TRABAJO DE GRADO
Opción Seminario-Diplomado.

Vulnerabilidades Presentes en la Ingeniería Social

Estudiante: Fraiman Yesid Jimenez Moreno
Corporación Universitaria Remington.
Facultad de Ingeniería de sistemas
Seminario de Ciberseguridad y Ciberdefensa

Ingeniero Esp. ALFONSO VALENCIA MSc
TUNJA
2026

Resumen

Se abordará la ingeniería social desde todos los puntos posibles, la finalidad es crear buenos hábitos al momento de descargar o manejar información crítica con el fin de evitar perdida de datos sensibles como datos económicos o de infraestructura critica.

Mediante este estudio buscamos informar y ayudar a no caer en estafas o robos de datos, dando pautas y explicaciones precisas de los diferentes métodos de ataques, dando ejemplos con sus afectaciones en caso de que sucedan con el fin de que se pueda coger conciencia sobre este gran problema que cada día evoluciona y busca siembre nuevas víctimas. Buscamos identificar todas las posibles vulnerabilidades que genera la ingeniería social mediante un análisis de cada posible ataque entender cómo podríamos protegernos y evitar que nos afecte. La ingeniería social recurre al miedo y al afán lo cual deja a las víctimas en una situación de desesperación impulsándolos a acceder bien sea links o directamente sin saber a otorgar permisos a los ciberdelincuentes a sus datos, daremos a conocer las posibles soluciones para no caer en estos ataques enseñando buenos hábitos a la hora de verificar información y a no caer en la desesperación ni miedo.

Palabras clave: ciberataque, vulnerabilidades, información Sensible, miedo y hábitos

Tabla de Contenidos

Resumen....2
Objetivo General....4
Objetivos Específicos....4
Marco conceptual....5
Tipos de ciberataques....5
Leyes para la protección de datos....6
Mapa Contextual....6
Figura 1....7
Figura 2....8
Figura 3....9
Tabla 1....9
Capítulo I....11
Planteamiento del problema....11
Justificación....12
Alcance....13
Capítulo II....14
Implementación....14
Conclusiones....15
Soluciones a las Vulneravilidades....16
1. Aplicar el principio de «Desconfía y Verifica»....16
2. Implementar una política de «mínimos privilegios» en empresas....17
3. Usar autenticación multifactor....17
4. Activar bloqueadores de anuncios y extensiones de seguridad en navegadores....17
5. Redes Wifi seguras y VPN....18
6. Realizar simulaciones de ataques en empresas....18
7. Tener cuidado con llamadas telefónicas sospechosas (Vishing)....18
8. Mantener software y sistemas actualizados....19
9. Tecnologías de protección: filtros de correo electrónico....19
Referencias....20

Objetivos

Objetivo General

Identificar las vulnerabilidades presentes a un ataque de la ingeniería social y sus variantes, además de proponer buenas prácticas para evitar ser víctimas de estas.

Objetivos Específicos

- Identificar, indagar y clasificar los diferentes tipos de ataques usados mediante la ingeniería social.

- Se Propondrá una posible solución a cada tipo de ataque y darla a conocer a todos los que más tengan riesgo de verse afectados.

- Se dará a conocer la ley 1581 de 2012 a quien sea necesario con el fin de que sepan que sus datos siempre estarán protegidos.

Marco conceptual

En el sistema existen variedades de ciberataques en este caso nos enfocamos en los que más utilizan la ingeniería social para atrapar víctimas.

Tipos de ciberataques

- **El phishing:** es un tipo de ciberataque que se manifiesta a través de correos electrónicos, llamadas y mensajes de texto, donde se suplantan identidades con ligeras similitudes, como logotipos de empresas, redirigiendo a los usuarios a sitios fraudulentos que pueden robar información financiera o credenciales de acceso, lo que puede comprometer la seguridad de la empresa. A continuación, presentamos algunas de las variantes que han surgido a lo largo de los años.

- **Spear Phishing:** Esta variante se dirige a un individuo, grupo u organización específica; los atacantes recopilan información de redes sociales y sitios web para crear correos electrónicos altamente convincentes que buscan acceder a información sensible o instalar malware.

- **Smishing:** Esta técnica se enfoca en mensajes SMS, utilizando ingeniería social para generar urgencia o curiosidad mediante enlaces que, al ser abiertos, permiten a los atacantes acceder a datos privados o bancario

- **Vishing:** Esta variante utiliza llamadas telefónicas o mensajes de voz para engañar a las víctimas.

Leyes para la protección de datos

En contraste estas son algunas de las normas que más nos pueden ayudar para mantenernos seguros y evitar algunos de esos ataques.

- **Norma ISO 27001 de 2022:** Esta norma se estableció para implementar, mejorar y mantener un sistema de gestión de la información dentro de una organización.

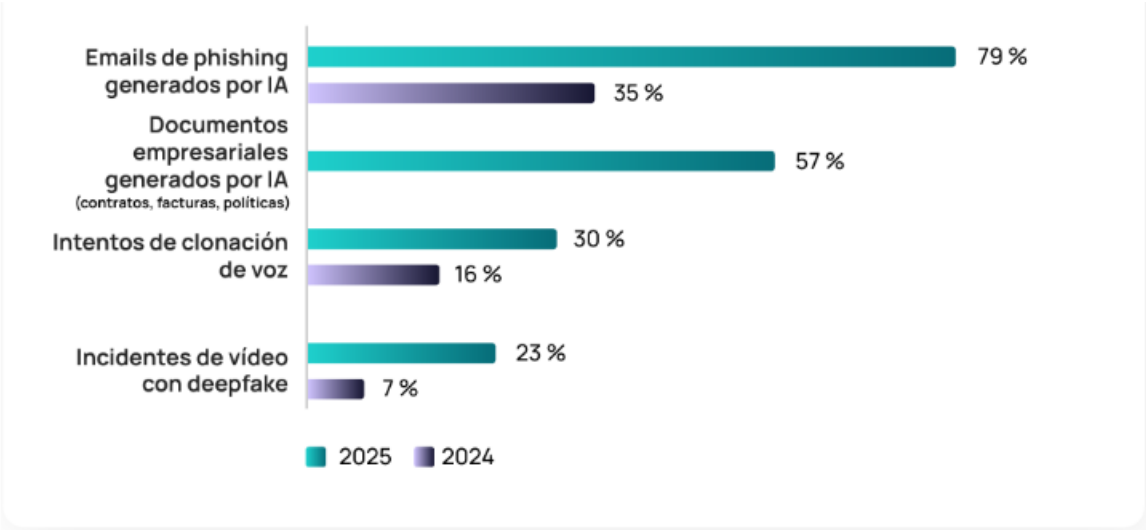
- **Ley 1581 de 2012:** La finalidad de esta es desarrollar el derecho constitucional de todas las personas a actualizar o rectificar lo amerite sus datos personales que hayan sido recopilados en bases de datos según la situación.

Mapa Contextual

Un estudio realizado en 2025 por sosafe nos muestra un aumento considerable en los ataques que usan la ingeniería social, se evidencia que el phishing representa el 69.8% de los ataques apoyándose en la ia, esta última les ha permitido a los ciberdelincuentes presentar ataques más sofisticados y de mayor volumen a las organizaciones. A su vez el 33% de estas organizaciones ya ha mostrado afectaciones por la evolución de estos ataques encontrando gran cantidad de correos phishing generados directamente por ia.

Figura 1

Ingeniería social impulsada por IA



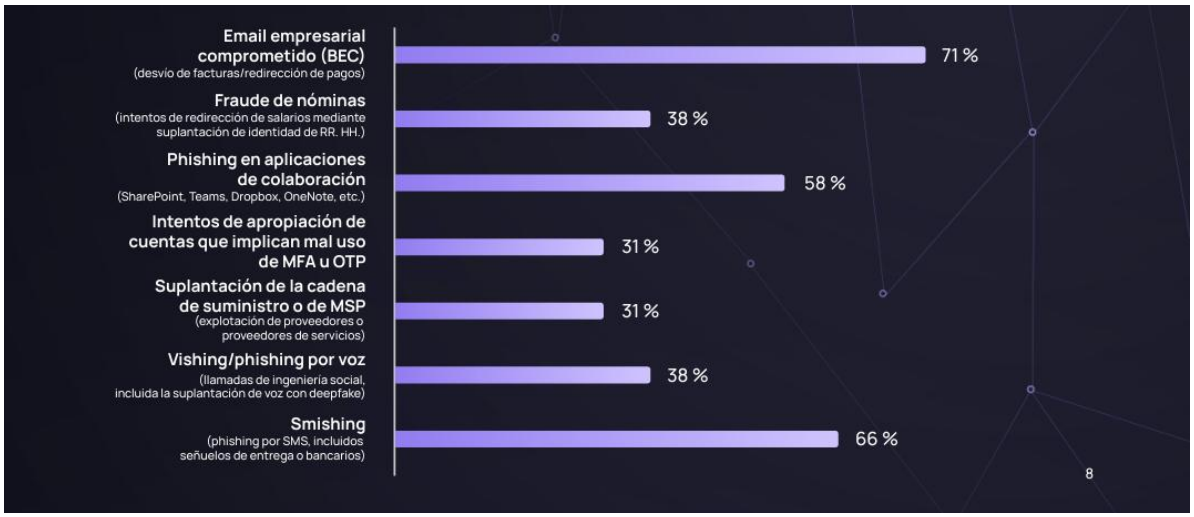
Fuente: Sosafe (En línea). Disponible en internet:www.sosafe-awareness.com/es/recursos/informes/informe-estado-ingenieria-social/

También se ven casos severos de ataques de ingeniería social a nivel multicanal atacando cada posible entrada a las organizaciones para atacarlas

haciendo creer que es flujo de trabajo, en este último año se han presentado un reporte del 51% de mensajes adaptados a un puesto de trabajo específico, y un 33% de intentos con imitación de procesos

Figura 2

Patrones de ataque a organizaciones en el último año



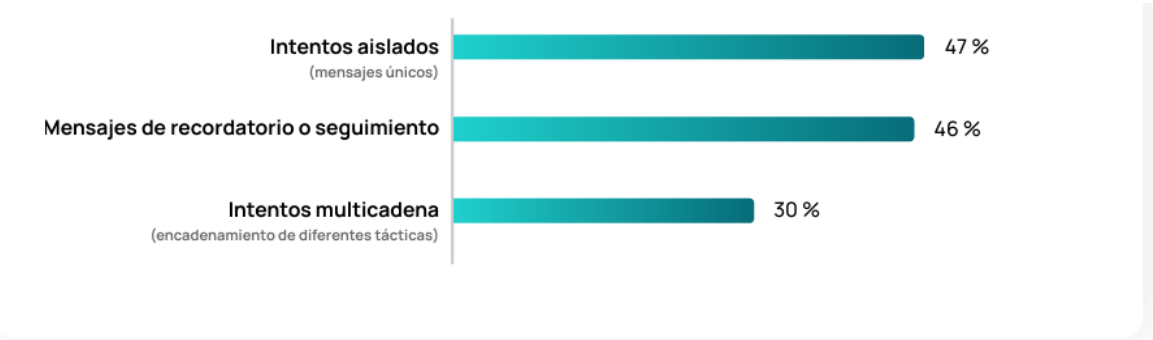
Fuente: Sosafe (En línea). Disponible en internet: www.sosafe-awareness.com/es/recursos/informes/informe-estado-ingenieria-social/

También hemos podido notar que los atacantes no se limitan a atacar una sola vez, tienden a intentar distintas formas una y otra vez, usando correos, llamadas y sms en ocasiones hasta simultáneamente buscando apoderarse de la mayor

cantidad de datos y generar un ataque a gran escala en las organizaciones. En este último año cerca del 28% de las organizaciones informan que los ataques aumentaron exponencialmente, por otro lado, casi un 50% reporto un aumento masivo en los mensajes de seguimiento por parte de los atacantes y cerca de un 30% informo de taques paso a paso a distintos puntos tratando de sortear la seguridad y acceder a la información. Esto se muestra en la figura 3.

Figura 3

Aumento de intentos de aplicar la ingeniería social



Fuente: Sosafe (En línea). Disponible en internet: www.sosafe-awareness.com/es/recursos/informes/informe-estado-ingenieria-social/

Tabla 1

Ciberataques en Colombia año 2025

Entidad	Ataque Usado	Fecha de ataque	Impacto del Ataque

Colpensiones	-Intrusión masiva -Escaneo automatizado -Fuerza bruta	Abril y mayo de 2025	Se intentaron cerca de 53000 millones de intentos para vulnerar la seguridad.
Emp	-Suplantación avanzada. -Desvió de transacciones.	23 y 24 de mayo del 2025	El canal de pagos fue comprometido y todo el dinero fue enviado a cuentas de terceros causando perdidas amplias
Avianca	-Archivos maliciosos -Instalación de quasar -Implementación de skimmers	Febrero y marzo del 2025	Se perdieron miles de millones, además de la marcación de fraude de muchas tarjetas de usuarios.
Sector comercio	Ransomware	24 de julio del 2025	Fue cifrado un servidor de información crítica para posteriormente proceder con la extorción.

Fuente: nsit (En línea). Disponible en internet: www.nsit.com.co/ciberataques-en-colombia-2025-los-incidentes-mas-relevantes/#:~:text=Los%20ciberataques%20en%20Colombia%202025%20marcaron%20un%20año,completo%20el%20panorama%20de%20riesgo%20en%20el%20país.

Capítulo I

Planteamiento del problema

La ingeniería social tiene un crecimiento desbordado el cual avanza de la mano con el avance tecnológico, esta se centra en el robo de información, suplantación de identidad e infiltración de malware, su principal arma es la desinformación por lo que se aprovecha del miedo incitando a dar información sensible o ingresar a links por afán sin tomar tiempo a indagar por el afán que aparentan al tener una amplia similitud con las entidades reales causando confusión y no permitiendo identificarlas, todos estos ataques llegan en muchos

de los casos por no tener buenos hábitos a la hora de cuidar nuestra información además de no tener una buena seguridad para protegerlos.

En los últimos años la suplantación de identidad ha sido una de las más usadas afectando tanto a entidades gubernamentales, organizaciones, así como a las personas, pero además de eso las distintas variantes de ciberataques que han venido surgiendo cada vez amplían más el alcance de afectación dejando cada vez más expuestas las vulnerabilidades y la necesidad de buscar soluciones que sean efectivas y permitan frenar su avance y tener más seguridad para todos.

Justificación

Identificar las vulnerabilidades de la ingeniería social ayudara a evitar pérdidas importantes en el tema económico, así como la perdida de información valiosa la cual puede ser usada de manera ilegitima causando suplantación de identidad, además de concientizar sobre lo delicado que es este tema hoy en día, en la red tenemos casi el cien por ciento de nuestra información y podemos estar a un clic de caer en una de estas estafas. Las identificaciones estas vulnerabilidades nos permitirán atacar anticipadamente los ataques y evitar pérdidas importantes y afectaciones a futuro que nos causen daños a la imagen propia, así como en la parte económica.

Uno de los principales problemas y el que más influye en estos ataques es el bajo conocimiento sobre el tama por parte de las personas u organizaciones lo cual los deja en una posición muy apta para los ciberataques en sus diferentes variantes, con un solo eslabón que logren infiltrar el daño que puede presentarse puede ser muy costoso y puede llegar a desencadenar ataques multicanales.

Alcance

Se planea llegar al cien por ciento de la totalidad de las vulnerabilidades, pero de manera completa dando la mejor calidad de información y entregando exactamente los puntos débiles y posibles soluciones para poder aconsejar de la mejor manera sobre el tema.

Buscamos identificar la mayor cantidad de vulnerabilidades de esta ingeniería analizando los antecedentes que se tengan, analizando las variantes y alcances de las mismas, dando así una información precisa y completa para que se puedan implementar en cada caso posibles soluciones y también saber cómo proteger la información personal así como la de las organizaciones implementando además concientización a la hora de abrir documentos o mensajes para no verse afectados y ser víctimas de alguno de ellos.

Capítulo II

Implementación

Se implementará una encuesta para indagar que tan profundos son los conocimientos sobre ciberataques implícitamente sobre la ingeniería social, basados en los resultados se procederá con las capacitaciones necesarias dando la información de acorde a las falencias encontradas y explicando a fondo con ejemplos y conceptos las normas y los posibles tipos de ciberataques de los cuales pueden ser víctimas concientizando a todos los involucrados en el manejo de información.

También será analizada la infraestructura digital con el fin de dar opciones de mejoramientos ante posibles vulnerabilidades que se detecten además de hacer énfasis en la implementación de buenas prácticas como indagar los documentos,

correos o mensajes de texto que se reciban, así como el cambio de contraseñas periódicamente y que estas sean amplias con caracteres muy variados con un mínimo de 20 letras.

Conclusiones

Identificamos un porcentaje alto de vulnerabilidades arraigados a la ingeniería social, al tomar acciones e informar puntualmente a las organizaciones se logra prevenir un numero de ciberataques que comprometan la integridad de la información crítica de la organización. Se capacito todos y cada uno de los involucrados en el manejo de la información crítica.

Logramos fomentar los buenos hábitos en las organizaciones lo que logro aumentar la seguridad y en contraste disminuir las afectaciones a causa de los ciberataques. Aunque sabemos que no es posible resolver al cien por ciento la afectación y evitar los intentos de ataques es preciso estar al tanto de todas las variantes de que utilizan la ingeniería social y estar constantemente vigilando las nuevas vulnerabilidades que surjan con estas.

Soluciones a las Vulneravilidades

La protección contra la ingeniería social requiere un enfoque multifacético que combine formación en seguridad, concienciación y el uso de tecnologías adecuadas.

1. Aplicar el principio de «Desconfía y Verifica»

Nunca confíes ciegamente en correos electrónicos, llamadas o mensajes que soliciten información personal o financiera. Antes de actuar:

- **Verifica la fuente**: Contacta directamente a la entidad a través de su sitio web oficial o número de teléfono.
- **Revisa la dirección de correo electrónico del remitente**: Los atacantes usan direcciones similares a las oficiales con pequeñas variaciones.

- **Cuidado con los enlaces y archivos adjuntos**: Pasa el cursor sobre los enlaces para ver la URL real antes de hacer clic.

2. Implementar una política de «mínimos privilegios» en empresas

En entornos corporativos, limitar el acceso a la información solo a quienes realmente la necesitan reduce la posibilidad de que un atacante obtenga datos críticos.

3. Usar autenticación multifactor

Incluso si un atacante roba una contraseña, la autenticación en dos pasos puede evitar accesos no autorizados. Usa aplicaciones como Google Authenticator o Microsoft Authenticator en lugar de SMS, ya que estos pueden ser interceptados.

4. Activar bloqueadores de anuncios y extensiones de seguridad en navegadores

Muchos ataques de phishing se ejecutan a través de anuncios maliciosos en sitios web. Extensiones como uBlock Origin o HTTPS Everywhere pueden evitar que hagas clic en enlaces peligrosos sin querer.

5. Redes Wifi seguras y VPN

Los atacantes pueden aprovecharse de redes Wifi-públicas para interceptar datos. Usa una VPN (Red Privada Virtual) y evita acceder a información sensible en redes no seguras.

6. Realizar simulaciones de ataques en empresas

Las organizaciones pueden realizar pruebas de phishing controladas para evaluar la reacción de sus empleados ante posibles ataques y reforzar la formación en seguridad.

7. Tener cuidado con llamadas telefónicas sospechosas (Vishing)

Los atacantes pueden hacerse pasar por representantes de bancos o empresas tecnológicas para obtener información. Nunca compartas contraseñas o códigos de seguridad por teléfono.

8. Mantener software y sistemas actualizados

Las actualizaciones de seguridad corrigen vulnerabilidades que pueden ser explotadas en ataques de ingeniería social. Activa las actualizaciones automáticas en todos tus dispositivos y aplicaciones.

9. Tecnologías de protección: filtros de correo electrónico

El uso de soluciones tecnológicas, como los filtros de correo electrónico, es esencial para prevenir que los mensajes maliciosos lleguen a las bandejas de entrada de los usuarios. Estas herramientas pueden:

- **Detectar y bloquear correos electrónicos fraudulentos**: Identificar patrones comunes en mensajes de phishing y evitar que lleguen al usuario final.
- **Analizar enlaces y adjuntos**: Escanear en busca de malware o redirecciones a sitios web falsos.
- **Implementar autenticación de remitentes**: Utilizar protocolos como SPF, DKIM y DMARC para verificar la legitimidad de los correos electrónicos entrantes.

Al combinar una sólida formación en seguridad con herramientas tecnológicas avanzadas, las organizaciones pueden reducir significativamente el riesgo de ser víctimas de ataques de ingeniería social. (cibersafety,2025, pag 4)

Referencias

Proofpoint (2022). Que es phishing y sus variantes. Sitio web: www.proofpoint.com/es/threat-reference/phishing

Gov.co (2012). Ley 1581 de 2012. Sitio web: www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#:~:text=La%20presente%20ley%20tiene%20por%20objeto%20desarrollar%20el,consagrado%20en%20el%20artículo%2020%20de%20la%20misma.

Iso.org (2013). Norma iso 27001 de 2022. Sitio web:

www.iso.org/standard/27001

Cibersafety (2025). Ingeniería Social: Riesgos y Protección. Sitio web: www.cibersafety.com/ingenieria-social-riesgos-proteccion

Mintic (2026). Ingeniería social. Sitio web: www.mintic.gov.co/portal/inicio/Glosario/I/18800:Ingenieria-Social