gestor normativo*. Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388>
- MINTIC - Ministerio de Tecnologías de la Información y las Comunicaciones. (18 de Marzo de 2021). *Noticias - Sala de Prensa*. Obtenido de <https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/56315:Gobierno-radico-Proyecto-de-Ley-para-adherirse-al-Convenio-de-Budapest-contra-la-ciberdelincuencia>