CIBERATAQUES, RIESGOS Y CONSECUENCIAS QUE HAN AFECTADO A LA POBLACIÓN COLOMBIANA ENTRE LOS AÑOS 2018 Y 2020

TATIANA ESPERANZA FIGUEROA CUBILLOS

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

CIBERATAQUES, RIESGOS Y CONSECUENCIAS QUE HAN AFECTADO A LA POBLACIÓN COLOMBIANA ENTRE LOS AÑOS 2018 Y 2020

TATIANA ESPERANZA FIGUEROA CUBILLOS

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

Directo Trabajo de grado
EDGAR MAURICIO LOPEZ ROJAS
Tutor de Curso
YENNY STELLA NUNEZ ALVAREZ

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

NOTA DE ACEPTACIÒN

_____

Firma del presidente de Jurado

_____

FIRMA DEL JURADO

_____

Firma del Jurado

Medellín. 28 de Septiembre 2022

CONTENIDO

FIRMA DEL JURADO 3

CONTENIDO 4

GLOSARIO 9

ABSTRACT 15

RESUMEN 16

INTRODUCCIÓN 17

1. DEFINICIÓN DEL PROBLEMA 18

1.1 ANTECEDENTES DEL PROBLEMA 18

1.2 FORMULACIÓN DEL PROBLEMA 19

2 JUSTIFICACIÓN 21

3 OBJETIVOS 22

3.1 OBJETIVO GENERAL 22

3.2 OBJETIVOS ESPECÍFICOS 22

4 MARCO REFERENCIAL 23

4.1 MARCO TEÓRICO 23

4.1.1 Ciberseguridad 23

4.1.2 Redes sociales 24

4.2 MARCO CONCEPTUAL 35

4.3 MARCO LEGAL 37

5. DESARROLLO DE LOS OBJETIVOS 39

5.1 IDENTIFICAR LAS DIFERENTES TÉCNICAS DE CIBERATAQUES MÁS FRECUENTES QUE SE HAN PRESENTADO ENTRE EL 2018 AL 2020 EN COLOMBIA. 39

5.2 DESCRIBIR LAS CONSECUENCIAS QUE GENERAN LOS CIBERATAQUES EN LA SOCIEDAD COLOMBIANA. 48

Ansiedad 50

5.3 EVALUAR LAS VULNERABILIDADES QUE EXISTEN EN LOS DISPOSITIVOS ELECTRÓNICOS COMO CELULARES, COMPUTADORES, Y LAS PLATAFORMAS DIGITALES MÁS UTILIZADAS POR LAS PERSONAS EN COLOMBIA. 53

5.3.1 Vulnerabilidades más comunes en los sistemas operativos de los dispositivos móviles más utilizados por los colombianos: 61

5.3.2 Vulnerabilidades en iOS: 62

5.3.3 Vulnerabilidades en plataformas de redes sociales 62

5.3.4 Vulnerabilidades en plataformas de mensajería instantánea 64

5.4 PROPONER UN MANUAL DE BUENAS PRÁCTICAS DE USUARIO QUE MITIGUEN EL RIESGO DE SUFRIR UN CIBERATAQUE EN LA POBLACIÓN COLOMBIANA. 65

5.4.1 Consejos para prevenir ataques en dispositivos móviles 66

5.4.2 Consejo para prevenir ataques en plataformas de mensajería instantánea 75

5.4.3 Consejos para prevenir ataques en plataformas de redes sociales 77

9. CONCLUSIONES 86

10. RECOMENDACIONES 87

11. BIBLIOGRAFÍA 89

LISTA DE FIGURAS

Figura 1 ¿Qué es el nodo de ciberseguridad? 24
Figura 2 El estado general del uso de móviles, Internet y redes sociales. 25
Figura 3 Redes sociales más usadas en Colombia. 26
Figura 4 Página principal de YouTube 27
Figura 5 Página para iniciar sesión en Facebook. 27
Figura 6 Chat de WhatsApp 28
Figura 7 Aplicación Instagram 29
Figura 8 Facebook Messenger 29
Figura 9 Línea de tiempo de los actos más relevantes respecto a los ciberataques. 30
Figura 10 Frases comunes en un ataque Phishing 32
Figura 11 Ataque Ransomware 40
Figura 12 Método de dispersión del Malware. 41
Figura 13 SIM Swapping. 42
Figura 14 ¿Tienes redes sociales? 44
Figura 15 ¿Con que frecuencia navegas por internet? 44
Figura 16 ¿Sabes que son ciberataques? 45
Figura 17¿Conoces los riesgos que tienes cada vez que realizas una publicación en redes o envías información por medios virtuales? 45
Figura 18 ¿Has sido víctima de un ciberataque? 46
Figura 19 Selecciona ¿Cuál fue el o los ciberataques que te realizaron? 46
Figura 20 ¿Sabes qué hacer cuando recibes un ciberataque? 47
Figura 21 ¿Inviertes presupuesto en ciberseguridad? 47
Figura 22 Money Mules 51
Figura 23 Delitos más comunes 52
Figura 24 Uso de dispositivos electrónicos en la sociedad colombiana 53
Figura 25 ¿Cuántos dispositivos utiliza para conectarse a internet? 54
Figura 26 Muestras analizadas por Sistema Operativo 55
Figura 27 Aplicación Corona APP 57
Figura 28 Formulario Web - Medellín me cuida. 58
Figura 29 Plataforma CaliValle Corona 59
Figura 30 App GAB (Bogotá cuidadora) 60
Figura 31 Plataforma Migración Colombia 61
Figura 32 Sistemas operativos más usados por las personas que realizaron la encuesta. 61
Figura 33 ¿Cuáles son tus redes sociales favoritos? 63
Figura 34 Contraseña Patrón 66
Figura 35 PIN Android 67
Figura 36 Cambiar contraseña en iOS 68
Figura 37 Eliminar datos de navegación en dispositivos. 69
Figura 38 Copia de seguridad en iCloud 70
Figura 39 Copia de seguridad en Google Drive. 71
Figura 40 App Store 71

Figura 41 Antivirus Kaspersky 73
Figura 42 Antivirus Avira.....74
Figura 43 Consulta sobre cuáles son las redes sociales más usadas por los Colombianos. 75
Figura 44 Pendiente actualización de YouTube en App Store.....76
Figura 45 Actualización de la APP de YouTube 76
Figura 46 Configurar privacidad en Facebook 77
Figura 47 Configuración de cada publicación en Facebook. 78
Figura 48 Depuración de contactos 79
Figura 49 Depuración de contactos en Instagram. 80
Figura 50 Cerrar sesión en Facebook.....81
Figura 51 Cerrar sesión en Instagram 81
Figura 52 Desactivar la localización en iOS.....82
Figura 53 Desactivar la ubicación en Android. 83
Figura 54 Denunciar en la página de la policía. 84
Figura 55 Página ADenunciar de la policía. 84
Figura 56 Continuación de la denuncia en la página ADenunciar de la policía. 84

LISTA DE ANEXOS

Anexo 1 Encuesta realizada a usuarios.....44

GLOSARIO

Análisis: Es la manera de entender un tema en específico, minuciosamente.

Autenticación: Medio que realiza la comprobación de identificación que permite a un usuario acceder un servicio o aplicación.

Ataques: Según la Real Academia de la Lengua Española[1], ataque se define como una acción de atacar, acometer o emprender una ofensiva.

Biometría: Es un método de reconocimiento de personas basado en sus características fisiológicas como (huellas dactilares, retinas, iris, cara[2]) En este tiempo es utilizada comúnmente en los dispositivos electrónicos, permitiendo un fácil acceso.

Caballos de Troya: Es un tipo de virus también conocido como troyano y es utilizado por ciberdelincuentes para acceder a la información de un usuario.

Ciber: Es un prefijo que se utiliza para denominar conceptos de las redes de internet.

Cibercrimen: Es cuando se comete cualquier tipo de actividad indebida en la informática, como redes, computadoras o cualquier otro dispositivo.

Ciberataques: Es un ataque informático organizado por una o un grupo de personas que provoca daños En un sistema informático o una Red. Estos ataques aprovechan alguna vulnerabilidad del recurso humano para acceder al software de algún dispositivo.

Ciberguerra: Es un enfrentamiento ejecutado en la web, que se deriva por causas tecnológicos dispositivos electrónicos.

---

[1] RAE. Ataque [en línea]. [Fecha de consulta: 29, de noviembre2020]. Disponible en https://dle.rae.es/ataque

[2] PAREJA. Deicy. ¿Pueden hackear tus datos biométricos con fotos de internet? [en línea]. agosto 08 de 2019 [Fecha de consulta: 13, de octubre 2020]. Disponible en https://www.pragma.com.co/blog/pueden-hackear-tus-datos-biometricos-con-fotos-de-internet

Confidencialidad: Es garantizar que la información almacenada en un sistema solo sea manejada por personas autorizadas y no por personas ajenas.

Crackers: Persona que ingresa sin autorización al Sistema e intenta sacar provecho.

Ciberstalking: Hace referencia al acoso que se realiza por medio de algunas tecnologías, el cibercriminal realiza una investigación obsesiva por una persona o empresa.

Darknet: Es una red ilegal que opera desde la Deep Web, donde comercia cocaína, heroína, pastillas y artículos ilegales.

Deep Web: Abarca la información que se tiene online, dicho contenido web no es buscado por el usuario en la red.

Delincuentes: Personas que cometen crímenes o actos indebidos muy a menudo.

Fraudes: Cometer prejuicio hacia alguien, es lo contrario a la rectitud.

Fraudes por de pagos en línea: De acuerdo a la información brindada por Asmar Salomón [3]informa que debido a la situación de la pandemia había una expansión de las transacciones En línea, por lo tanto, los pagos digitales han tenido un auge a favor De la población Evitando el contagio del coronavirus al utilizar efectivo y no salir de la casa. Como mencionamos anteriormente los puntos positivos también se incrementado los fraudes cibernéticos, operando de diversas formas como enviando un correo electrónico para solicitar dinero, solicitando donaciones para organizaciones o un correo electrónico de alguna entidad financiera, con el pasar Del tiempo los ciberdelincuentes adoptan medidas más creíbles hacia las personas para lograr su cometido, por lo tanto, hay que mantenerse informado y protegido.

[3] ASMAR SOTO Salomón. Transacciones digitales han aumentado, pero solo 20% de los usuarios las hacen [en línea]. Bogotá D.C 09 mayo de 2020 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible https://www.larepublica.co/especiales/el-boom-de-los-pagos-en-linea/transacciones-digitales-han-aumentado-pero-solo-20-de-los-usuarios-las-hacen-3036049

Grooming: Acto de abuso o pedófila que se realiza en por medio de una relación en línea con un menor de edad, involucrarlo en actos sexuales, por medio de imágenes y en conversaciones basados en sexualidad.

Gusanos: Programa diseñado especialmente para contrastar con algún virus informático o redes.

Hackear: Es ingresar a la información de una red, sistema, o computadora sin autorización y también se relaciona con la piratería.

Hacker: Persona que sabe acerca de redes de una manera más profunda, fallas de seguridad, y advierte de los errores a tiempo.

Ingeniería: Es el estudio de las tecnologías en diferentes ramas.

Informática: Es todo lo que trata las redes de datos, hardware, software y todo lo necesario para manejar la información.

Identidad: Información de datos que diferencian a una persona de otra.

Método Phishing: El BBVA como entidad financiera, invierte en de ciberseguridad para que sus clientes se sientan confiados en los procesos que realiza en dicho banco. Para el BBVA es importante ayudar a las personas y brindar de forma clara, información de algunos métodos. Esta modalidad de delito ejecutado por Internet, el cual llega un correo electrónico suplantando la identidad de un banco, con el fin de que la persona ingrese a una simulación de página de un banco e ingrese sus datos[4].

Método Smishing: Se realizan por medio de mensaje de texto y WhatsApp, haciéndose pasar por una entidad financiera, informando alguna novedad sospechosa con su tarjeta de crédito.

[4] BBVA. Phishing', 'Vishing', 'Smishing', ¿qué son y cómo protegerse de estas amenazas? [en línea]. España abril 25 de 2019 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible en https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

Método Vishing: La entidad financiera BBVA [5]indica que este método de estafa que suplanta alguna entidad bancaria a través de VoIP, solicitando a la víctima información personal para realizar el respectivo robo.

Pagos en línea: Es la modalidad de pagar algo en internet (forma electrónica).

Parental: Es un control de la internet, normalmente se usa para las restricciones de contenido sexual.

Pharming: Es una técnica de ciberataque que se deriva a partir del phishing, logrando desviar el tráfico para obtener datos de la víctima por un sitio web engañoso.

Sniffer: Es una herramienta utilizada por los gestores de redes que analiza la información, datos, y paquetes que circulan por la red.

Sniffing: Técnica que se utiliza para capturar información que circula por la red, como por ejemplo contraseñas, datos bancarios, etc. Es un ataque para robar información.

Social: De acuerdo con la definición realizada por Concepto definición[6] indica la pertenencia a una sociedad o grupo de personas que son participes de la misma cultura, se relacionan entre sí logrando conformar una sociedad. Al hablar de la palabra social se refiere a pertenecer a una comunidad, compartiendo cierto estilo de vida social, la correlación social, los modos de vivir, conformando una sociedad.

Ransomware: Es un método que se utiliza para infectar un equipo y de manera remota, bloquear y robar información para controlarla y así pedir un pago para el rescate de esta.

Red: Sistema que conecta entre sí a lugares para la comunicación de datos.

[5] Ibid., p.1
[6] CONCEPTODEFINICION. Social [en línea]. 13 enero de 2017 -. [Fecha de consulta: 29, de noviembre2020]. Disponible en https://conceptodefinicion.de/social/

Riesgos: Es algún tipo de información que puede ser expuesta y así se puedan cometer atentados o amenazas, eso ya depende de la vulnerabilidad de la información.

Spams: Se ve a menudo en los correos electrónicos, y es cuando algún tipo de información o comunicación digital no es solicitada, pero aparece constantemente.

Seguridad de las aplicaciones: Encaminada a defender el software y los dispositivos para manteneros libres de amenazas. Las aplicaciones se usan en el día a día, por lo tanto, si una aplicación se afecta esta puede abrir una puerta hacia el acceso de los datos que deben estar protegidos.

Seguridad de la información: La información confidencial debe ser protegida ya que el atacante puede robarla y cometer actos delictivos con los datos, por lo tanto, la seguridad de la información protege la integridad y la privacidad.

Seguridad de red: Protege y defiende una red informática de atacantes o de virus informático.

Suplantación: Técnica para conseguir información confidencial y en su mayoría sacar de ella provecho económico.

TI: Hace referencia a la información que es almacenada y procesada por los dispositivos tecnológicos.

Tracear: Es una forma de hacer rastreos de líneas telefónicas o direcciones y también se utiliza en el mundo hacker para desproteger programas.

Usuario: Se refiere a alguien que hace uso constante de un servicio, pueden ser redes sociales o aplicaciones.

Virus: Microorganismo que infecta y causa diversos malestares.

Virus informático: Es una amenaza para los archivos de un ordenador, se incorpora en el sistema y daña otros programas.

Vulnerabilidades: Es la capacidad mínima de una persona para pronosticar que su acto puede ser un peligro.

Xcode: Entorno de desarrollo exclusivo para iOS, actualmente solo se encuentra instalado en las MAC.

XcodeGhost: Es un malware que afecto varias aplicaciones de Apple, cuyo propósito era atacar directamente a Xcode.

ABSTRACT

This monograph inquired about the most frequent cyberattack techniques that occurred between 2018 and 2020 in Colombia, these dates were chosen because there was a world before and after the year 2020, causing alarming impacts on the Colombian population since childhood. until old age. In this way, the seriousness of the matter is measured and the little importance that people give to this type of criminal act, therefore, having information on the figures of the victims, of the attacks that occur, the risks to the that society is exposed by various technological means and the consequences that a cyber-attack leaves on a victim. Taking into account the research sources that were consulted, the way to help Colombian citizens is reasoned, indicating how to proceed, avoid and prevent this type of cyber-attacks, taking into account real experiences and how to proceed in the event that happen.

Through surveys and interviews, the analysis of a select group of people will be developed to identify how informed they are on the subject and what their vulnerabilities are, explaining the importance of protecting equipment, strengthening personal and business passwords, using security protocols , check the authenticity of links and profiles, avoid giving personal data either by telephone or unsafe pages, do not download pirated content, make a backup copy, report to the authorities through web pages or authorized lines.

RESUMEN

En esta monografía se indagó sobre las técnicas de ciberataques más frecuentes que se presentaron entre el 2018 al 2020 en Colombia, estas fechas fueron elegidas porque a nivel mundial hubo un antes y un después del año 2020, causando impactos alarmantes en la población colombiana desde niños hasta la tercera edad. De esta manera se dimensiona la gravedad del asunto y la poca importancia que le brindan las personas a este tipo de acto criminal, por lo tanto, al tener información de las cifras de las víctimas, de los ataques que se presentan, los riesgos a los que la sociedad está expuesta por diversos medios tecnológicos y las consecuencias que un ataque cibernético deja en una víctima. Teniendo en cuenta las fuentes de investigación que se consultó, se razona la manera de ayudar a los ciudadanos colombianos indicando como proceder, evitar y prevenir este tipo de ataques cibernéticos, teniendo en cuentas las experiencias reales y cómo se debe proceder en caso tal de que suceda.

Por medio de encuestas y entrevistas se desarrollará el análisis de un grupo selecto de personas para identificar qué tan informados están sobre el tema y cuáles son sus vulnerabilidades, explicando la importancia de proteger los equipos, fortalecer las contraseñas personales y empresariales, utilizar protocolos de seguridad, comprobar la autenticidad de enlaces y perfiles, evitar dar datos personales sea de manera telefónica o paginas no seguras, no descargar contenido pirata, realizar una copia de seguridad, denunciar a las autoridades por páginas web o a las líneas autorizadas.

INTRODUCCIÓN

A través de este trabajo se pretende generar en la población colombiana conciencia respecto al tema de Ciberataques entre los años 2018 al 2020, exponiendo las estrategias más comunes utilizadas por los cibercriminales a nivel nacional, que burlan la protección de las plataformas digitales y dispositivos tecnológicos, logrando obtener información personal y así cumplir con su objetivo.

Por esta razón se realizará un análisis qué permite identificar los riesgos y las consecuencias que estos ciberataques han generado. Dicho análisis se realiza bajo investigaciones que ha desarrollado el periodo El Tiempo, El Espectador, la revista Dinero, el Tanque de Análisis y creatividad de las TIC - TicTac de la Cámara Colombiana de Informática y Telecomunicaciones (CCTI) y la Policía Nacional - Centro cibernético, fuentes confiables que permiten un acceso fácil a la información, brindando datos reales y exponiendo algunos casos de ciberataques intentando evitar que más ciudadanos colombianos caigan estos tipos de fraudes.

Teniendo en cuenta que la tecnología cada día toma más control en la población, ¿Cómo puede la sociedad colombiana identificar si las páginas de internet que consulta son seguras? ¿Cómo identificar que la información que esté llegando a los correos electrónicos o mensajes de texto provienen de una entidad segura?, ¿Cómo se puede mejorar el proceso de enseñanza y aprendizaje sobre los temas de ciberataques, riesgos y consecuencias?, ¿Qué función cumplen las familias en este proceso cultural que capturan las redes sociales a las personas?, ¿Conoce cómo pueden robar su información?, ¿Cómo prevenir los ciberataques?, ¿Qué hacer en caso de que sea víctima de un ciberataque?

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Según el estudio Tendencias del Cibercrimen 2019-202[7], presentado por el Tanque de Análisis y Creatividad de las TIC (TicTac) de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y su programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) en asocio con el Centro Cibernético de la Policía Nacional, en Colombia los ciberdelitos se incrementaron un 54% del año 2018 al 2019, siendo los incidentes más reportados: los casos de Phishing, suplantación de Identidad, el envío de malware y los fraudes en medios de pago en línea.

La baja seguridad en los datos y en los sistemas de información sustentada en la falta de conciencia de la sociedad, genera que los ciberdelincuentes puedan acceder a información confidencial, logrando obtener datos personales y sensibles, que son utilizados con fines lucrativos, ya que la motivación de los ciberdelincuentes en Colombia es económica, las personas se ven muy afectadas ya que, sin importar su género o edad, son engañadas por las diferentes estrategias utilizadas por los ciberdelincuentes. El uso de los dispositivos informáticos, herramientas tecnológicas y el acceso a internet son cada vez más accesibles para toda la sociedad, quienes en algunos casos desconocen de los riesgos y amenazas que existen en internet y por lo tanto no se toman las medidas necesarias para evitar ser víctima de ataques informáticos y en otros casos se desconocen los procedimientos a seguir cuando se es víctima de los ciberdelincuentes.

Teniendo en cuenta la opinión de Morales[8], quien informa que las herramientas virtuales han sido de gran ayuda para muchos emprendedores y gente con ideas extraordinarias en Colombia, estas son las redes sociales; por medio de ellas han impulsado sus negocios a través de la publicación de imágenes, videos, contenidos, en vivos entre otros, y han generado trabajo a muchos colombianos, también han ayudado a superar personas por medio campañas sociales, siendo una fuente de inspiración para muchos de sus seguidores . Pero la falta de conocimiento de las personas en el uso adecuado de redes sociales y en las diferentes medidas de

[7] CCIT. Estudio tendencias del cibercrimen 2019-2020 [en línea]. Bogotá 2019-. [Fecha de consulta: 05 de octubre 2020]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

[8] MORALES, Juan David. Las redes sociales, un nuevo universo para emprendedores. [En línea]. Bogotá D.C 28, mayo de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible https://www.eltiempo.com/tecnosfera/novedades-tecnologia/las-redes-sociales-un-nuevo-universo-para-emprendedores-500800

seguridad que se deben tomar, hacen de esta herramienta un blanco para los ciberataques.

SPUTNI[9] informa que los delitos informáticos aumentaron en Colombia durante el año 2020, ya que con la emergencia sanitaria generada por la pandemia del Coronavirus COVID-19, se generó la necesidad de utilizar con más frecuencia los medios electrónicos para la adquisición de bienes, servicios o productos y el uso de tramites financieros, esto ha sido una oportunidad enriquecedora para los ciberdelincuentes. Por lo tanto, con el paso de los años han ido innovando de acuerdo a los avances tecnológicos que facilitan la vida de los colombianos, por esta razón, los ciber atacantes están alertas a las vulnerabilidades de la sociedad y de acuerdo a esto crean sus ataques.

1.2 FORMULACIÓN DEL PROBLEMA

Threat Intelligence Insider[10], es una plataforma de la compañía Fortinet encargada de ofrecer servicio de seguridad, recopiló y analizó los incidentes de ciberseguridad en todo el mundo indica, que en el año 2019 durante los primeros tres meses del año Colombia recibió aproximadamente 42 billones ataques cibernéticos, cifra que ya era bastante escandalosa. En el año 2020 a nivel mundial se inició una pandemia llamada Coronavirus, la cual obligó a muchas personas a trabajar desde casa, generando una puerta de entrada a los ciberdelincuentes a cada hogar colombiano. De acuerdo con El Espectador[11], los intentos de ciberataques en Colombia llegan a más de 5.400 millones entre el primer semestre del año. El aumento de esta actividad criminal se debe a la inseguridad que se ha incrementado por la pandemia. Los ciberdelincuentes trabajan con varias técnicas informáticas para lograr realizar el fraude de acuerdo a lo que requiera, una de sus modalidades es adivinar las credenciales de una víctima usando diferentes usuarios y contraseñas para acceder a un sistema, adicional al uso y configuración inadecuada del protocolo RDP para acceso a plataformas digitales, la falta de seguridad en los dispositivos electrónicos y la navegación entre páginas de procedencia dudosa, han facilitado el trabajo a los

[9] SPUTNI, PACHON. Andrés. Las redes sociales, un nuevo universo para emprendedores [en línea]. Costa Rica 06 de junio 2020-. [Fecha de consulta: 05 de octubre 2020]. Disponible en https://www.elpais.cr/2020/06/06/otra-pandemia-en-colombia-se-expande-por-correo-electronico/

[10] CIBERSEGURIDAD. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. [en línea]. Bogotá D.C 09 mayo de 2020 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible en https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

[11] TECNOLOGÍA. Detectan más de 5.400 millones de intentos de ciberataques en Colombia. [en línea]. Bogotá D.C 21 agosto de 2020 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible en https://www.elespectador.com/noticias/tecnologia/detectan-mas-de-5400-millones-de-intentos-de-ciberataques-en-colombia/

ciberdelincuentes, los cuales cada día se lucran con los fraudes que finalizan de manera exitosa.

Al ser víctimas de un ciberataque, se circula por una cadena de consecuencias y acontecimientos que perjudican gravemente la integridad de una persona. Los ataques y los objetivos pueden ser diferentes dependiendo de la meta del atacante, puede ser desde un robo o simplemente sabotaje. En la ejecución de los ciberataques se puede extraviar información confidencial o personal, acarreando pérdidas económicas o irrupción a la privacidad, robo de fotos que se guardaron con credenciales que el ciberdelincuente debe tener en su poder, desfalco en las cuentas bancarias, hurto de contactos del teléfono móvil para engañar a las personas haciéndose pasar alguien específico y muchas situaciones que crean estos ciberdelincuentes de manera audaz y creíble que atrapan a la población colombiana para caer en dichos actos.

¿Cuáles son los riesgos y las consecuencias generadas por los ciberataques en la población colombiana entre los años 2018 y el 2020?

2 JUSTIFICACIÓN

Debido a la gran influencia tecnológica que se tiene en los últimos años, la ola de ciberataques crece al mismo nivel, permitiendo que los cibercriminales generen una ganancia económica derivada por diferentes delitos como hurto por medios informáticos, violación de datos personales, acceso abusivo a un sistema informático, transferencia no consentida de activos y el uso de software malicioso. El factor humano sabe de la existencia de este tipo de delitos, pero no hay conciencia del gran peligro al que se encuentra expuesto.

La importancia de esta monografía radica en explicar los métodos más comunes que los ciberdelincuentes utilizan para realizar ciberataques a la población colombiana y sus consecuencias en lo económico y moral, revelando estadísticas de estudios y análisis realizados por diversas fuentes a nivel nacional. Estos ataques son ejecutados por diversos medios virtuales o telefónicos ocasionando daños irreversibles en una empresa o en una persona. En este trabajo se exponen los ciberataques, riesgos y consecuencias que han afectado a los colombianos en los últimos 2 años.

Los ciudadanos colombianos no conocen los riesgos a los que se exponen a diario por medio de sus redes sociales, ingresando a páginas no seguras o descargando un archivo en cualquier dispositivo sin tener conocimiento de su origen. Por lo tanto, es fundamental dar a conocer las buenas prácticas logrando fortalecer el avance cultural de la ciberseguridad, permitiendo aumentar la confianza digital tanto en empresas como en ciudadanos, con un dialecto poco técnico para entendimiento de las personas que por falta de conocimiento comenten errores permitiendo un ataque cibernético.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Identificar las estrategias más comunes utilizadas por los cibercriminales en Colombia, a través de las diferentes investigaciones realizadas por los organismos competentes con el fin de evitar algunos de esos ataques o disminuir sus impactos.

3.2 OBJETIVOS ESPECÍFICOS

Identificar las diferentes técnicas de ciberataques más frecuentes que se han presentado entre el 2018 al 2020 en Colombia.

Describir las consecuencias que generan los ciberataques en la sociedad colombiana.

Evaluar las vulnerabilidades que existen en los dispositivos electrónicos como celulares, computadores, y las plataformas digitales más utilizadas por las personas en Colombia.

Proponer un manual de buenas prácticas de usuario que mitiguen el riesgo de sufrir un ciberataque en la población colombiana.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Ciberseguridad: La compañía Kaspersky [12] dedicada a la seguridad informática, define que la tecnología ha traído un cambio drástico a la vida diaria de la comunidad colombiana, de trabajos y empresas, pero ha llegado cargado de amenazas cibernéticas. Una de las amenazas típicas es la seguridad de los sistemas informáticos, ya que todos los días se usan diversos dispositivos por diferentes motivos sea trabajo, entretenimiento, comunicación etc. Los riesgos qué anteriormente se veían lejanos a la existencia, han llegado apropiarse de la vida cotidiana, atacando a la población y a las empresas recibiendo amenazas diarias de robo de identidad, robo de información confidencial o chantajes. Por lo tanto, es importante tener herramientas que ayuden a detener este tipo de amenazas, las personas teniendo precauciones accediendo a sitios seguros, haciendo caso omiso a correos maliciosos, denunciando ante las autoridades cualquier acontecimiento no malo y respecto a las empresas la inversión necesaria que se tiene que hacer a la seguridad para guardar su información confidencial.

La falta de conocimiento de las personas respecto al tema de ciberseguridad ha permitido que muchos ciber atacantes utilicen diversas técnicas para cometer sus actos delictivos, por diversos medios, sea por redes sociales, modalidad telefónica, envió de correos electrónicos entre otros. Al abordar el elemento de ciberseguridad más inestable: las personas. Al incumplir las buenas prácticas de seguridad, por error una persona puede dejar entrar un virus en cualquier dispositivo electrónico.

El internet es considerado un campo de batalla ya que a nivel mundial se vive una ciberguerra por falta de conocimiento en la sociedad sobre ciberseguridad. El Ministerio de tecnologías de la información y las comunicaciones (MinTIC) [13] menciona que Colombia ha planteado la forma de buscar los lineamientos sobre las políticas de Ciberseguridad, encaminados a desplegar una estrategia nacional que hace frente al incremento de las ciber amenazas que impactan a la sociedad colombiana. Por tal razón el estado trabaja para minimizar el riesgo al que día a día, están expuestos sus ciudadanos.

[12] KASPERSKY. ¿Qué es la ciberseguridad? [en línea]. Agosto de 2019-. [Fecha de consulta: 24 de noviembre 2020]. Disponible en https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[13] MINTIC. Investigación, desarrollo e innovación. [en línea]. Bogotá D.C 07 septiembre de 2020 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible en https://www.mintic.gov.co/portal/inicio/Micrositios/I+D+I/Nodos/6120:Ciberseguridad

Los segmentos de desarrollo que se muestran en el Network Device Interface (NDI) se enfocan en fortalecer métodos que ayuden a la ciudadanía y autoridades a la formación de políticas públicas basadas en seguridad ciudadana, mejorando el posicionamiento de Colombia en procesos de seguridad, alineando estrategias nacionales derivadas de las entidades del estado y del sector privado. Como se puede observar en la figura 1, el nodo de ciberseguridad abarca la capacidad del estado permitiendo mitigar el riesgo a la ciudadanía respecto a incidentes en ciberseguridad.

Figura 1 ¿Qué es el nodo de ciberseguridad?

Fuente: https://www.mintic.gov.co/portal/inicio/Micrositios/I+D+I/Nodos/6120:Ciberseguridad.

4.1.2 Redes sociales: Son sitios web y aplicaciones que conectan a un mundo cibernético, permitiendo a la población mundial estar más conectada y en cierta forma sentir compañía así sea desde la distancia. También se comparten diversos intereses, noticias, fotos, videos, opiniones, estados de ánimo, música, foros, dependiendo de la red social y sus características.

El ser humano por naturaleza no quiere sentirse solo e intenta buscar compañía para su propio bienestar, por esta razón las redes sociales han sido una revolución notoria en la última década. El Internet y las redes sociales son parte fundamental en este tiempo, ya que son parte esencial del diario vivir. El mundo cibernético ha beneficiado a la comunidad colombiana, ya que, gracias a esto se puede tener información de primera mano de las novedades de los amigos, estar al día con las noticias, tener oportunidades laborales más tangibles o mirar la variedad de productos y servicios que son visibles teniendo en cuenta las preferencias del usuario. Rosgaby[14] describe en la figura 2 un análisis detallado entre el año 2019 y 2020, a continuación, se verá el estado general del uso de móviles, Internet y redes sociales.

Figura 2 El estado general del uso de móviles, Internet y redes sociales.

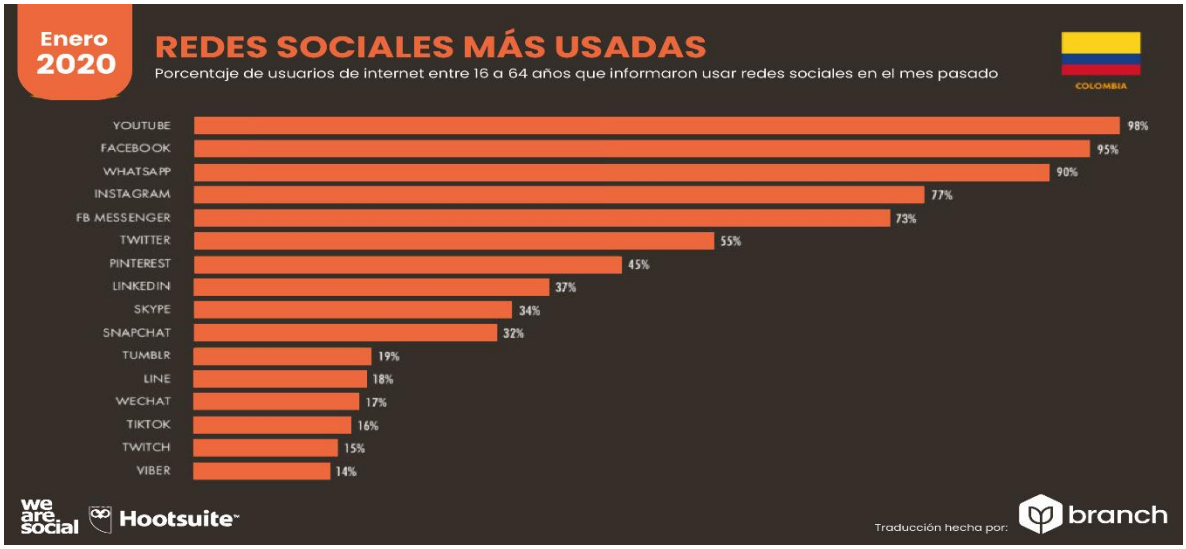
Fuente: https://branch.com.co/marketing-digital/estadisticas-de-la-situ

La mayoría de los colombianos utilizan el móvil de manera cotidiana, algunos llegan a tener hasta 2 líneas activas, ya sea por uso personal o corporativo, por lo tanto, esto explica por qué la cantidad de teléfonos conectados es de 60.38 millones el total de la población colombiana que es de 50,61 millones de personas. Por otro lado, los usuarios que se conectan a internet son 35 millones más de la mitad del

[14] MEDINA Rosgaby. Estadísticas de la situación digital de Colombia en el 2019 y 2020. [en línea]. Colombia 17 abril de 2020 -. [Fecha de consulta: 25, de noviembre 2020]. Disponible en https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2019-y-2020/#:~:text=de%20redes%20sociales-,El%2069%25%20de%20la%20poblaci%C3%B3n%20total%20de%20Colombia%20es%20usuaria,de%203.4%20millones%20de%20personas

total de la población, esto expresa porque hay tantas personas activas en redes sociales, como se muestra en la siguiente figura 3.

Figura 3 Redes sociales más usadas en Colombia.

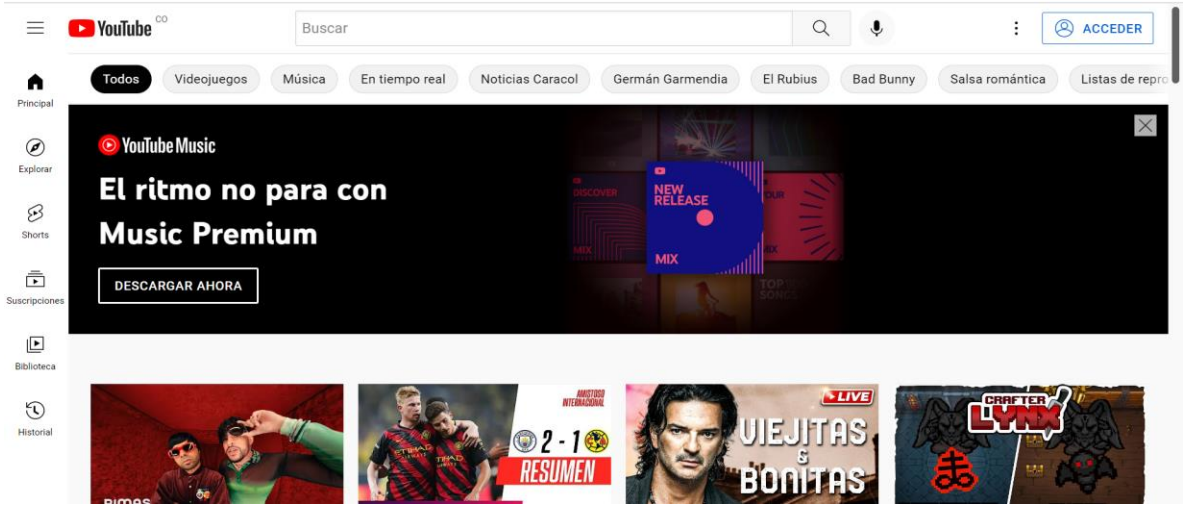


Fuente: https://branch.com.co/marketing-digital/estadisticas-de-la-situ

A continuación, se indicarán las 5 redes sociales favoritas por los colombianos:

4.1.2.1. YouTube: Es una plataforma virtual cuya función principal es facilitar la visualización de videos en streaming, es decir, verlos en línea sin tener que descargarlo en el equipo. Los usuarios, inician la búsqueda de acuerdo con lo que quiera ver y escuchar. Para acceder a la plataforma de YouTube, debe acceder al siguiente link https://www.youtube.com/ como se evidencia en la figura 4:

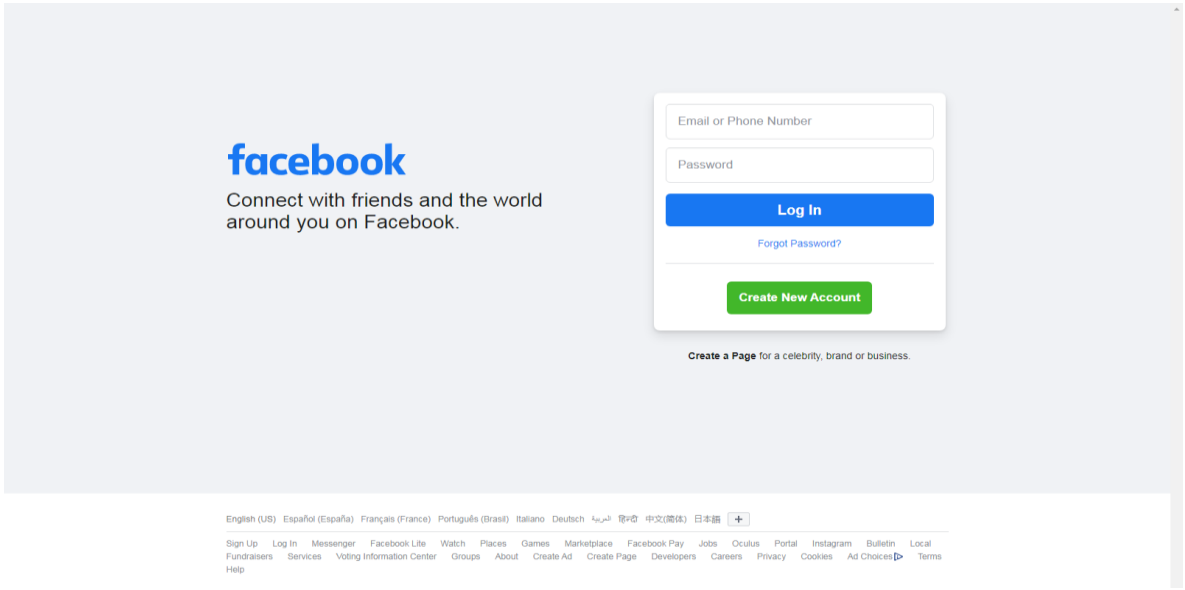
Figura 4 Página principal de YouTube



Fuente: https://www.youtube.com/

4.1.2.2. Facebook: Es una de las redes sociales más usadas a nivel mundial, su objetivo de creación fue poder mantener a las personas de cualquier lugar del mundo contactadas, adicional compartir información, como fotos, mensajes videos, música, grupos de interés entre amigos y familiares. Para acceder a la plataforma de Facebook, debe acceder al siguiente link https://www.facebook.com/ como se evidencia en la figura 5:

Figura 5 Página para iniciar sesión en Facebook.

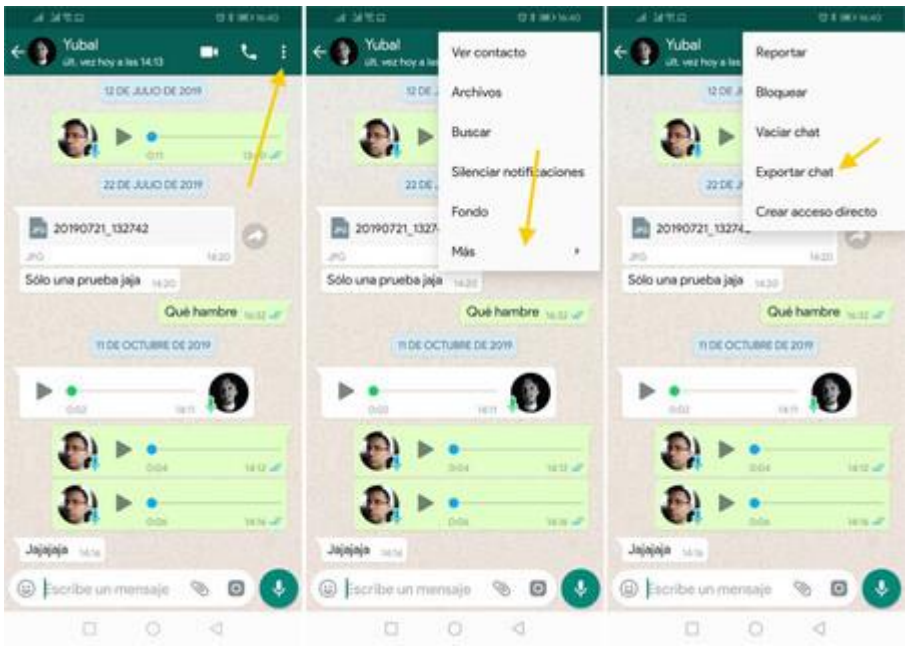


Fuente: https://www.facebook.com/

4.1.2.3. WhatsApp: Esta aplicación es de mensajería instantánea para smartphone, por medio de esta se envían y reciben mensajes al estar conectado a Internet,

adicional se pueden enviar imágenes, vídeos, audios, notas de voz, archivos, ubicaciones, también se pueden realizar llamadas y videollamadas, el detalle de la explicación brindada anteriormente, se puede observar en la figura 6.

Figura 6 Chat de WhatsApp



Fuente: https://www.xatakandroid.com/tutoriales/como-guardar-chat-whatsapp-verlo-tarde-como-aplicacion

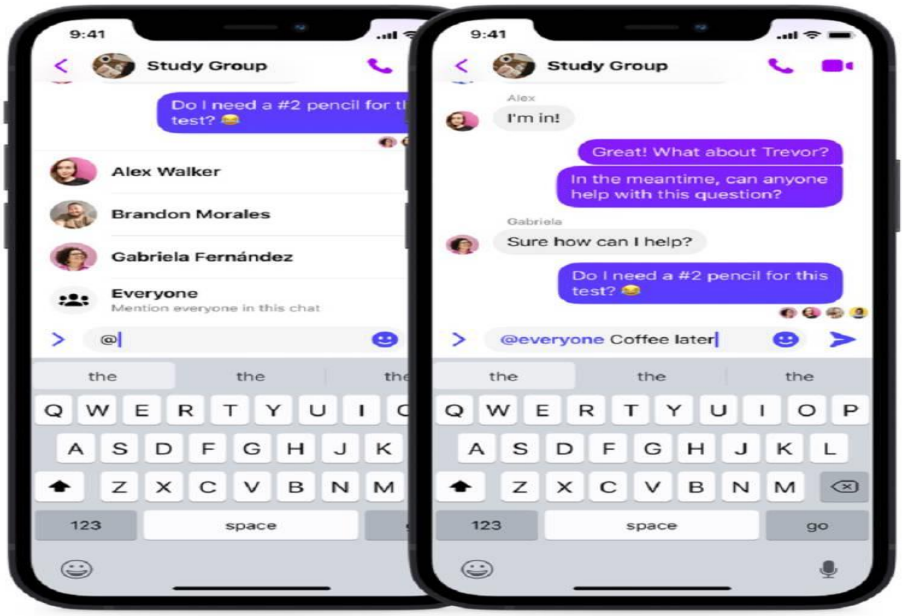
4.1.2.4. Instagram: Aplicación y red social visual cuya función principal es compartir fotografías y vídeos con los seguidores. Se puede instalar en cualquier teléfono inteligente ya que está disponible para sistemas operativos, Android y iOS. En esta aplicación como en Facebook, las empresas publican y ofrecen sus servicios para dar a conocer sus productos, ganar seguidores y la confianza de ellos, en la figura 7 se observa la página principal de Instagram.

Figura 7 Aplicación Instagram

Fuente: https://www.abc.es/tecnologia/redes/abci-instagram-no-quiere-usuarios-sigan-resubiendo-contanido-tiktok-social-202102101038_noticia.html

4.1.2.5. FB Messenger: Facebook Messenger es una aplicación de mensajería que permitiendo el intercambio de mensajes de los usuarios de Facebook. En este Messenger se chatea, se realiza llamadas de voz y videollamadas, así sea a un solo usuario o a un grupo.

Figura 8 Facebook Messenger

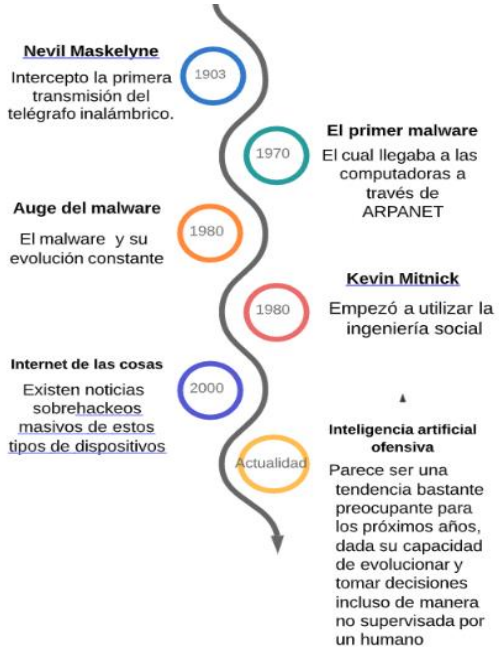


Fuente: https://cincodias.elpais.com/cincodias/2022/03/30/lifestyle/1648653594_790244.html

4.1.3. Ciberataques: Sofistic[15] habla brevemente de la historia de los ciberataques:

Desde el año 1988 el día 30 de noviembre se celebra el día mundial de la ciberseguridad, la principal causa de la celebración es intentar concientizar a la población sobre los riesgos qué tiene los diversos ciberataques que se realizan la población. Los ciberataques son un problema tanto para empresas, como para cualquier persona que utilice un dispositivo electrónico, teniendo en cuenta que el atacante sólo espera un error humano para aprovecharse de su vulnerabilidad, esto ocurre por falta de información, cultura y concienciación. En la figura 9, se detalla la línea de tiempo, con los respectivos actos de ciberataques:

Figura 9 Línea de tiempo de los actos más relevantes respecto a los ciberataques.



Fuente: Propia

El director del DANE, Oviedo Juan Daniel[16], indica que hay 50.3 millones de habitantes en Colombia, de acuerdo con la información anterior, se investiga ¿Cuántas personas tienen acceso a internet? El periodista Simón Granjas indica que:

> Es innegable que en los últimos años se ha hecho un esfuerzo por mejorar esta realidad. Según el Ministerio de las TIC, actualmente Colombia tiene 24,3 millones

[15] SOFISTIC. La breve historia de la ciberseguridad. [En línea]. Bogotá D.C 30 noviembre de 2019 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

[16] FORBES STAFF. En 2020 Colombia tendría 50,3 millones de habitantes. [En línea]. Bogotá D.C 31 enero de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://forbes.co/2020/01/31/actualidad/en-2020-colombia-tendria-503-millones-de-habitantes

> de conexiones a internet (entre fijo y móvil 4G) con una velocidad superior a los 10 Mbps, frente a 23,8 millones que están en las zonas más apartadas y no tienen este beneficio. “Lo anterior representa 9,4 millones de nuevas conexiones a internet con mayores prestaciones, durante el gobierno del presidente Duque”, según un comunicado de esa cartera[17].

Teniendo en cuenta la cita anterior se identifica que casi a mitad de la población colombiana no tiene acceso a internet, por lo tanto, la mayoría de las personas no tienen más información sobre ciberseguridad. Tecnosfera18 indica que en Colombia los ciberataques en el año 2019 tuvieron un incremento del 51% comparado con el año 2018, de acuerdo con el informe del C4 que brinda la policía en el país 28.827 casos fueron reportados y 15.948 fueron denunciados como infracciones a la ley 1273 de 2009, este análisis lo realiza los investigadores de las TicTac, la Cámara colombiana de informática y telecomunicaciones y el centro de capacidades para la ciber seguridad de Colombia de la policía nacional.

A continuación, se indicarán las amenazas principales en la web: Es importante conocer las principales amenazas en la Web en caso tal que se presente en una página en la que se esté navegando, de esta manera se podrá identificar el riesgo que se corre y así poder mejorar la seguridad en los dispositivos que se usan con frecuencia, con el fin de evitar problemas sufriendo algún robo de información, que ponga en riesgo los dispositivos o haya complicaciones al momento de navegar por la Red.

La Web redirecciona a sitios maliciosos 19 : Este es uno de los principales inconvenientes que afectan las páginas web, logrando poner en riesgo a los usuarios que ingresan a cualquier sitio web y es un tema que los propietarios de la página web deben tener en cuenta. Este ataque se realiza cuando el usuario ingresa a cualquier página y le da clic a un enlace que lo redireccione a un sitio diferente, por ejemplo, si se está navegando en cualquier página de noticias y se accede a un nuevo artículo, al darle clic se evidencia que lleva a la persona a una página diferente a la que quería acceder.

---

[17] GRANJAS, Matías. Colombia, uno de los países con más dificultades en acceso a internet [en línea]. Bogotá D.C 28, mayo de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/internet-calidad-de-conexion-en-colombia-con-mas-dificultades-en-el-mundo-529850.

[18] TECNOSFERA. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. [en línea]. Bogotá D.C 20, octubre de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

[19] JIMENEZ. Javier. Principales amenazas de seguridad en una web. [en línea]. Bogotá D.C 23 junio de 2021 -. [Fecha de consulta: 17, de marzo 2022]. Disponible en https://www.redeszone.net/tutoriales/seguridad/principales-amenazas-seguridad-web/

Los piratas informáticos logran inyectar código malicioso cuyo objetivo es cambiar los enlaces del sitio al cual se está accediendo, de esta manera el usuario al acceder al enlace infectado puede erradamente descargar un software malicioso y así tener un ataque Phishing.

Ataque Phishing: Es un método que se usa para engañar a la víctima haciendo que comparta sus contraseñas, números de tarjeta de crédito e información confidencial pasándose por una empresa de confianza y el método común utilizado es un correo electrónico, mensaje de texto o una llamada telefónica, como se explica en la figura 10:

Figura 10 Frases comunes en un ataque Phishing

Fuente: https://www.fundacionunam.org.mx/unam-al-dia/sabes-como-funciona-el-phishing/

Ataque Malware: Este ataque se realiza por medio de la instalación de un software con el fin de atacar a una víctima desde un ordenador, con el fin de robar información privada como datos personales, información financiera o comercial.

Ataques a la base de datos: Estos son orientados puntualmente a hacer el robo en la base datos, allí se obtiene información de todo tipo recopilado en la web, por lo tanto, el ciberatacante obtiene la información privada del usuario como correo electrónico, números telefónicos, nombres información puntual que guarda dicha base de datos.

Autenticación fraudulenta: Estos ataques van dirigidos a los inicios de sesión, los ciber atacantes buscan obtener credenciales y contraseñas del usuario y así pueden suplantar la identidad de la víctima. Adicional también puede generar un efecto

dominó y obtener cuentas y servicios con los que el usuario accede con la misma contraseña. Es fundamental que al momento de iniciar sesión se aseguren de qué la página a la cual accede sea una página web segura así evitar inconvenientes a futuro.

El área de tecnología del periódico El Espectador[20], informa que el año 2020, afectado a nivel mundial por una pandemia llamada coronavirus, la cual ha impactado de diversas maneras la economía a nivel global, también ha sido una oportunidad de lucro para los cibercriminales, ya que, se ha evidenciado el incremento de los ataques cibernéticos por el teletrabajo. Heidy Monterrosa [21]indica que el reto de las compañías en este año 2020 ha sido un mentar e invertir en ciberseguridad para proteger su información confidencial teniendo en cuenta que los sectores más impactados son las empresas, la salud, educación, finanzas y gobierno, con el factor común del error humano.

La revista Semana[22] informa que teniendo en cuenta que la actividad ilícita por la web ha incrementado debido a la pandemia del Coronavirus que ataca a nivel mundial. Debido al cambio de vida que se ha tenido en el año 2020 y el uso excesivo que se le está dando al internet, los ciberdelincuentes han implementado medidas para lograr cumplir con sus actos delincuenciales, a lo que se pregunta, ¿Por qué se han beneficiado los ciberdelincuentes en la pandemia? Con el fin de evitar algún tipo de contagio e impidiendo ser multados por no cumplir la orden de confinamiento, los colombianos utilizan diversos medios informáticos para cumplir con sus deberes, esto ha generado que los ciberdelincuentes estén realizando más ataques por diversos medios electrónicos para robar datos o dinero por medio de cuentas falsas de internet, esta actividad ilegal ha aumentado un 150%. El jefe del centro cibernético de la policía indica que el coronavirus ha sido una oportunidad para el cibercrimen, pero las autoridades ya se encuentran adelantando procesos judiciales contra personas que han cometido delitos cibernéticos, basado en el análisis de información confirma que hay 41 perfiles que están en judicialización.

[20] TECNOLOGIA. Detectan más de 5.400 millones de intentos de ciberataques en Colombia. [en línea]. Bogotá D.C 21 agosto de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.elespectador.com/noticias/tecnologia/detectan-mas-de-5400-millones-de-intentos-de-ciberataques-en-colombia

[21] MONTERROSA BLANCO, Heidy. Este es el costo en el que incurren las empresas al no detectar a tiempo un ciberataque. [en línea]. Bogotá D.C 19 septiembre de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.larepublica.co/internet-economy/este-es-el-costo-de-no-detectar-a-tiempo-un-ciberataque

[22] TECNOLOGIA. Delitos informáticos aumentaron en Colombia durante la cuarentena. [en línea]. Bogotá D.C 04 agosto de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.semana.com/on-line/tecnologia/articulo/delitos-informaticos-aumentaron-en-colombia-durante-la-cuarentena/662686/

El expresidente Duque en el congreso Andicom, Informa que en el transcurso de los años 2018 y 2020 considera qué están enfocados en la dirección correcta, mostrando la evolución que se ha tenido en el transcurso de estos dos años teniendo en cuenta los avances en la reforma del marco jurídico para telecomunicaciones. “Creo que, en estos dos años, nosotros tenemos que hacer de Colombia ese propósito de que Colombia sea el Silicon Valley de América Latina”, dijo Duque en el discurso de apertura. “Yo creo que estamos caminando la dirección correcta, en el marco regulatorio, en la inversión, en los proyectos, en la filosofía del Estado”[23].

Lo contradictorio de la información expuesta por el presidente de la República, es que las cifras muestran un incremento absurdo de los ataques que reciben los ciudadanos en Colombia. El diario El tiempo [24] informa que los crímenes informáticos en las empresas impactan económicamente alrededor de 1 billón de dólares al año, en el país en el transcurso del 2019 se produjo un incremento del 612% con ataques de malware, está Información es linda por la CCIT. Los procesos que debe realizar una empresa para de tenerte aquí de robo de información acarrea aproximadamente 280 días, generando un impacto negativo a la operación. Los ataques cibernéticos no sólo afectan empresas, afecta a cualquier tipo de persona que no tenga buenas prácticas para navegar por internet, impactando su privacidad ya que puede robar fotos, información personal, sus redes sociales etc. estos ataques genera un impacto negativo en la población víctima, por qué uno confía que su información esté segura, pero normalmente siempre hay alguien esperando leer rumano para ejecutar un ataque y lucrarse ilegalmente.
Es valioso que las empresas invierten en la seguridad para no tener su información confidencial vulnerable ante cualquier evento malicioso, así como muchas personas también conocen los riesgos, una de las estrategias que se puede implementar, Por medio de los mismo recursos que se utilizan a diario que son las redes sociales, se realiza diversas campañas con contenido de fácil entendimiento advirtiendo del peligro que hay al exponer cualquier tipo de información, ya que lo que se publica o envía por internet nunca vuelve a ser privado.

[23] FORBES STAFF. ‘Tenemos que lograr que Colombia sea el Silicon Valley de América Latina’. [en línea]. Bogotá D.C 02 septiembre de 2020 -. [Fecha de consulta: 08, de octubre 2020]. Disponible en https://forbes.co/2020/09/02/tecnologia/tenemos-que-lograr-que-colombia-sea-el-silicon-valley-de-america-latina/.
[24] TECNOSFERA. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. [en línea]. Bogotá D.C 30, octubre de 2019 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

4.2 MARCO CONCEPTUAL

Para hablar del tema, es necesario tener claro algunos conceptos para mejor entendimiento, haciendo referencia a los 5 ciberataques más utilizados por los cibercriminales en Colombia y otro tipo de definiciones específicas.

Análisis de riesgos: Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para tratar el riesgo.

Ciberdelincuentes: "Con el uso de las nuevas tecnologías para cometer ataques cibernéticos contra gobiernos, negocios e individuos, palabras y frases que hace una década apenas existían, forman ahora parte del vocabulario diario. Estos delitos no conocen fronteras, ni físicas ni virtuales, causan importantes daños y suponen un peligro muy real para las víctimas de todo el mundo. "[25] Son actos criminales, delictivos o ilícitos que implican el uso de ordenadores o de internet.

Ingeniería social: Procedimiento que utilizan los ciberatacante para mentir a los usuarios informáticos, con el fin de ejecutar una acción que causará efectos negativos, como descarga descargar un virus informático o la circulación de información confidencial o personal.

Ciberseguridad: Es una práctica que protege los dispositivos electrónicos como celulares, redes, sistemas electrónicos e información de ciberataques. De acuerdo con la información que brinda Kaspersky esta definición es aplicada en varios ámbitos, desde las empresas hasta la informática móvil.

Firewall: La función del Firewall o Cortafuegos es proteger un equipo, una red de ordenadores o servidores, dando indicaciones ante accesos no deseados ordenados desde una tercera red, es la primera línea de defensa ante un ataque de internet y debe ser capaz de evitar un acceso no autorizado antes de que el atacante entré a la red interna, ya que al acceder una persona malintencionada puede lograr obtener información confidencial importante para la empresa. Su ubicación principalmente se encuentra entre el punto de unión de dos redes, toda la información que se transmite por medio de router es analizado por los cortafuegos que se encuentre instalado en la red, si el tráfico es apto puede entrar o salir de la Red, si pasa lo contrario y no se cumple con las normas que se ha configurado

[25] INTERPOL. Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad. [en línea]. 11 agosto de 2020 -. [Fecha de consulta: 20, de noviembre2020]. Disponible en https://www.interpol.int/es/Delitos/Ciberdelincuencia.

automáticamente sale un mensaje bloqueado o que no se tiene acceso a la página por lo tanto no llegará al destino[26].

Control parental: Security Kids [27] indica que es una herramienta que permiten realizar un control para evitar que los menores de edad ingresen a contenidos de inapropiados en la web. Esta sería una excelente forma para controlar la visual que tienen los menores de edad, evitando ser expuestos al mundo de internet con ciertas precauciones, en los dispositivos informáticos, existe la opción de control parental, el padre realiza la modificación de acuerdo con lo que considere correcto.

Malware: Es un software malicioso, cuyo objetivo principal es dañar los sistemas de un dispositivo, siendo hostil, intrusivo, invasor de dispositivos electrónicos perjudicando o deshabilitando el sistema, redes, tabletas y dispositivos móviles, controlando las ejecuciones realizadas en el dispositivo.

- Redes sociales: Obeso Paula [28]indica que al existir una necesidad para el ser humano cómo es la cercanía con los suyos, estar comunicado, enterado de lo que ocurre a su alrededor, se inicia en el año 1995 la primera red social llamada ClassMates y de ahí se derivan muchas mejores en diversas aplicaciones para complacer a cada individuo de acuerdo con sus gustos y prioridades. La agencia de publicidad Neoattack [29], comunica que las redes sociales son aplicaciones que permiten socializar y comunicarse con personas a nivel mundial, de acuerdo con la Red social su gusto se pueden realizar publicaciones, comentarios, realizar anuncios, impulsar campañas y muchas cosas más. Las redes sociales más utilizadas a nivel mundial son Facebook, YouTube, WhatsApp, Instagram, Twitter, Skype, LinkedIn, Snapchat, Pinterest entre otras. Las ventajas de las redes sociales son la comunicación que es inmediata, el auge de oportunidades laborales sea para empresas grandes que tengan perfiles y soliciten empleados por sus redes o emprendedores que buscan salir adelante, entretenimiento, partir conocimiento de diversas culturas y temas, Ayuda al crecimiento de las marcas permitiendo explotar a un 100% todo el tema visual de algún producto o servicios que ofrezco una empresa. Así como existe un mundo de oportunidades positivas en las redes sociales también hay un sinfín de

[26] IDGRUP ¿Qué es un Firewall? [en línea].14 octubre de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://idgrup.com/firewall-que-es-y-como-funciona/

[27] SECURE KIDS. ¿Qué es el control parental y para qué sirve?
[en línea].25 agosto de 2015 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://securekids.es/que-es-el-control-parental-y-para-que-sirve/

[28] OBESO, Paula**.** Redes sociales: qué son, cómo funcionan, qué tipos existen y cómo influyen en las estrategias de Marketing. [en línea].12 diciembre de 2019 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://rockcontent.com/es/blog/que-son-las-redes-sociales/

[29] NEOATTACK. (15 de 10 de 2020). Redes sociales, ventajas y desventajas [en línea].15 octubre de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://neoattack.com/ventajas-y-desventajas-de-las-redes-sociales

desventajas cómo las estafas en redes, configuración de la privacidad, incumplimiento en las normas de uso, suplantación vi entidades, ciber bullying, Grooming, adicción a las redes y obsesión de personas que no conocen y quieren ser como ellas, y las empresas también afecta su imagen porque las críticas son más visibles y esto puede reducir la confiabilidad la empresa.

- Suplantación de identidad: Las validaciones realizadas por el grupo Ático 3430 comentan que es un problema muy común en esta época, debido al crecimiento de la era de internet y el auge digital, ha promovido a los ciberdelincuentes a que accedan de manera fácil cualquier identidad que se encuentre publicado en internet, este robo puede ser por medio de los correos electrónicos, redes sociales o simplemente teniendo información de la persona y se hagan pasar por cualquier persona, con el fin de cometer algún delito, obtener datos de manera ilegal, cometer cibercrímenes, hacer ciberbullying o Grooming. Una de las metodologías típicas de suplantación es crear perfiles falsos en redes sociales como Facebook, Instagram, Twitter, Tik Tok o si se ingresa por medio de correo electrónico obtienen tu número y pueden crear un perfil falso conforto teniendo acceso a todos contactos.

4.3 MARCO LEGAL

De acuerdo con la identificación de los ciberataques más comunes en Colombia, se indaga sobre la Ley 1273 de 2009 para identificar penalidad deben pagar los ciberdelincuentes al cometer este tipo de ataques cibernéticos. Teniendo en cuenta el documento expuesto por el Congreso de la República se obtiene la siguiente información.

4.3.1: Artículo 269I: Hurto por medios informáticos y semejantes: Al burlar las medidas de seguridad informáticas, ejecute un comportamiento inadecuado señalada en el artículo 239 (Hurto) operando un sistema electrónico, telemático, informático o una red, sustituyendo a una persona de manera ilegal, venciendo los sistemas de autenticación y de autorización determinados, incurrirá en la pena de prisión desde seis (6) a catorce (14) años.

4.3.2: Artículo 269F: Violación de datos personales. El ciberdelincuente que no esté autorizado para tener esta información, logrando obtener un beneficio propio o de

[30] ÁTICO 34. Suplantación de identidad. Tipos y causas [En línea]. 25 julio de 2019 -. [Fecha de consulta: 10 de octubre 2020]. Disponible en https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/

un tercero de manera ilegal, sustrayendo, ofreciendo, vendiendo, intercambiando, enviando, comprando, interceptando, divulgando, modificando datos personales o información de bases de datos, tendrá una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

4.3.3 Artículo 269J: Transferencia no consentida de activos. El ciberdelincuente, que con ánimo de lucro manipulando información, logre realizar una transferencia no aprobada por el dueño de la cuenta bancaria de cualquier activo. La pena sería de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes.

4.3.4 Artículo 269A: Acceso abusivo a un sistema informático. El ciberdelincuente, sin estar autorizado, accede a un sistema informático protegido, sin ninguna medida de seguridad o se conserve en dentro de dicho sistema burlando la seguridad. La pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

4.4.5 Artículo 269E: Uso de software malicioso. El ciberdelincuente, importe, obtenga, comercie, venda, remita, meta o saque de Colombia software malicioso o programas sean dañinos. La pena será de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

5. DESARROLLO DE LOS OBJETIVOS

5.1 IDENTIFICAR LAS DIFERENTES TÉCNICAS DE CIBERATAQUES MÁS FRECUENTES QUE SE HAN PRESENTADO ENTRE EL 2018 AL 2020 EN COLOMBIA.

Un informe realizado por la Cámara Colombiana de Informática y Telecomunicaciones[31] en el mes de octubre del año 2019, expone los diversos métodos que utilizan los ciberdelincuentes para atacar a las personas. La actividad actual de los ciberdelincuentes se visualiza de acuerdo con el crecimiento de las incidencias que reportan los usuarios afectados por medio de la página de la Policía Nacional o en la línea de atención de la Fiscalía General de la Nación. En el año 2019 la totalidad de casos registrados fueron 15.948 denunciando la violación a la ley 1273 de 2009.La policía Nacional indica que el 45% de las denuncias por ciberdelitos son realizadas por medio de la aplicación ADenunciar desde el año 2017 se han reportado 24.711 denuncias por ciberataques. En el año 2019 fueron reportados 12.879 incidentes de seguridad, esto quiere decir un 43% se gestionaron sin interponer algún tipo de denuncia. Entre el año 2018 y 2019 se evidencia un incremento del 54%, ya que, en el año 2018 se gestionaron 8.363 casos.

De acuerdo con las denuncias analizadas realizadas por los colombianos, se confirma que los ciberataques más utilizados por los ciberdelincuentes son, método Phishing con un 42%, Suplantación de Identidad 28%, virus malicioso 14% y robo por medio de pago en línea con 16%.

5.1.1 Delitos informáticos que más afectan a los colombianos según la CCIT[32]:

Hurto por medios informáticos: Teniendo en cuenta la cifra de denuncias del año 2019, con un total de 31.058 casos, encabeza la lista el hurto por medios informáticos. Su objetivo principal es llegar a las operaciones bancarias de los clientes, ya que por medio de sus dispositivos electrónicos se almacenen o se copia información digital. Por medio de este delito los ciberdelincuentes ingresan a las cuentas bancarias de los usuarios y realizar movimientos de dinero sin autorización del propietario.

Violación a los datos personales: Se produce cuando la información de una persona sufre un incidente de seguridad, esto genera el robo de identidad. Es el segundo caso más reportado por los colombianos, con un total de 8.037.

[31] CCIT. Estudio tendencias del cibercrimen 2019-2020 [en línea]. Bogotá D.C. 2019-. [Fecha de consulta: 05 de octubre 2020]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf
[32] Ibid. p. 8

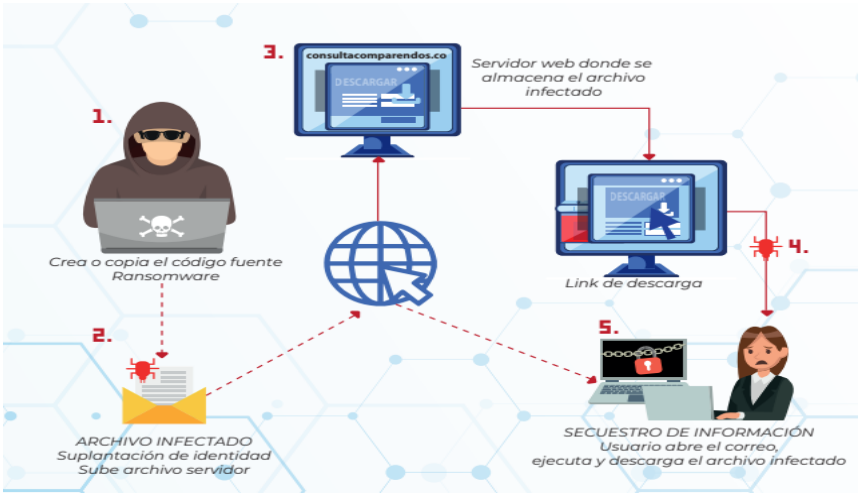
Acceso abusivo a sistema informático: Es el tercer delito más denunciado con 7.994 casos; Los cibercriminales acceden de manera ilegal a un sistema, comprometiendo su información expuesta solo para personal autorizado.

Transferencia no consentida de activos: Con 3.425, ocupa el cuarto lugar. El comportamiento criminal permite al atacante quitar el dinero de una víctima o realizar transferencias de activos financieros.

Uso de Software Malicioso: Por último, ocupando el quinto lugar se encuentra reportado con 2.387 casos.

Ransomware: La CCIT [33] indica que una de las estrategias que utilizan los ciberdelincuentes realizan un envío masivo de correos electrónicos, especificando en el asunto algo critico que capte la atención de las personas. Al dar clic para abrir el correo este puede tener enlaces o archivos adjuntos como fotos de comparendo, citaciones o embargos judiciales, notificación de transferencias no realizadas, reporte en las centrales de riesgos. El medio de propagación más utilizado del Ransomware es de tipo Lockscreen este bloquea el acceso al equipo. Al engañar a un usuario su información se dirige a un servidor que descargar el malware. Al ejecutar el archivo infectado, cifra los datos de información, ejecutando su ataque exigiendo dinero a cambio de restablecer la información. Existen ataques de Ransomware que retiene la información de los móviles. En la figura 11 se explica cómo se realiza el ataque, este se ejecuta por medio de un enlace enviado a través de un mensaje de texto o chat.

Figura 11 Ataque Ransomware



Fuente: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

[33] Ibid. p. 19

La Cámara Colombiana de Informática y Telecomunicaciones[34] informa algunos tipos de Ransomware detectados en Colombia.

- Ransomware de cifrado: Este virus cifra los archivos, imágenes y videos de la víctima.

- Ransomware de cifrado de servidores web: Este va direccionado a los servidores web para cifrar sus archivos.

- Lock Screen Ransomware WinLocker: Este realiza el bloqueo del monitor y solicita una suma de dinero para liberar la información.

- Master Boot Record (MBR) Ransomwarealware: El ataque va directo al disco duro de la máquina permitiendo tomar el control de ella.

- Ransomware de dispositivos móviles: Los dispositivos móviles se infectan por medio de descargas no autorizadas.

- Malware: Continuando con los análisis realizados por la CCIT [35]especifica que los ciberdelincuentes utilizan el programa maligno con varios propósitos, tales como obtener datos personales y contraseñas, hurto de dinero o bloqueo de un dispositivo. Este es un software malicioso que afecta una máquina, móvil u otro dispositivo. Es considerado un software dañino, ya que está programado para acceder a diversos dispositivos sin previa autorización del usuario logrando obtener información de los datos de la víctima, en la figura 12 se puede observar los métodos por los cuales realiza el ataque.

Figura 12 Método de dispersión del Malware.

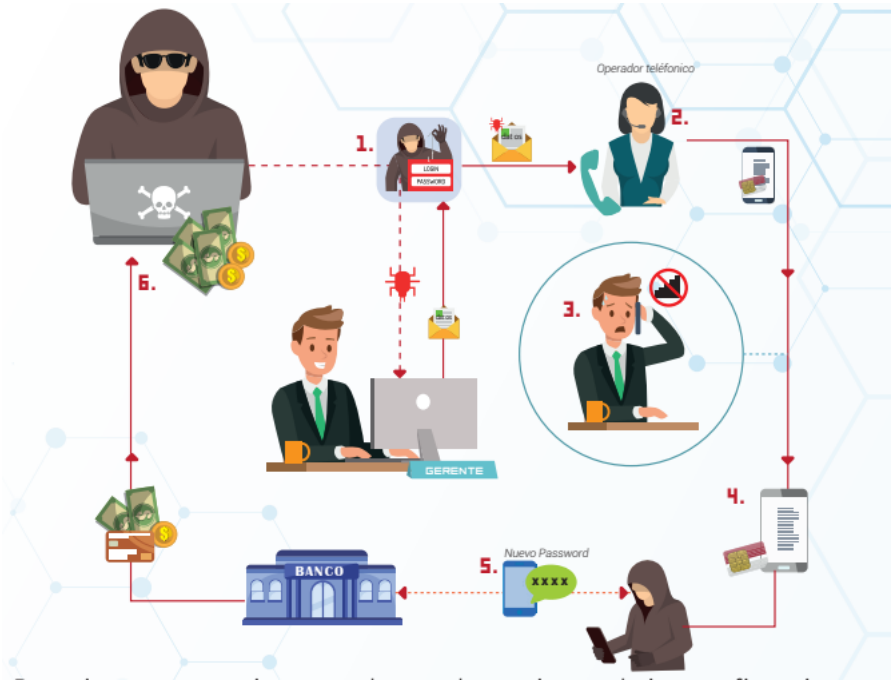
Fuente: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

[34] Ibid. p. 21
[35] Ibid. p. 35

El factor más utilizado para propagar el virus es el envío de correos electrónicos masivo, estos correos contienen archivos adjuntos que ocultan el programa infectado que el atacante, requiere instalar para cumplir con su fraude. Para lograr obtener víctimas, el asunto del mail debe ser llamativo, para lograr capturar la atención de los usuarios, las estrategias más comunes son las alertas, notificaciones y citaciones judiciales y suplantación de identidades gubernamentales.

SIM Swapping: El análisis realizado por la CCIT [36]informa que esta estafa utiliza al máximo las vulnerabilidades de las SIM card, este ataque funciona en cualquier plataforma y con ayuda de ingeniería social, esta modalidad permite a los ciberdelincuentes cometer el SIM Swapping. Este ataque confunde a los vendedores de empresas de móviles, logrando transferir el número telefónico a tarjetas SIM controladas por los ciberdelincuentes. Al obtener el número telefónico de la víctima se puede tener acceso a cuentas bancarias, que tengan configurada autenticación de dos factores por medio de mensajes de texto.

Figura 13 SIM Swapping.



Fuente: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

Ingeniería social: " En el marco del sexto foro de seguridad informática de ESET Latinoamérica se reveló que Colombia es el tercer país en ataques de ingeniería social con un 19% después de Costa Rica y Uruguay, que tuvieron un porcentaje

[36] Ibid. p. 43

de 21% y 24% respectivamente." 37 Molano Natalia 38 agrega Es una gran amenaza que se ha visto incrementada a partir del año 2018, ya que se basa en un conjunto de técnicas para buscar un objetivo, que las persona brinden información sensible por diversos métodos tales como Mensajes de texto, mensajes de WhatsApp o incluso archivos que tienen enlaces falsos y el usuario acceder al sitio y este sitio este clonado; Colombia es el tercer país con más ataques de ingeniería social en América latina de acuerdo.

Los ciberdelincuentes consiguen información de sus posibles víctimas en el mercado ilegal Darknet, usuarios que se encuentren infectados con Malware y víctimas suplantación de identidad. Al tener esta información realizan un reporte en el proveedor móvil informando el robo de un celular, de esta forma consiguen el duplicado de la tarjeta SIM de la víctima.

En el primer trimestre del año 2020 según la CCIT[39], se presentó un incremento de un 27% en las denuncias por ciberdelitos con respecto al año 2019, entre los delitos más denunciados se encuentran el hurto por medios informáticos, casos de Phishing o suplantación de sitios web y violación de datos personales, de acuerdo con el Informe Tendencias del cibercrimen primer trimestre 2020. En los incidentes de suplantación y de usurpación de identidad, su crecimiento se debe en algunos casos por fuga de los datos o vulnerabilidades en los sistemas de información de algunas compañías lo cual es aprovechado por los ciberdelincuentes mediante intrusiones; según el estudio de medidas de seguridad en el tratamiento de datos personales realizado por la SIC a más de 32.763 empresas públicas y privadas del País donde se evidenció que en altos porcentajes las organizaciones en Colombia deben fortalecer su sistema de gestión de seguridad de la información, ya que, en algunos casos no cuentan con medidas apropiadas ni efectivas que garanticen la seguridad de la información, en otros casos no tienen políticas de seguridad o no las han implementado, siendo la deficiencia más alta en las entidades, la falta de poner en marcha una política de protección para el acceso remoto a la información personal**.** Para completar este punto, se realiza una encuesta a un selecto grupo de personas las cuales responden de acuerdo con su experiencia y conocimiento. Esta encuesta se hace con el fin identificar, analizar y validar cuales son los errores más comunes que la sociedad colombiana y así poder implementar el manual de buenas prácticas cuyo objetivo es tratar de minimizar los ciberataques.

[37] MOLANO TORRES, Natalia. Colombia es el tercer país con más ataques de ingeniería social en América Latina. [en línea]. 06 noviembre de 2019 -. [Fecha de consulta: 29, de noviembre2020]. Disponible en https://www.larepublica.co/empresas/colombia-es-el-tercer-pais-con-mas-ataques-de-ingenieria-social-en-america-latina

[38] Ibid., p. 1

[39] CCIT. Informe Tendencias del cibercrimen primer trimestre 2020 [En línea]. Bogotá 2019-. [Fecha de consulta: 05 de octubre 2020]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-abril-2020-final.pdf

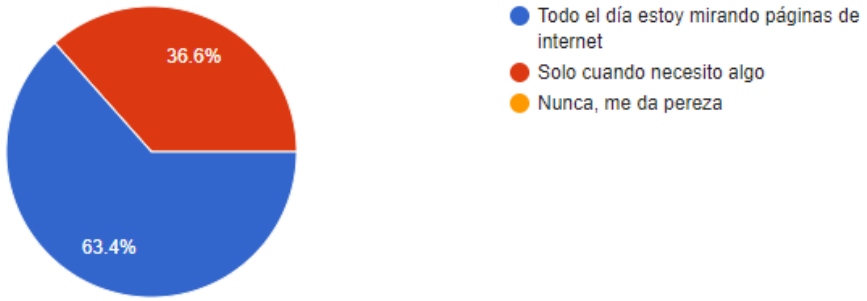
Anexo 1 Encuesta realizada a usuarios

Figura 14 ¿Tienes redes sociales?

Fuente: Propia

Se realiza encuesta a 41 personas las cuales responden a preguntas puntuales, esta encuesta se realiza con el fin de identificar que tan informados se encuentran los usuarios respecto a ciberataques, riesgos y consecuencias a las que se enfrentan cada vez que utilizan internet, se conectan a una red social o simplemente conectarse a una red pública. Inicialmente se pregunta ¿Tienes redes sociales? y el 100% de los usuarios confirman que sí.

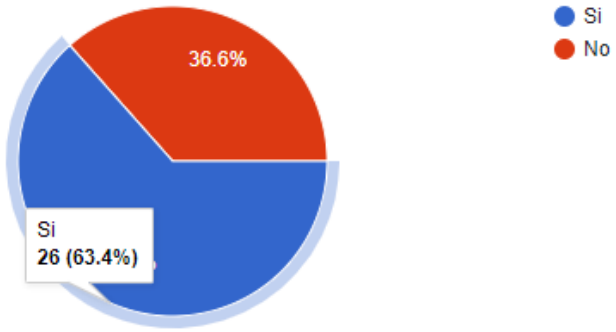
Figura 15 ¿Con que frecuencia navegas por internet?



Fuente: Propia

Teniendo en cuenta la respuesta brindada por los usuarios, se logra identificar que la población encuestada siempre está de algún modo conectada a internet, por lo tanto, es indispensable para la sociedad colombiana, estar conectada a internet.

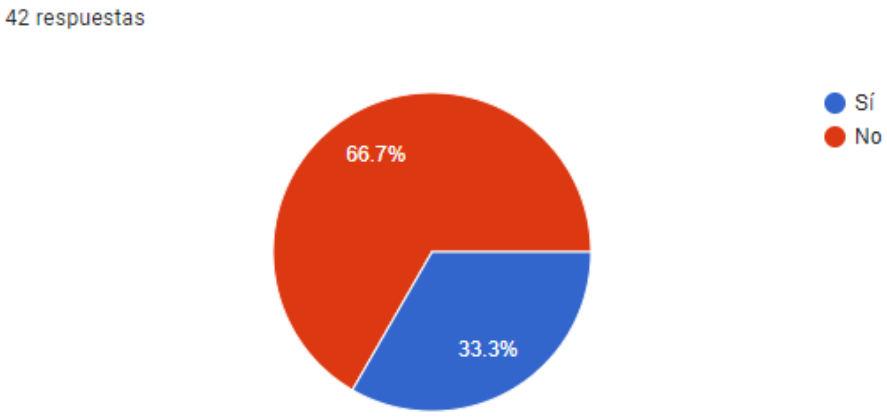
Figura 16 ¿Sabes que son ciberataques?



Fuente: Propia

Los usuarios confirman que saben que son ciberataques, por lo tanto, se asume que tienen conocimiento de cómo prevenirlos, se continúa con la encuesta para confirmar la afirmación anterior.

Figura 17¿Conoces los riesgos que tienes cada vez que realizas una publicación en redes o envías información por medios virtuales?

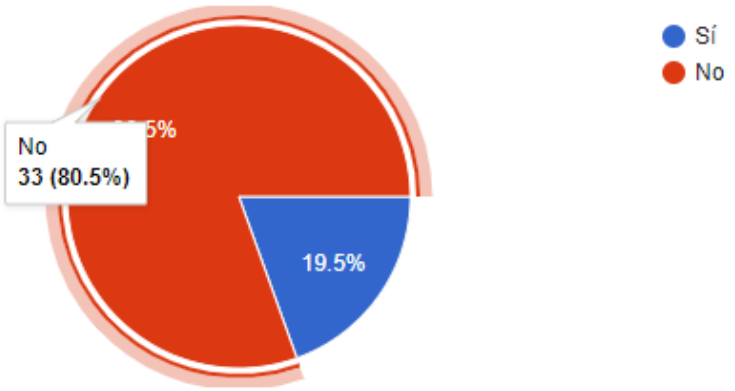


Fuente: Propia

El 66.7% de la población entrevistada, indican que no tienen conocimiento del riesgo que tienen al publicar su vida por las redes, por lo tanto, es fundamental

aclarar los riesgos que este tipo de divulgación presenta para el usuario, para que lo realice de manera consiente, sin poner en riesgo su vida privada y la de su círculo cercado.

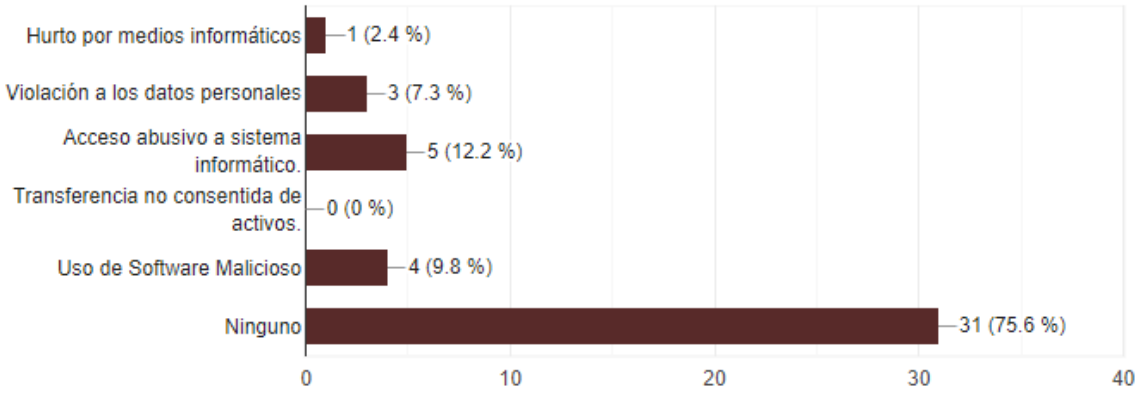
Figura 18 ¿Has sido víctima de un ciberataque?



Fuente: Propia

El 80.5% confirma que no ha sido víctima de un ciberataque.

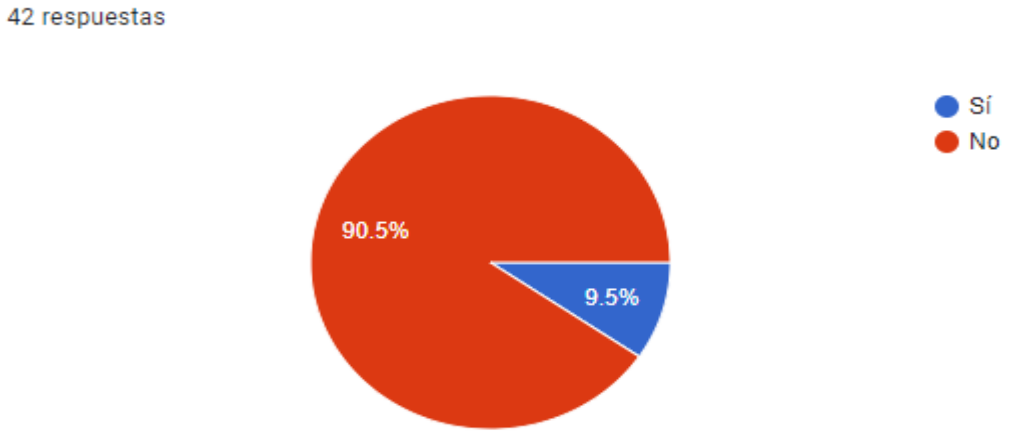
Figura 19 Selecciona ¿Cuál fue el o los ciberataques que te realizaron?



Fuente: Propia

El 12.2% confirma que el ciberataque que ejecutaron en su contra fue “Acceso abusivo a sistemas informáticos” cuyo objetivo es acceder a un sistema informático sin previa autorización y que este se encuentre protegido o no por alguna contraseña.

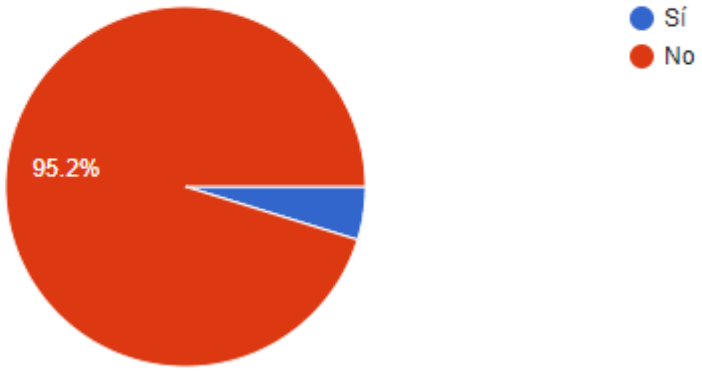
Figura 20 ¿Sabes qué hacer cuando recibes un ciberataque?



Fuente: Propia

Acorde a la respuesta brindada anteriormente, se puede identificar que los usuarios no tienen conocimiento de cómo proceder al momento de un ataque, en este caso se deben utilizar los medios que expone la Policía Nacional y la Fiscalía General de la Nación.

Figura 21 ¿Inviertes presupuesto en ciberseguridad?



Fuente: Propia

El 95.2% confirma que no invierte en seguridad para sus dispositivos, como se puede observar es delicado el tema, debido a que no se tiene en cuenta la dimensión del daño que un ataque cibernético no controlado a tiempo pueda generar.

5.2 DESCRIBIR LAS CONSECUENCIAS QUE GENERAN LOS CIBERATAQUES EN LA SOCIEDAD COLOMBIANA.

La falta de conocimiento de la población colombiana hacia los riesgos que existen en el mundo del internet ha permitido que los ciberdelincuentes trabajen sin descanso burlando las vulnerabilidades de los dispositivos, como se puede observar a diario se presentan ataques por correo electrónico, mensaje de texto, ventanas emergentes, mensajes por WhatsApp entre otros, que con sólo con un clic abre un infierno el cual no se cierra pronto debido a la falta de conocimiento sobre la actuación de los ciberdelincuentes.

El auge de la tecnología ha capturado la atención a nivel mundial por completo y su sin fin de aplicaciones que día a día aportan a la facilidad de la vida humana, las páginas web y las redes sociales han atrapado a la población colombiana de una manera explicable, ya que, pueden pasar horas mirando las actividades favoritas de su círculo de amigos o sus celebridades y esto acapara la atención absoluta de la gran mayoría de colombianos. Esto permite ignorar el peligro virtual que acecha silenciosamente, un enemigo que no se ve, pero está alerta a algún descuido que le permita robar información valiosa para cometer su ataque y beneficiarse ilegalmente.

En la última década, la tecnología ha traído bastantes cambios tanto positivos como negativos. Las familias han perdido su comunicación y el don de compartir, de conocerse, de amarse y disfrutarse, En el pasado, quedó el preciado modo de la privacidad, ya que las personas quieren exhibir su vida, publicando en sus redes sociales cada uno de sus movimientos, demostrando ante la sociedad, la vida perfecta que realmente todos quieren tener. El Inconveniente radica en que hay enemigos virtuales que evalúan todos los movimientos y realizan un estudio de ingeniería social. Gracias a la variedad de publicaciones de una persona, le facilita conocer a su objetivo e identificar el ataque perfecto para aprovecharse de ello. Por lo tanto, se debe ser precavidos, responsables, estar alertas, tener conocimiento de las páginas que siguen, de las páginas que se consultan, las publicaciones que realizan para que no se facilite el ataque de un ciberdelincuente.

A continuación, se expone el testimonio de personas que han sufrido de ataques cibernéticos, estas también fueron participes de las encuestas presentadas anteriormente, con previa autorización del encuestado, se exhibe su nombre en cada testimonio.

Uso de Software Malicioso: La señora Gabriela Figueroa residente de la ciudad de Neiva Huila, recibe un ataque de acceso a uso a sistema informático por medio de su correo electrónico, ya que, el asunto indicaba que su cuenta de correo y va a ser deshabilitada. Ante el desespero de no permitir cerrar su cuenta, ella accede a un enlace e ingresa su usuario y contraseña. Según cuenta, no pasaron más de 30 minutos para recibir la primera llamada donde le pregunta hoy él porque estaba pidiendo dinero desde otro móvil, a lo que ella responde: que ella en ningún momento le ha solicitado dinero a nadie. Luego de tres horas, les habían escrito a todos sus contactos informándole un supuesto cambio de número y algunos les solicitó dinero por medio de mensajes de WhatsApp.

Transferencia no consentida de activos: Carolina Vanegas residente de la ciudad de Bogotá se encuentra mirando su celular y recibe la notificación bancaria informándole un pago de un hotel en Italia por 1 millón de pesos, al parecer no le presta atención y omite el mensaje. Al día anterior recuerda dicho mensaje y vuelve a revisar confirmando la información que habían dado el día anterior, de inmediato se comunica Entidad financiera informando lo ocurrido, por lo tanto, en el banco me indica que deben cancelar la tarjeta de crédito y le llegará una nueva a los tres días hábiles para evitar más inconvenientes, este ataque hace parte de la transferencia no consentida y activos. A continuación, se documentan unas entrevistas realizadas a personas víctimas de ciberataques.

Violación a los datos personales: Stephania Ferro, una mujer de 22 años, que le encantan las redes sociales, subiendo sus fotos diarias y manteniendo a sus seguidores actualizados de su grandiosa vida, pero lo que no sabe Stephania es que por culpa de esas publicaciones recibe un ataque de uno de sus tantos seguidores, el cual se encontraba haciendo la ingeniería social para investigar en qué momento y cómo sería más fácil atacarla. El ciber delincuente ataca sus redes sociales ingresando sus mensajes y su página principal solicitando cambio de dólares en Facebook. La primera reacción de Stephania es hundirse en llanto porque no tiene conocimiento de cómo puedo ocurrir dicho ataque.

Los colombianos al tener una experiencia de un robo cibernético, es normal que se tenga una sensación invariable de inseguridad y acoso.

Miedo: El miedo va de la mano con la inseguridad, por lo tanto, es un elemento que perjudica gravemente dicha sensación. Al no tener conocimiento de quien tiene la información, genera una sensación de angustia que impide a la persona continuar con su vida normal.

Pánico: Cualquier persona que de manera sospechosa llame o escriba por medios electrónicos, genera miedo porque si bien se sabe, los ataques cibernéticos, son en su gran mayoría culpa del factor humano y la persona sabe en donde abrió la puerta para que ingresara el atacante. Por lo tanto, la persona se encuentra insegura ante cualquier sonido que presente su móvil.

Ansiedad: Los ataques de ansiedad y estrés son muy frecuentes al inicio de los ataques, sumándole otros efectos secundarios de la experiencia del ciberataque. Recordar lo ocurrido genera alteración del pulso y temblores.

Depresión: Luego del suceso es normal que se experimente una sensación de rechazo hacia lo ocurrido, generando un estado de melancolía. Generando cambios en la personalidad, sumidos en una constante tristeza.

El CCIT[40] informa que Colombia refleja un porcentaje gradual de incidentes en aumento reportados por las autoridades del ecosistema de seguridad. La policía tiene canales los cual ayudan a los ciudadanos a realizar estas denuncias y por medio de éstos fueron registrados 28,827 casos durante el año 2019. Cabe aclarar que la población colombiana cuando tienen un escenario de estos, la mayoría de las veces no sabe cómo actuar, esto quiere decir que en ocasiones no tiene conocimiento de qué estos canales existen y pueden servir de ayuda y apoyo para dar solución al ciberataque. Los delitos informáticos qué más afectan a los colombianos de acuerdo con la información brindada por la Cámara colombiana de informática y telecomunicaciones es el hurto por medios informáticos con 31,058 casos.

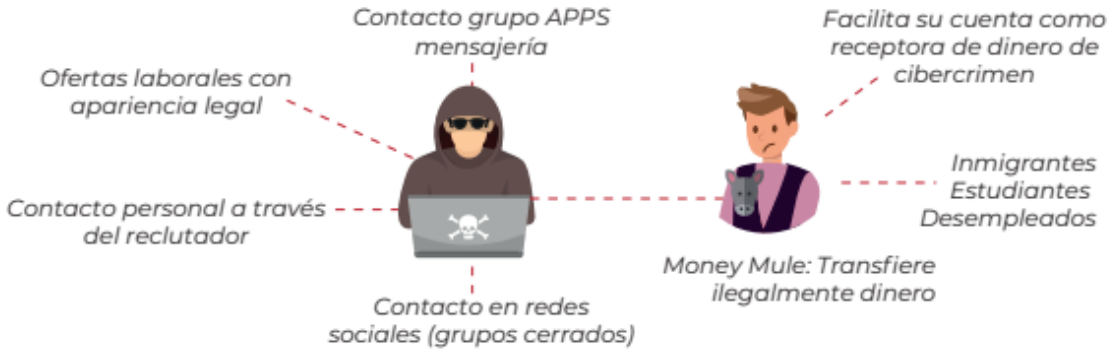
Los ciberdelincuentes actúan de manera rápida, tienen conocimiento de qué los usuarios en su mayoría de veces utilizan sus dispositivos electrónicos para manejar sus cuentas bancarias, por lo tanto, su objetivo es comprometer dichos dispositivos y así realizar una interacción entre usuarios y el banco de su preferencia. Los usuarios que manejan sus cuentas bancarias por medio de móvil, en ocasiones nos cierran sesión de manera correcta, de esta manera el ciberdelincuente puede navegar y esperar hasta que desee hacer el ataque.

El segundo ciberataque más común en la población colombiana es la violación de datos personales con 8.037 casos reportados en ADenunciar. Como se explicó anteriormente uno de los testimonios fue el de Stephania Ferro dónde ella cuenta de su experiencia respecto a su violación de datos en las redes sociales que ella utiliza, de esta manera logró el ciberdelincuente Lucrarse económicamente usando las redes sociales de la víctima mencionada anteriormente.

La mayoría de los ciberataques son para fines lucrativos, por lo tanto, es indispensable para los ciberdelincuentes tener un Money Mules, ya que, estas personas son las encargadas de prestar su nombre y su respectiva cuenta bancaria para que se realicen las transferencias del ataque que se esté ocasionando, logrando obtener de manera ilícita el dinero, como se evidencia en la figura 22.

[40] CCIT. Estudio tendencias del cibercrimen 2019-2020 [en línea]. Bogotá D.C. 2019-. [Fecha de consulta: 10 de abril 2022]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Figura 22 Money Mules

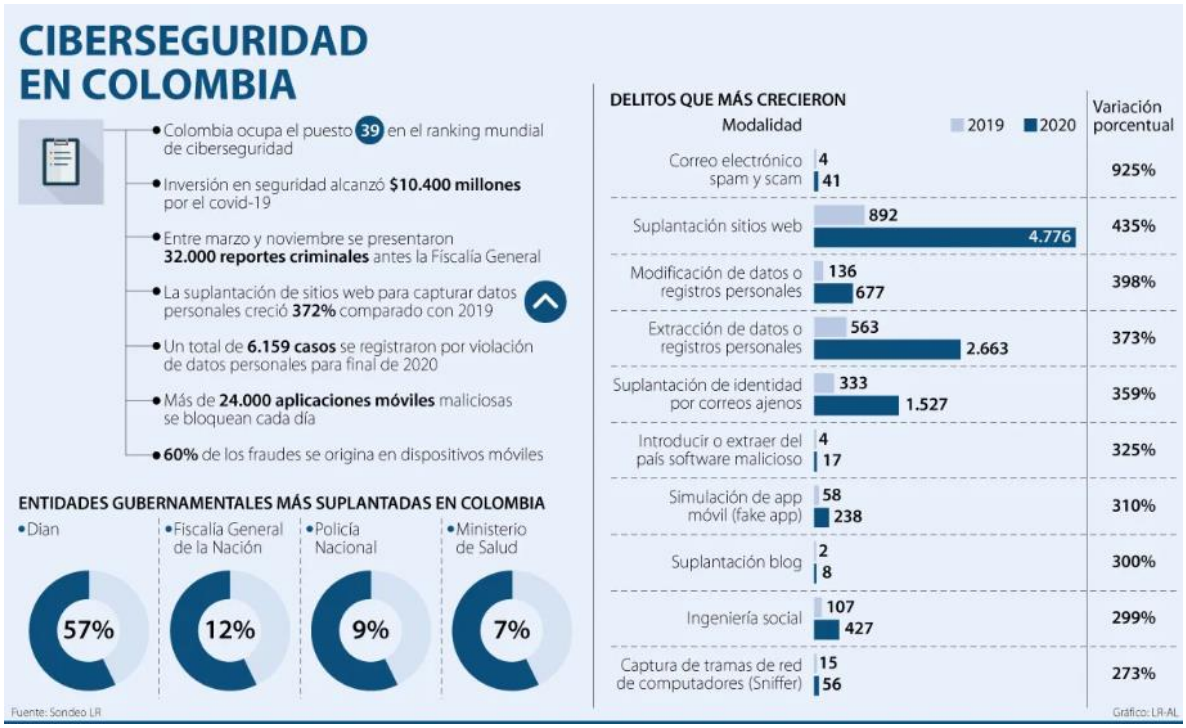


Fuente: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

En el año 2020[41] la pandemia ayuda a que los colombianos utilicen con más frecuencia sus dispositivos electrónicos facilitando infinidad de procesos que comúnmente se realizan estando en la calle. Por el peligro del contagio, por evitar tumultos y muchas cosas más, las personas optan por utilizar sus equipos para realizar compras como mercado, ropa, artículos indispensables para el hogar, dispositivos etc. desafortunadamente a mayor uso de tecnología los ataques en los canales virtuales aumentaron inevitablemente. Por medio de engaños y haciendo uso del COVID-19 se recibían mensajes de texto, correos electrónicos o incluso avisos en las mismas redes sociales. En la figura 23 se evidencia la modalidad implementada y la variación porcentual del ataque entre el año 2019 a 2020.

[41] PORTAFOLIO. Cifras de ciberseguridad en Colombia prenden alarmas al cierre de 2020 [en línea]. Diciembre 10 2020 Bogotá D.C. [Fecha de consulta: 10 de abril 2022]. Disponible en https://www.portafolio.co/tendencias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020-547412

Figura 23 Delitos más comunes



Fuente: https://amp.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

El estudio que realizó el centro operaciones de ciberseguridad de Claro indica que las cifras expuestas durante la pandemia entre el mes de marzo y noviembre aumentaron[42] al 98% teniendo más de 32,000 reportes sobre ataques cibernéticos presentados ante la fiscalía general de la Nación. En 2020 el delito que más se ejecutó fue suplantación de sitios web, Logrando obtener datos personales con un incremento del 372% comparado con el año 2019, este delito se cometió utilizando modalidades como Phishing, Spoonfing y Pharming, detrás de todos los inconvenientes que se presentan a diario con los ciberataques, los prestadores de servicios como Claro indica que durante el año 2020 en un promedio de 4 millones de eventos de seguridad se presentaron al mes, por tal motivo, la compañía mexicana Claro qué es una de las prestadoras de servicio más importantes de Colombia, trabajan en proteger los servicios propios para garantizar la confidencialidad de la información y los datos personales de los clientes que hacen uso de dicho operador, esta información la brinda Flavio Rodríguez Correa empleado de la empresa Claro.

[42] Ibid., p 1

5.3 EVALUAR LAS VULNERABILIDADES QUE EXISTEN EN LOS DISPOSITIVOS ELECTRÓNICOS COMO CELULARES, COMPUTADORES, Y LAS PLATAFORMAS DIGITALES MÁS UTILIZADAS POR LAS PERSONAS EN COLOMBIA.

El crecimiento del uso de Internet durante el año 2020, los nuevos hábitos que la sociedad colombiana adquirió sobre el consumo de los dispositivos y lo influyente que fue el Covid19 para que los colombianos dependieran más de la tecnología.

Colombia[43] tiene una población con más de 51.07 millones ciudadanos y estos habitan especialmente zonas urbanizadas.

Cómo es de esperarse los colombianos uso frecuente de dispositivos móviles, conexiones móviles, tablets y equipos, de acuerdo con la información que brinda Branch indica que aproximadamente hay 60.83 millones de dispositivos conectados a Internet, lo que quiere decir es que la conexión de dispositivos supera a la población por un total del 119%.

Figura 24 Uso de dispositivos electrónicos en la sociedad colombiana

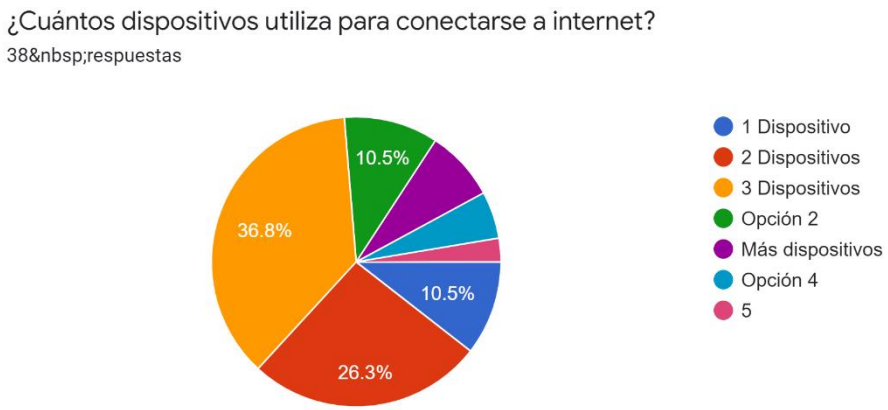
Fuente: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2020-2021/#:~:text=Dispositivos%20que%20m%C3%A1s%20utilizan%20los%20usuarios%20de%20Internet&text=%E2%80%93%20Tel%C3%A9fonos%20inteligente%20(smartphone)%3A%2097.5,%E2%80%93%20Tablets%3A%2035.6%25.

[43] BRANCH. Estadísticas de la situación digital de Colombia en el 2020-2021. [en línea]. -. [Fecha de consulta: 11, de abril 2022]. Disponible en https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2020-2021/#:~:text=Dispositivos%20que%20m%C3%A1s%20utilizan%20los%20usuarios%20de%20Internet&text=%E2%80%93%20Tel%C3%A9fonos%20inteligente%20(smartphone)%3A%2097.5,%E2%80%93%20Tablets%3A%2035.6%25.

En el primer objetivo se mencionan las plataformas digitales que más utilizan los colombianos, las comunes son Facebook, Tik Tok, Instagram y YouTube, pero en el 2020 también hubo necesidad de acceder a aplicaciones que permitían controlar el estado de salud de la población colombiana entre ellas las más utilizadas fueron Corona App, Medellín me cuida, Cali valle corona, Gab, página de Migración Colombia, entre otras.

A continuación, se expondrá una encuesta realizada a un grupo selecto de personas, donde se indaga sobre sus dispositivos de preferencia, navegadores que utiliza con frecuencia y tiempo de conexión a Internet, el resultado permitirá identificar las preferencias de los internautas en Colombia.

Figura 25 ¿Cuántos dispositivos utiliza para conectarse a internet?

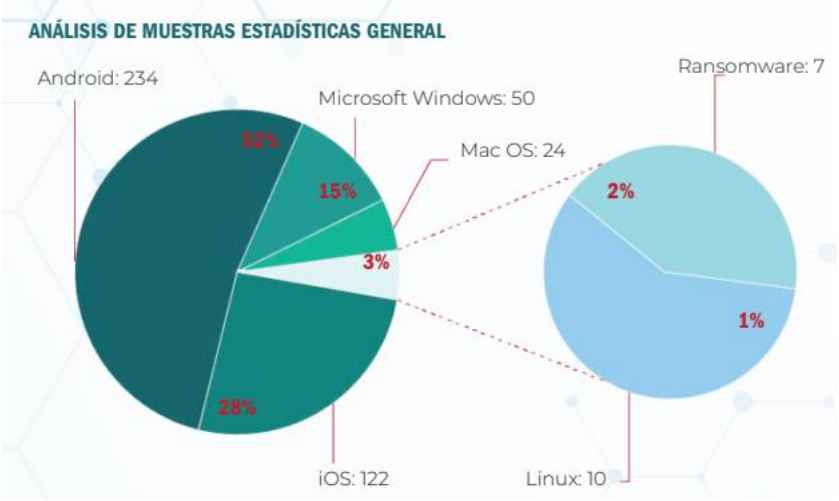


Fuente: Propia

Como se puede observar el 40% de las personas encuestadas utilizan 3 dispositivos, lo cual se afirma lo que indica el análisis que Bran realiza, ya que, el número de dispositivos conectados superan la población colombiana.

Por facilidad, los internautas prefieren usar los dispositivos móviles, como se puede observar un 96% realiza sus actividades desde su teléfono inteligente, ya que, desde el móvil se pueden acceder con mayor brevedad a redes sociales, realizar trámites bancarios, mensajería instantánea, ETC, como se expone en la figura 26.

Figura 26 Muestras analizadas por Sistema Operativo



Fuente: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Con el pasar del tiempo se ve como el dispositivo móvil se vuelve fundamental para cada persona, por muchas razones tales como tener el banco de su preferencia a la mano, estar en contacto con amistades o familiares de manera constante, para divertirse entre muchas cosas más.

Estos dispositivos también tienen vulnerabilidades, que afectan a sus millones de usuarios de una u otra manera, por lo tanto, cada compañía trabaja arduamente identificando sus falencias y así mejorar día a día, aunque el peligro no sólo está en el sistema operativo, también puede ser robado, sufrir algún daño o ser víctima de algún ataque. En la Universidad de Cambridge [44] algunos investigadores identificaron que el 80% de los teléfonos Android están expuestos a una vulnerabilidad crítica, descubrieron que dicho sistema operativo puede ser saboteado con un mensaje de texto. Apple también fue infectado por un programa maligno llamado XcodeGhost cuyo propósito era atacar Xcode, logrando infectar varias aplicaciones de Apple Store y afectar millones de usuarios.

A continuación, se relacionan algunas vulnerabilidades en los dispositivos móviles, aplicaciones web y computadores:

Vulnerabilidades en dispositivos móviles: Fuga de datos [45] :Esta vulnerabilidad principalmente se dirige directamente al usuario que no toma decisiones de manera

[44] KASPERSKY. Amenazas de seguridad móvil dirigidas a dispositivos Android. [en línea]. [Fecha de consulta: 13, de marzo 2022]. Disponible en https://latam.kaspersky.com/resource-center/threats/mobile

[45] PERALLIS SECURITY. 7 amenazas a la seguridad de los dispositivos móviles que debe tomar en serio en 2019. [en línea]. [Fecha de consulta: 13, de marzo 2022]. Disponible en

prudente sobre cada página a la que ingresa o aplicaciones que utiliza y así transferir información sin detenerse a analizar ningún contenido. Dionisio Zumerle, sugiere que una de las soluciones es hacer uso de las aplicaciones que analizan el comportamiento de fuga y así generar un bloqueo automático cuando identifique problemas de fuga en algún proceso.

Aunque esta falla cómo se menciona inicialmente va dirigida directamente al usuario, la posible solución de Zumerle funcionaría para mitigar algunos problemas, pero no da la solución definitiva al inconveniente que se presenta. El usuario también puede optar por usar herramientas de prevención de pérdidas de datos de acuerdo con el sistema operativo que maneje en su dispositivo móvil o Tablet, ya que, estos softwares se diseñaron principalmente para evitar que la información del usuario sea expuesta incluso durante situaciones crítica.

Ingeniería social: El 91% de los delitos cibernéticos inician por un correo malicioso, de acuerdo con la información brindada por FireEye, adicional indica que el ataque phishing creció en el año 2018 un 65% comparado con el año anterior, uno de los posibles análisis que se realiza es que el usuario verifica con facilidad su correo electrónico desde el móvil, esto impide ver el remitente en primera plana, esta información es respalda tanto por IBM como Verizon. Este correo va con un asunto atemorizador el cual la persona que lo ve, no se detiene analizar de donde proviene, si no, que se deja llevar por su instinto y brinda información sensible que termina perjudicándolo. Cabe aclarar que el ataque phishing se puede realizar también por mensajes de texto, Facebook, WhatsApp, por medio de mensajes llamativos para que el usuario realice clic donde no debe.

Interferencia en WI-FI: El mundo gira alrededor de internet, es indispensable estar comunicados con el mundo, por lo tanto, las personas deben conectarse donde quiera que se encuentren, pero ¿Conoce los riesgos que puede tener su información al conectarse a cualquier red pública?, La empresa Wandera realiza una encuesta y logra definir que los dispositivos móviles o equipos laptop utilizan Wi-Fi casi 3 veces más que los datos, esto deduce que una cuarta parte de los celulares han sido conectados a redes Wi-Fi públicas, que no garantizan ninguna seguridad.

Dispositivos desactualizados: Al no tener el dispositivo actualizado con la última versión que brinda el fabricante, puede generar algunos conflictos de seguridad para el usuario, impidiendo ejercer control sobre la información que obtienen las aplicaciones, de esta manera el móvil o el equipo se vuelven paulatinamente vulnerables y de esta manera el atacante puedo acceder a información sensible.

En el año 2020 la pandemia del coronavirus toma de manera desprevenida a nivel mundial todo lo que en ello existe, alterando a cada ser humano. El revuelo que esto

---

https://www.perallis.com/noticias/7-amenazas-a-la-seguridad-de-los-dispositivos-moviles-que-debe-tomar-en-serio-en-2019

tiene es inevitable, es un abrir y cerrar de ojos que deja muchas enseñanzas en todos los ámbitos. Cada gobierno debió realizar acciones para cuidar a sus ciudadanos de algo que no se tenía conocimiento pleno y así mismo crear la facilidad de qué las personas no salían de casa, por esto fue necesario crear métodos de trabajo diferentes y desde el ámbito tecnológico aplicaciones que facilitaron la vida de encierro en la población. En Colombia[46] se crearon varias aplicaciones que permitían Hacerle seguimiento de la salud a cada persona como corona app Colombia, Cali valle corona, Gabo (Bogotá cuidadora), página de migración Colombia, entre otras. Las vulnerabilidades qué se encontraron fueron críticas teniendo en cuenta que a nivel nacional obtenían información de cada ciudadano, al ser aplicaciones que se tuvieron que poner en ejecución prácticamente de inmediato carecieron de control de calidad y auditorías.

Corona App: Se identificaron dos vulnerabilidades en dicha aplicación, la primera es la transmisión de datos sensibles en texto plano y la ausencia autorización en endPoints de la API. El inconveniente era que la aplicación no utilizaba de TLS, eso utilizaba HTTP y de esta forma se comunicaba con la API. Esto quiere decir que todos los datos personales que transitaban Estaban sin cifrar, por lo tanto, esta información la podría tener cualquier atacante pasivo. En la figura 27 se observa la aplicación Corona APP.

Figura 27 Aplicación Corona APP

Fuente: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/MinTIC-en-los-medios/126607:CoronApp-la-aplicacion-que-monitorea-y-actualiza-en-Colombia-los-casos-de-COVID-19

[46] FUNDACION KARISMA. Vulnerabilidades reportadas por el K+LAB de Karisma a entidades públicas en 2020 [En línea]. 27 enero de 2021 -. [Fecha de consulta: 15 de marzo 2022]. Disponible en https://web.karisma.org.co/vulnerabilidades-reportadas-por-el-klab-de-karisma-a-entidades-publicas-en-2020/#ancla2

Formulario Medellín me cuida: La vulnerabilidad identificada fue la ausencia de autorización en integración con empresas públicas de Medellín, esto quiere decir que, sin ninguna autenticación o autorización, se podía consultar datos sensibles de los usuarios desde la empresa e EPM sólo teniendo el número de contrato. En la figura 28 se observa el front-end del formulario.

Figura 28 Formulario Web - Medellín me cuida.

Fuente: https://www.medellin.gov.co/medellinmecuida

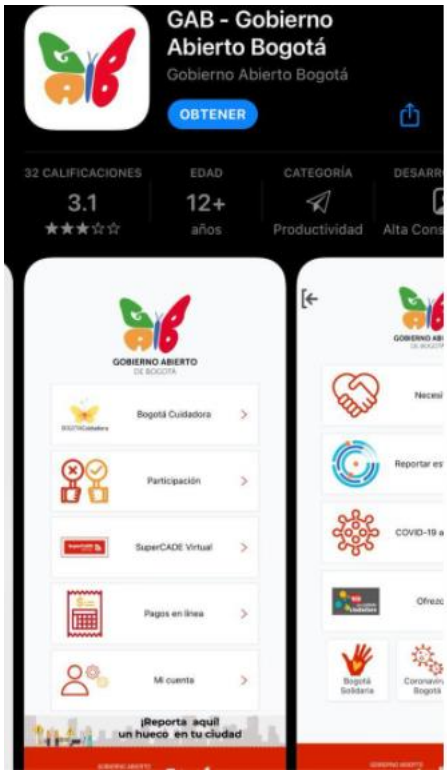
CaliValle corona: La vulnerabilidad identificada fue la ausencia autorización en dos endPoint de la API. Esta vulnerabilidad dejaba consultar información de cualquier persona registrada en la aplicación con su respectivo número de cédula, por lo tanto, era demasiado peligroso porque la recolección de datos puede tener la ubicación de las personas y así realizar seguimientos y analizar sus movimientos sólo con su identificación, las dos vulnerabilidades dejaban que el atacante modificara las consultas que iban a la API y así se lograba contar y calcular la extracción de información qué era útil para el atacante. En la figura 29 se puede observar el front-end de la aplicación.

Figura 29 Plataforma CaliValle Corona

Fuente: https://www.valledelcauca.gov.co/publicaciones/65721/los-vallecaucanos-cuentan-con-calivallecorona-la-app-que--les-permitira-realizar-una-autoevaluacion-sobre-covid-19/

Gab (Bogotá cuidadora): La vulnerabilidad que se identificó en esta aplicación fue la transmisión de datos sensibles en texto plano. Como se menciona en corona app esta aplicación tampoco usaba TLS por lo tanto los datos que estaban expuestos cualquier persona los podían observar ya que no se encontraban cifrados. En la figura 30 se observa el front-end de GAB.

Figura 30 App GAB (Bogotá cuidadora)



Fuente: Propia

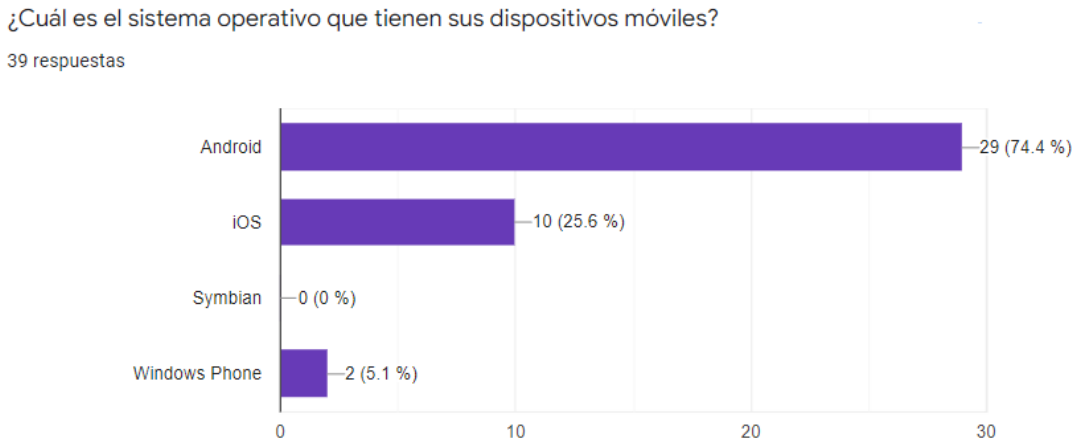
Página de migración Colombia: La vulnerabilidad identificada fue la ausencia de utilización en la API de agenda miento de citas, esta vulnerabilidad permitía acceder a la API por medio de la página de migración Colombia sin realizar algún tipo de autenticación o autorización, por lo tanto, dejaba expuesta la información de las personas que la utilizaban; Se logró identificar que uno de los endPoint del API tenía aproximadamente 4.000 documentos visibles, exponiendo a los usuarios. Figura 31 muestra el front-end de la plataforma de Migración Colombia.

Figura 31 Plataforma Migración Colombia

Fuente: https://www.migracioncolombia.gov.co/

Teniendo en cuenta la encuesta realizada, se evidencia que lo móviles preferidos por los colombianos tienen sistema operativo Android y iOS.

Figura 32 Sistemas operativos más usados por las personas que realizaron la encuesta.



Fuente: Propia

5.3.1 Vulnerabilidades más comunes en los sistemas operativos de los dispositivos móviles[47] más utilizados por los colombianos:

[47] INTERNETPASOAPASO. ¿Cuáles son las principales vulnerabilidades de los dispositivos móviles y cómo podemos protegernos antes diversas amenazas? [En línea] -. [Fecha de consulta: 11 de abril 2022]. Disponible en https://internetpasoapaso.com/vulnerabilidades-dispositivos-moviles/

Rasomware: El ataque que se realiza es bloqueando la información personal del usuario. De esta forma puede cifran las imágenes, videos obligando al usuario a realizar un pago para desbloquear dicha información, este virus es muy utilizado por los ciber atacantes y ha logrado tener mucho éxito en los dispositivos móviles.

Malware en MMS: Por medio de un mensaje en multimedia el ciber atacante puede enviar un malware a varios contactos del usuario, la persona que recibe este mensaje, Instagram el virus en su dispositivo.

Troyanos en SMS: Por medio de un mensaje de texto cuyo contenido sea un troyano, el ciberatacante puede acceder a la información bancaria y así obtener información exclusiva del banco, por lo tanto, el ciberdelincuente tomar la cuenta bancaria del usuario afectado y así realizar acciones con ella.

Spyware: Se realiza la instalación del programa malicioso que viene Mio oculta en aplicaciones de terceros, cuando se instala en el dispositivo, inicia una recopilación de información importante del usuario como contraseñas, Mail, correos electrónicos y multimedia.

5.3.2 Vulnerabilidades en iOS:

Certificados falsos: Esta es una de las amenazas más frecuentes en este sistema operativo y es capaz de insertar el dispositivo móvil y así se descarga una aplicación supuestamente oficial de Apple Store en un sitio web que no es oficial.

Webkit de iOS: Los ciber delincuentes indagan las diversas vulnerabilidades que puede obtener un iPhone, para esto encargan de crear un portal web con scripts de su propia creación y así se burlan de los sistemas de seguridad del sistema operativo.

Perfiles falsos: Estos perfiles se crean con el fin de redireccionar el tráfico de información desde los equipos móviles a un servidor controlado por un ciberdelincuente.

5.3.3 Vulnerabilidades en plataformas de redes sociales

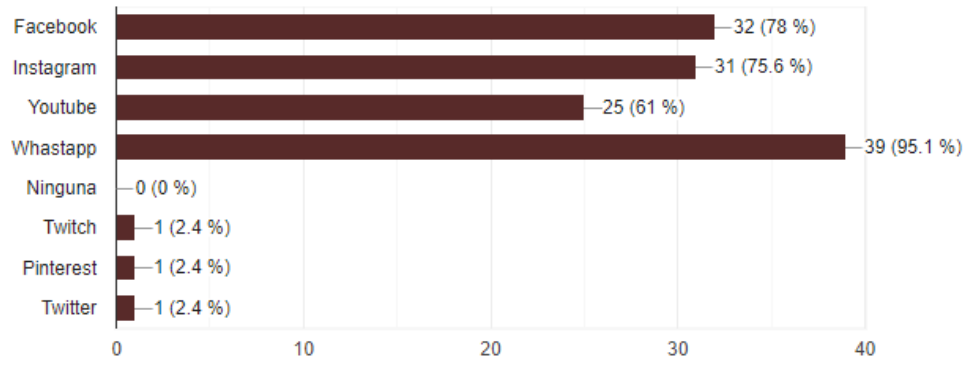
Las redes sociales[48] son un servicio expuesto a usuarios que inicialmente en crear un perfil personal con su información básica logran interactuar con más usuarios que ya se encuentran dentro de la misma Red estos usuarios pueden comunicarse por medio de Mensajes, pueden compartir información que incluso a veces es

[48] UNIVERSIDAD PAMPLONA. Instructivo_ICONTEC_1486. {En línea}. {Consultado el 17 de marzo 2022}. Disponible en: https://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

privada, comparten fotos, videos y cosas que pueden ser vistas acordé a la configuración de su privacidad.

La encuesta realizada arroja que las redes sociales más usadas por los encuestadores son Facebook con un 78% e Instagram con un 75.6%.

Figura 33 ¿Cuáles son tus redes sociales favoritos?



Fuente: Propia

Teniendo en cuenta la encuesta realizada, se expone las vulnerabilidades de Instagram y Facebook porque son las redes sociales con mayor porcentaje de uso.

Suplantación de identidad: Cómo se explicó anteriormente es necesario crear un perfil y así se puede acceder a la Red social que se desee, por lo tanto, alguien puede hacerse pasar por esa persona, con el fin de buscar un beneficio propio. El inconveniente de este ataque es que puede lograr robar información, robar dinero etc. Cuando la víctima identifique que fue atacada se recomienda denunciar a la Fiscalía General de la Nación en los números expuestos en la página web acorde a la ciudad de los encuentre.

Malware: Los ciberdelincuentes andan atentos a cualquier vulnerabilidad que se presente, por lo tanto, están dispuestos a lograr su cometido por medio de la instalación de código malicioso que robe información desde el dispositivo que el usuario utiliza para ingresar a la red social o página web a la que esté generando el ataque. Este ataque se realiza por medio de links falsos, correos, anuncios o publicaciones falsas de otros perfiles, a la víctima se le recomienda instalar antivirus y estar atentos a las actualizaciones que se realicen a nivel de sistema operativo y antivirus para que así se detecten las vulnerabilidades con más facilidad.

Ciberbullying: Este es uno de los ataques que afecta no sólo a la víctima de forma material sino también de manera psicológica, ya que es uno de los más frecuentes que se percibe en la era digital, el ciberbullying es cuando cualquier persona que se

encuentra en Internet o en algún dispositivo electrónico es acusado, amenazado, humillado, avergonzado o abusado por otra persona simplemente con el fin de manipular a su víctima y así lograr el cometido que requiera.

Uso indebido de Fotos y otros contenidos: Los usuarios acostumbran que por medio de redes sociales se comparta información, fotos, Videos, contraseñas y en ocasiones se filtran de manera rara logrando perder el control hasta del mismo usuario propietario de dicho contenido, cada usuario debe documentarse de las políticas del uso de la Red social que maneja, indagar sobre su política de seguridad y también ser cuidadoso al momento de compartir información en la Red.

Fake News: Esto hace referencia a las noticias falsas que se difunden por medio de las redes sociales y generan un impacto negativo, desinformado y coge gran velocidad causando temor, caos y confusión en la opinión pública. Es importante no creer en cada noticia que se divulga a nivel general en Internet, si usted tiene dudas puede dirigirse a fuentes de investigación más confiables y así obtener información verídica.

5.3.4 Vulnerabilidades en plataformas de mensajería instantánea

En los últimos tiempos la manera de comunicación[49] ha cambiado en todos los niveles, desde el uso de correo electrónico ya que anteriormente era uno de los pilares ha perdido peso contra la mensajería instantánea. Hoy en día se utilizan varias aplicaciones en su mayoría móviles con las que se puede estar en continuo contacto con otras personas sin tener necesidad de acceder a un correo electrónico. Esto quiere decir que en ocasiones se utiliza esta mensajería para enviar información, documentos, imágenes, videos etc. El uso de las aplicaciones de mensajería instantánea puede traer consecuencias en cuestión de seguridad y privacidad.

El riesgo de sustituir el correo electrónico por mensajería instantánea: Cuando uno manda documentos importantes, con la firma e información privada que correspondía mensajes corporativos al compartir forma información confidencial, el correo electrónico sigue siendo uno de los medios más usados porque da confiabilidad respecto a las aplicaciones de mensajería instantánea, aunque eso ha ligado a la preferencia del usuario, como la facilidad del uso de las herramientas como WhatsApp, Facebook Messenger, Telegram entre otras en ocasiones sustituyen el correo electrónico.

Al hablar de mensajería instantánea es claro que se refieren a las aplicaciones móviles como WhatsApp, Telegram, Line; entre otras, pero, cabe aclarar que

[49] JIMENEZ. Javier Consejos de seguridad y privacidad para mensajería instantánea. [en línea]. Bogotá D.C 13 septiembre de 2019 -. [Fecha de consulta: 17, de marzo 2022]. Disponible en https://www.redeszone.net/tutoriales/seguridad/mensajeria-instantanea-sustituye-email-seguridad/

también se puede tener mensajería instantánea abriendo una aplicación web como por ejemplo Facebook.

Principales causas de problemas de seguridad a través de la mensajería en WhatsApp, Telegram y Facebook Messenger. El alto porcentaje de los ataques que se han generado entre el año 2018 al año 2020 ocurren en el día y es necesario tener la interacción del usuario. El ciber atacante en la mayoría de los casos necesita que su víctima lleve a cabo alguna acción y así comete el error de instalar algún programa malicioso o ingresar sus datos en un lugar indebido, la mayoría de veces el malware a través de cualquier programa llega por medio de una descarga de archivos que se recibe sea por mensajería de texto, correo electrónico o dar clic en alguna página web erradamente.

Otro de los problemas es la configuración de la privacidad que se tiene en cada aplicación, la población colombiana normalmente es muy confiada y expone mucha información respecto a su vida y no identifica que hay ciberatacantes atentos algún descuido para aprovechar su momento, por lo tanto, la información puede filtrarse entre la red y fácilmente tener algún tipo de afectación, lo recomendable es que se lean las políticas de privacidad de cada una de estas aplicaciones y así tener completa seguridad a quien se le comparte información privada y personal, es elemental tomar conciencia para proteger la seguridad del usuario y de los que lo rodean al momento de hacer uso de la mensajería instantánea.

5.4 PROPONER UN MANUAL DE BUENAS PRÁCTICAS DE USUARIO QUE MITIGUEN EL RIESGO DE SUFRIR UN CIBERATAQUE EN LA POBLACIÓN COLOMBIANA.

No hay dudas que alistar un manual de buenas prácticas es un pilar fundamental para lograr que la población colombiana tenga un poco más de conocimiento frente a este tema tan delicado que día a día se ve impactado y la información más expuesta sin tomar ningún tipo de acción por cada uno de los usuarios que utilizan diversas plataformas y exponen de manera indebida información confidencial.

Se procede a dar algunos consejos acordes a las vulnerabilidades encontradas, y expuestas en el objetivo anterior, para así, lograr dar un mensaje a los usuarios que hacen uso de estas aplicaciones y logren captar el mensaje de lo importante que es tener claridad respecto a la privacidad que se debe tener.

5.4.1 Consejos para prevenir ataques en dispositivos móviles[50]

Bloqueo por contraseña del dispositivo: Asignar una contraseña al dispositivo que se esté utilizando al momento que se suspenda por inactividad, esta medida se complementa con el cifrado de la memoria, la interna y la tarjeta, con el bloqueo de la pantalla, es importante recordar que el almacenamiento de información privada en el dispositivo debe tener los datos cifrados.

Configuración de la contraseña en Android:

- Abrir la opción de configuración del teléfono.
- Clic en la opción seguridad.
- Se debe elegir el tipo de bloqueo de su preferencia y presiona bloqueo de pantalla.

Las opciones de bloqueo pueden ser:

- Patrón: Se realiza un dibujo con la yema de los dedos.
- En la figura 34 se observa cómo es la contraseña patrón en Android

Figura 34 Contraseña Patrón

Fuente: https://androidayuda.com/android/tutoriales/patrones-de-desbloqueo-mas-seguros/

[50] LEADER. 10 consejos de seguridad para dispositivos móviles. [en línea]. B -. [Fecha de consulta: 17, de marzo 2022]. Disponible en https://www.leader-network.com/movilidad/10-consejos-de-seguridad-para-dispositivos-moviles/

- PIN: Se ingresan mínimo 4 dígitos, entre más dígitos se agreguen, la contraseña es más segura.
- En la figura 35 se observa cómo es el PIN en Android

Figura 35 PIN Android

Fuente: https://www.xatakandroid.com/moviles-android/algunos-google-pixel-estan-entrando-bucle-fallo-desbloqueo-pin

Contraseña: Se caracteriza por tener letras y números.

Configuración de la contraseña en iOS:

- Ir al icono de configuración.
- Clic en la opción Contraseña y seguridad.
- Cambiar contraseña.
- Solicita la contraseña que ya se encuentra registrada en el móvil, esta contiene 6 dígitos.
- Posteriormente se redirige a una pantalla nueva donde se debe poner nuevamente la contraseña actual y luego ingresar la nueva.
- Dar clic en cambiar.
- En la figura 36 se observa cómo se cambia la contraseña en iOS.

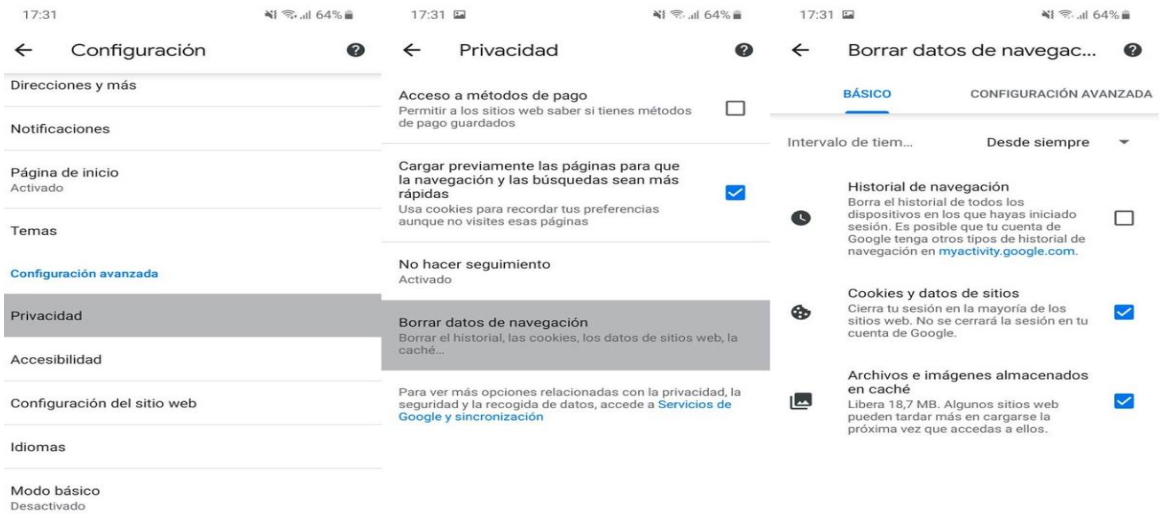
Figura 36 Cambiar contraseña en iOS

Fuente: Propia

Revisar borrado de historial de navegación: Desde el móvil se accede al navegador se su preferencia, ir a configuración o privacidad:

- Elegir la opción de borrar datos de navegación.
- La explicación se encuentra en la figura 37.

Figura 37 Eliminar datos de navegación en dispositivos.



Fuente: https://www.xatakandroid.com/tutoriales/como-borrar-todas-cookies-datos-uso-tu-movil-android#:~:text=Accede%20a%20la%20configuraci%C3%B3n%20avanzada,guardados%20en%20la%20memoria%20cach%C3%A9.

Realizar copia de seguridad esporádicamente: Para realizar estas copias de seguridad recuerde que hay aplicaciones online que permiten sincronizar la información con su equipo, de esta manera siempre va a tener su información actualizada y disponible, es importante cuidar la información que se exponga.

Copia de seguridad en iOS:

- Se debe tener el móvil conectado a una red inalámbrica confiable.
- Ir a ajustes y en el nombre dar clic en iCloud
- Elegir copia de seguridad de iCloud.
- En la figura 38 se detalla cómo realizar una copia de seguridad en iCloud

Figura 38 Copia de seguridad en iCloud

Fuente: Propia

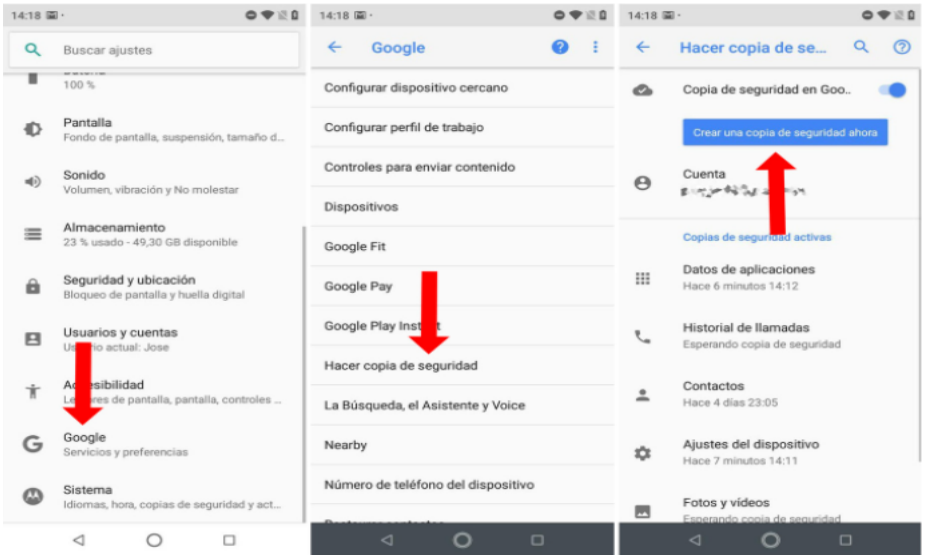
- El punto negativo es que Apple no brinda mucho espacio libre, da 5gb y se llena con facilidad.

Una de las aplicaciones que se puede utilizar tanto en iOS como en Android es Google Drive. Por lo tanto, se dará una breve explicación de cómo hacer la copia de seguridad en dicha aplicación. De igual forma se debe tener en cuenta, que el administrador de dicho espacio es la persona que lo requiere, por lo tanto, tiene libertad de elegir que se guarda y que no.

Copia de seguridad en Google Drive:

- Ir ajustes, Google, hacer copia de seguridad
- Se crea una copia de seguridad
- Al finaliza el paso anterior, los datos del móvil o equipo estarán en Google Drive.
- En la figura 39 se detalla como realizar una copia de seguridad en Google Drive.

Figura 39 Copia de seguridad en Google Drive.



Fuente: https://www.xatakandroid.com/tutoriales/como-hacer-copia-seguridad-completa-movil-android

Instalar aplicaciones confiables: En la figura 40, se detalla aplicación de los supositorios oficiales como App Store, Google Play o App Word, por lo tanto, es recomendable que las aplicaciones que se instalen sean descargadas directamente de dichos repositorios.

Figura 40 App Store

Fuente: Propia

Instalar aplicaciones necesarias: En ocasiones se instala un exceso de aplicaciones que disminuye el buen funcionamiento del dispositivo lo recomendable es minimizar el riesgo de exposición con esta medida, se debe tener en cuenta que el instalar una aplicación es importante tener en cuenta los permisos y condiciones que está trae y así saber cuál es la exposición de información privada del usuario.

Tener protección antivirus: Para los teléfonos también se usa como medio de seguridad en contra de los ciberatacante hay muchas opciones que brindan los repositorios que pueden ser descargados, otra recomendación es estar atentos a las actualizaciones que el sistema operativo exponga, ya que, en estas actualizaciones se corrigen vulnerabilidades de las versiones anteriores, cualquier antivirus sirve solo se debe buscar el que se ajuste a su necesidad, recuerde que hay antivirus que son gratuitos, otros cobran poco y otros más robustos cobran mucho más.

Para Android se recomienda instalar el antivirus Kaspersky

- Ir a Google Play y busque la aplicación Kaspersky.
- Al instalar en el móvil proceda a seguir los pasos que se solicitan como nombre, correo etc. y al finalizar clic en instalar.
- En las opciones de permisos, dar clic en aceptar políticas.
- Al ingresar se debe elegir la ubicación.
- Y, por último, se debe elegir iniciar análisis.
- En la figura 41 se observa el contenido del Antivirus Kaspersky.

Figura 41 Antivirus Kaspersky

Fuente: https://androidbasico.com/descargar-antivirus-kaspersky-gratis.html

Para Apple se recomienda instalar el antivirus Avira Security

- Ir a Apple Store y descargar Avisar Security
- Al descargar abra la aplicación y pedirá que ingrese usuario y contraseña, puede acceder con su usuario Apple ID, correo Gmail o Facebook, elija el que prefiera.
- Ingrese a la aplicación y puede elegir la opción PRO que cuesta alrededor de $24.900 o la versión gratuita por una semana.
- Y, por último, dar clic en análisis inteligente, para que le indique si su celular tiene alguna novedad.
- En la figura 42 se observa el contenido del Antivirus Avira.

Figura 42 Antivirus Avira

Fuente: Propia

Tener cuidado a las redes públicas a las que se conecta: Es elemental estar conectados y en ocasiones se ve la necesidad de acceder a Internet y por algún motivo no es posible tener datos en su móvil y se va a conectar a una Red que le permita tener conexión con el mundo, el inconveniente que generan las redes públicas es que son demasiado atacadas por externos y estos podrían afectar a todos los que estén conectados en esa Red, por lo tanto, es preferible no utilizarlas, pero si es algo urgente trate de no acceder a realizar operaciones bancarias, descargar documentos confidenciales o ingresar alguna contraseña en algún sitio que pueda afectar su privacidad.

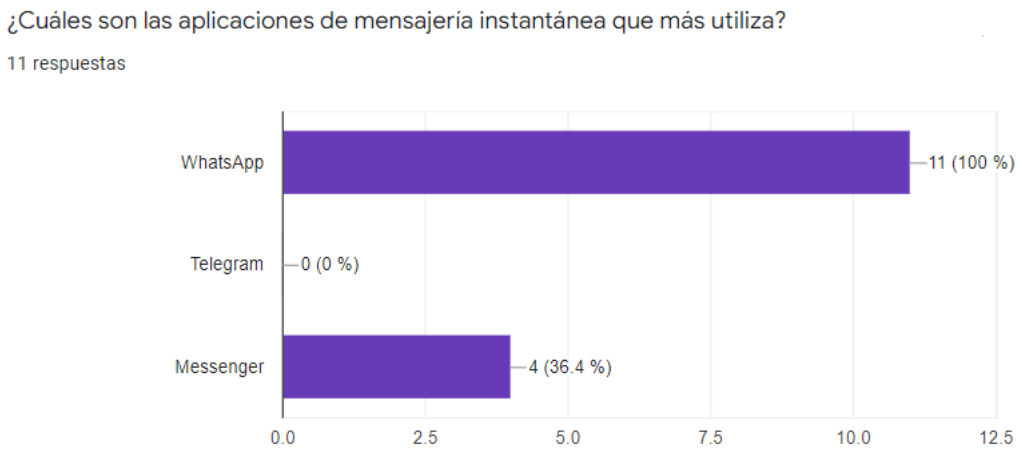
Desactivar redes inalámbricas: Por medio de las redes inalámbricas públicas o por bluetooth, los atacantes pueden engañar al usuario que estén haciendo uso de su dispositivo, ya que, este se conectará automáticamente a una Red y está puede

estar siendo atacada de esa manera se logra supervisar la actividad del usuario en su dispositivo.

5.4.2 Consejo para prevenir ataques en plataformas de mensajería instantánea[51]

Utilizar antivirus: Esta recomendación se realizará en todas las aplicaciones que tengan acceso a la Red, sea desde un dispositivo móvil, un equipo o el uso de mensajería instantánea, es importante contar con un software que brinde seguridad al dispositivo en el que se encuentra instalada la aplicación. Es importante tener en cuenta el utilizar mensajería instantánea enviando cualquier tipo de mensajes se pueden recibir archivos peligrosos y por error instalar un software malicioso en el dispositivo. Cabe aclarar que los archivos que se reenvíen en ocasiones ni el remitente tiene conocimiento que es un archivo infectado, por lo tanto, es importante tener un buen antivirus que permita identificar este tipo de inconvenientes, anteriormente se sugieren los antivirus más usados acorde a S.O más utilizados en los usuarios. De acuerdo con la encuesta realizada se identifica que las aplicaciones de mensajería instantánea más utilizada es WhatsApp.

Figura 43 Consulta sobre cuáles son las redes sociales más usadas por los Colombianos.



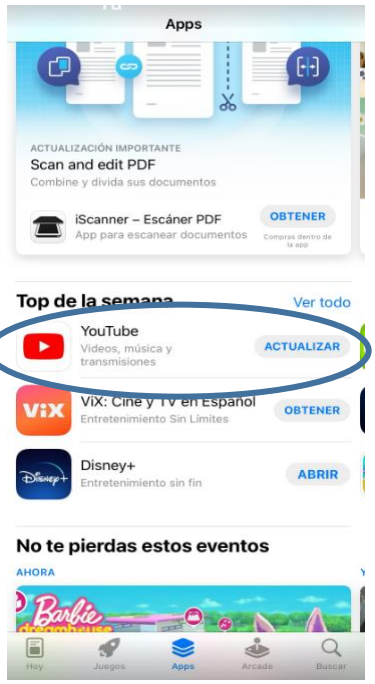
Fuente: Propia

Dispositivos y aplicaciones actualizadas: Es importante siempre contar con las últimas versiones que brindan las aplicaciones, porque esto corrige vulnerabilidades que identificaron los expertos en la aplicación en versiones anteriores, contando con

[51] JIMENEZ. Javier Consejos de seguridad y privacidad para mensajería instantánea. [en línea]. Bogotá D.C 13 septiembre de 2019 -. [Fecha de consulta: 17, de marzo 2022]. Disponible en https://www.redeszone.net/tutoriales/seguridad/mensajeria-instantanea-sustituye-email-seguridad/

la última actualización, restringe ataques de los piratas cibernéticos, a continuación, se ingresa al APP Store y se expondrá como se ve una actualización pendiente como se observa en la figura 44 y 45.

Figura 44 Pendiente actualización de YouTube en App Store



Fuente: Propia

Figura 45 Actualización de la APP de YouTube

Fuente: Propia

Como se puede observar en la figura anterior, se especifica puntualmente para qué es la actualización, por eso es fundamental tener las aplicaciones de uso frecuente actualizadas y las que no se usan preferiblemente eliminarlas.

Descargar aplicaciones en repositorios recomendados como son Apple Store o Google Play.

5.4.3 Consejos para prevenir ataques en plataformas de redes sociales

Información privada: Al exponer la vida social de manera pública se enfrenta a un peligro inminente, los ciberatacantes están atentos a cualquier debilidad que se presente y asimismo puede atacar sea de manera virtual o física, ya que, por medio de publicaciones se puede llegar incluso hasta la ubicación de la casa de la víctima. Publiqué con precaución y de manera responsable.

Para configurar la privacidad de Facebook:

En la aplicación en la parte superior hay una opción que parece una tuerca, ese es el menú de configuración de Facebook. Al abrir la configuración de Facebook se detalla cada uno de los ítems que son considerables para tener un manejo de privacidad, por lo tanto, ya va acorde a la elección de cada usuario. En la figura 46 se especifica la configuración de Facebook.

Figura 46 Configurar privacidad en Facebook

Fuente: Propia

Cada vez que se realiza una publicación es posible modificar la privacidad de dicha publicación y preferiblemente elegir que solo lo vean sus amigos, ya que, la ven exclusivamente las personas que tienes agredas en su perfil. En la figura 47 se muestra la configuración de cada publicación en Facebook.

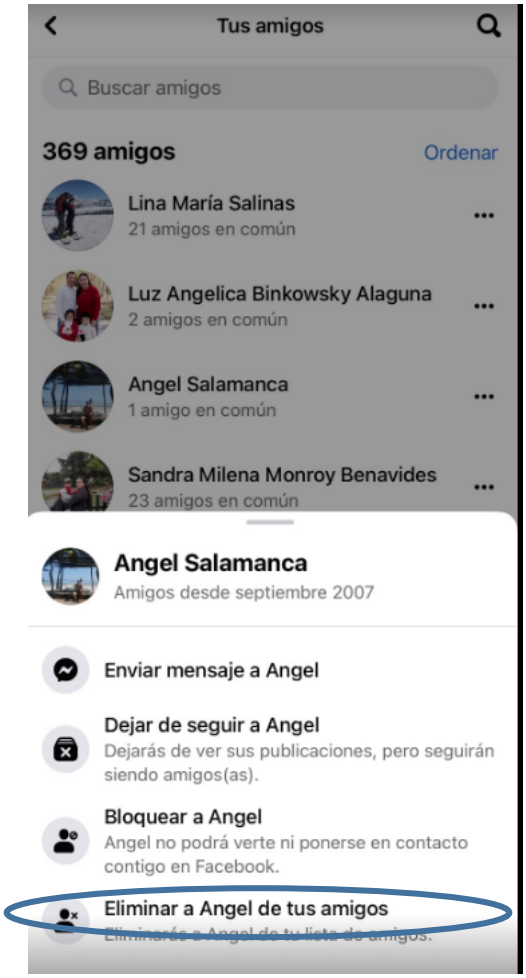
Figura 47 Configuración de cada publicación en Facebook.

Fuente: Propia

Para configurar la privacidad de Instagram:

En Instagram es un poco más sencillo, se dirige a configuración y elige configuración y la opción privada esto quiere decir que solo verán los movimientos dentro de la red las personas que haya aceptado, la privacidad en Instagram se configura como se evidencia en la figura 48.

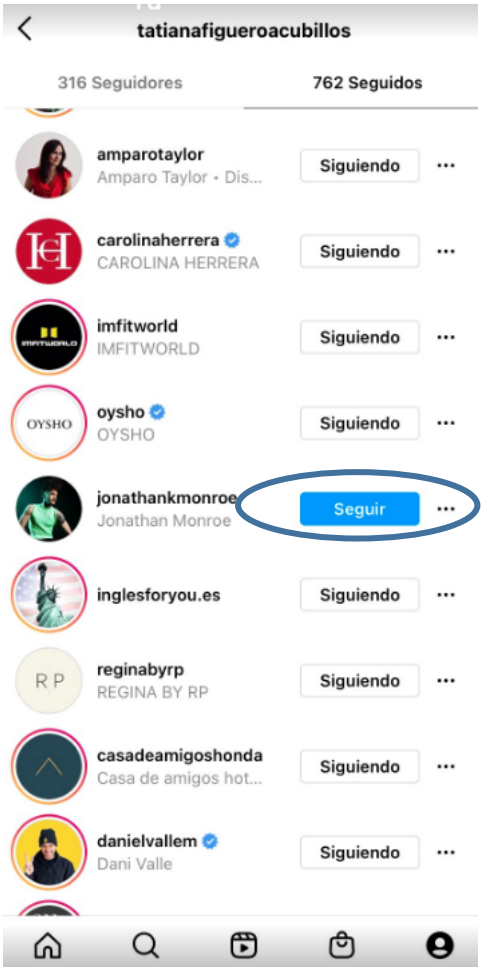
Figura 48 Depuración de contactos



Fuente: Propia

- En Instagram, le da clic en seguidos y se despliega la lista de las personas que sigue.
- Luego dar clic siguiendo y automáticamente se habilita la opción de seguir, esto quiere decir que ya no sigue a esta persona.
- En la figura 49 hay una breve explicación de como depurar contactos en Instagram.

Figura 49 Depuración de contactos en Instagram.



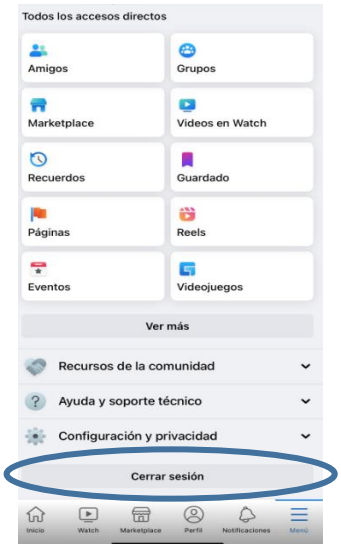
Fuente: Propia

Evitar citas a ciegas: El cambio de comunicación en los últimos años ha generado que también cambié algunas costumbres las cuales están implementadas en la sociedad, por ejemplo, el encontrar el amor en una red social es algo normal en estos últimos tiempos, lo recomendable es que evite este tipo de práctica teniendo en cuenta que los ciberatacantes tienen sus métodos para ganar su confianza y así lograr siento interés hasta obtener lo que realmente quiere.

Cerrar sesión: Al acceder a las redes sociales es normal que al conectarse al mismo dispositivo siempre se tenga inicial, pero, no se sabe si se pueda presentar alguna situación atípica como robo del dispositivo o un intruso dentro del mismo y éste puede obtener información de manera indebida simplemente por no haber cerrado, lo recomendable es que por más que el equipo sea seguro con el fin de evitar los inconvenientes mencionados anteriormente. En la figura 50 y 51 se explica como cerrar sesión en cada una de las aplicaciones. Tanto en Facebook como en

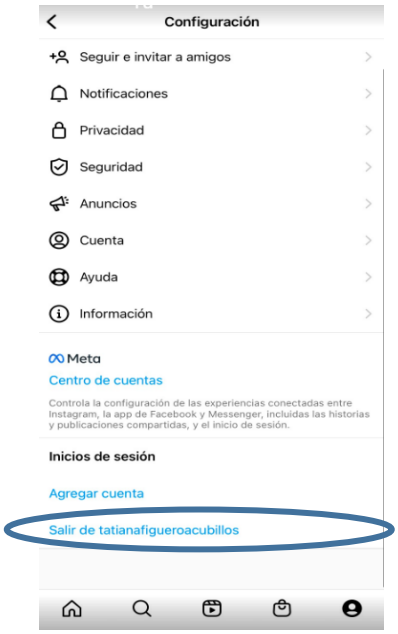
Instagram, se elige la opción de configuración, luego deslizar hacia abajo hasta encontrar la opción de cerrar sesión.

Figura 50 Cerrar sesión en Facebook



Fuente: Propia

Figura 51 Cerrar sesión en Instagram



Fuente: Propia

Desactivar la geolocalización: Este es un ítem que todas las redes sociales últimamente y se usa para rastrear el movimiento del perfil del usuario, si es necesario utilizarlo actívelo periódicamente.

Para desactivar localización en iOS:

- Ir a configuración.
- Elija la opción de privacidad.
- Dar clic en Localización y desactivar la opción.
- Se recomienda usar solo cuando sea necesario.
- En la figura 52 se indica como desactivar la ubicación en iOS

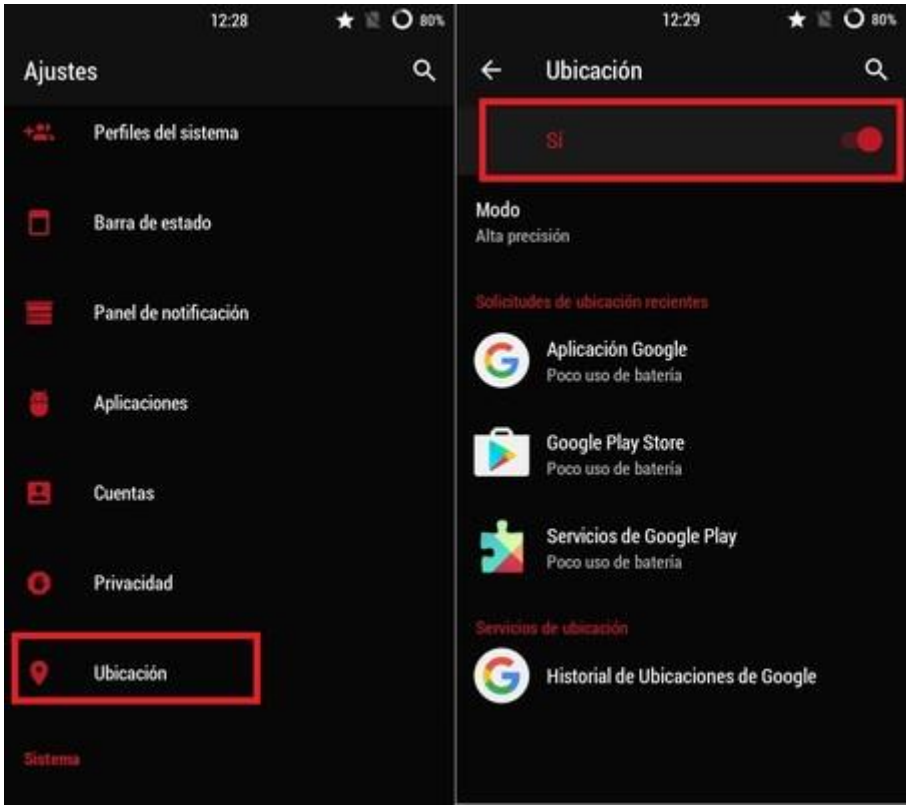
Figura 52 Desactivar la localización en iOS

Fuente: Propia

Para desactivar localización en Android:

- Ir a la opción de ajustes.
- Elegir el menú de ajustes rápidos.
- Dar clic en ajustes avanzados y luego la opción de “Precisión de la ubicación de Google”.
- En la imagen 53 se observa la ubicación activa, por lo tanto, se debe desactivar inactivando la opción de sí.

Figura 53 Desactivar la ubicación en Android.

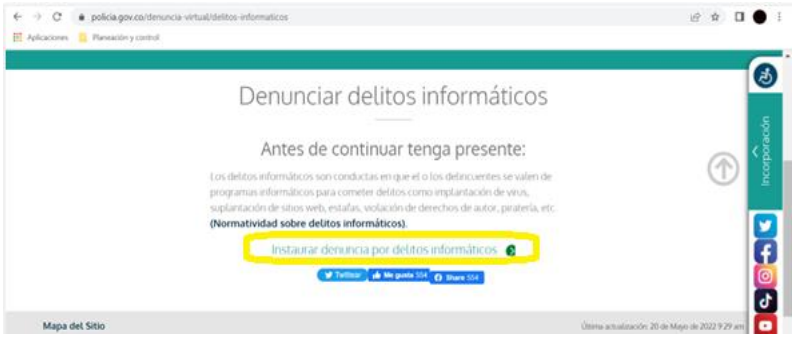


Fuente: https://www.xatakandroid.com/seguridad/como-evitar-que-las-aplicaciones-accedan-a-la-ubicacion-de-tu-dispositivo-android

Evite enviar cadenas: Las cadenas son mensajes que posiblemente tengan oculto algún software malicioso y así usted puede afectar masivamente varios dispositivos y participar en el ataque quiere ejecutar, los ataques pueden ser denegación del servicio, robo de datos, estafas, entre otras formas de ataque.

En caso tal que sea víctima de un ataque, puede realizar la denuncia en el siguiente link https://www.policia.gov.co/denuncia-virtual/delitos-informaticos. En las figuras 54,55 y 56 se enseña cómo realizar la denuncia.

Figura 54 Denunciar en la página de la policía.



Fuente: Propia

Otra página expuesta por la policía es https://adenunciar.policia.gov.co/Adenunciar/Login.aspx

Figura 55 Página ADenunciar de la policía.

Fuente: Propia

Luego acepte términos y condiciones; luego elija la opción de delitos informáticos y proceda a brindar la información que se solicita.

Figura 56 Continuación de la denuncia en la página ADenunciar de la policía.

Fuente: Propia

Existen las siguientes líneas telefónicas[52], la cuales se encuentran disponibles 24/7, los números 601-5702000 Opción 7 en la ciudad de Bogotá, línea nacional 018000919748 o línea celular 122 para el resto del país.

[52] FISCALÍA GENERAL DE LA NACIÓN. [En línea]. [Fecha de consulta: 21 de mayo 2022].¡Disponible en https://www.fiscalia.gov.co/colombia/servicios-de-informacion-al-ciudadano/donde-y-como-denunciar/#:~:text=En%20el%20Centro%20de%20contacto,sistema%20de%20denuncia%20virtual%20%C2%A1ADenunciar!

9. CONCLUSIONES

El presente trabajo identificó las diferentes técnicas de ciberataques más frecuentes que se han presentado entre el 2018 al 2020 en Colombia, la importancia de conocer las técnicas que utilizan los ciberdelincuentes que afectan a la población colombiana, ya que, recurrentemente estos ataques se han convertido en un dolor de cabeza para la comunidad. Los colombianos no están preparados para este tipo de ataques por falta de conocimiento, esta información se brinda teniendo en cuenta la encuesta realizada a un grupo selecto de personas que desconocen varios factores de esta índole, ya que, todos se conectan a internet y manejan sus respectivas redes, pero, no cuentan con instrucciones técnicas de redes, S.O, ciberdelincuentes, páginas no seguras, entre otros.

Durante la investigación realizada se describieron las consecuencias que generan los ciberataques en la sociedad colombiana, al indagar diversas fuentes, se logra identificar las secuelas que deja un ataque cibernético afectando de forma psicológica y económica a la víctima del asalto. Cabe resaltar que un ciberatacante no tiene límites, por lo tanto, puede chantajear, robar y sabotear, de acuerdo con el objetivo que desee cumplir ilícitamente.

A través de la evaluación de vulnerabilidades que existen en los dispositivos electrónicos como celulares, computadores y las plataformas digitales más utilizadas por las personas en Colombia se identificó mediante encuestas que la mayoría de la población colombiana desconoce los ataques cibernéticos y sus consecuencias, esta desinformación deja a los colombianos indefensos ante un ciberataque, dándole una ventaja desmesurada al atacante, permitiéndole obtener la información de su víctima de forma más fácil y accesible.

Se propone un manual de buenas prácticas de usuario que mitiguen el riesgo de sufrir un ciberataque en la población colombiana, mediante este, sus lectores podrán conocer cuáles son las consecuencias que podría traer ser víctima de un ataque cibernético y múltiples métodos que serán de ayuda para prevenirlos, evitando la filtración de su información, este manual además de explayará las vulnerabilidades más comunes en los dispositivos electrónicos utilizados por los colombianos, educándolos en el adecuado y seguro uso de éstos.

10. RECOMENDACIONES

Manejar distintas contraseñas seguras en los diferentes sitios en los que se navega, tales como redes sociales, correos electrónicos, páginas bancarias y demás. Tener en cuenta que las contraseñas se ponen acorde a los requerimientos del sitio o servicio al que se pretenda acceder. Es importante aclarar que las contraseñas seguras contienen letras mayúsculas y minúsculas, números y caracteres especiales.

Validar que la página en la que se encuentra navegando posea el ícono de cerrojo que indica navegación en página segura. El símbolo del cerrojo afirma que el navegar ha tenido una conexión privada con el sitio web, adicional cuenta con certificado de seguridad y que el navegador que se está utilizando confía en dicho certificado.

Realizar una limpieza frecuente en los navegadores utilizados, eliminando cookies, historial, contraseñas y caché. Esta acción soluciona inconvenientes que se presentan en algún sitio web y el formato de este, también mejora la velocidad del sitio y el más importante, borra los datos que se tenían guardados para navegar en algunos sitios más rápido sencillo, evitando que intrusos al entrar al equipo, roben información por no cerrar sesión de manera correcta.

Conectar sus dispositivos electrónicos a redes que sean confiables y seguras. Las redes seguras son aquellas que se conocen, por ejemplo, la del trabajo, casa, algún familiar cercano etc. Evitar conectarse a redes públicas, como en aeropuertos, centros comerciales, restaurantes etc.

Evitar compartir sus contraseñas de cualquier índole (dispositivos electrónicos, redes sociales, cuentas bancarias) y demás con otras personas. La seguridad es primordial y esta puede ser una brecha para que accedan y manipulen información privada.

Utilizar un antivirus acorde a sus necesidades descargándolo desde una fuente completamente fiable. Todos los antivirus realizan la misma función, desde que este activo, se utilice, se actualice frecuentemente y se haga uso correcto de páginas y descargas, no se tendrá problemas con la fuga de información y los dispositivos estarán seguros.

Descargar un gestor de contraseñas que le permita guardar las contraseñas encriptadas. Se sugiere la aplicación LastPass, ya que, dicha aplicación permite guardar diversa cantidad de contraseñas seguras, almacenarlas en una bóveda y acceder a ellas con facilidad, teniendo en cuenta que están en línea y no estarán almacenadas donde sean vistas con facilidad.

Recurrir al uso de VPN’s o aplicaciones de cifrado de tráfico al ingresar a páginas web que desconozca o sean no fiables.

Evitar exponer su día a día en redes sociales, no comparta su ubicación, relaciones cercanas, lugares frecuentes o estados financieros.

Usar los canales que expone la Fiscalía General de la Nación y la Policía Nacional para denunciar los ataques cibernéticos.

11. BIBLIOGRAFÍA

ÁTICO 34. Suplantación de identidad. Tipos y causas [En línea]. 25 julio de 2019 -. [Fecha de consulta: 10 de octubre 2020]. Disponible en https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/

ASMAR SOTO Salomón Transacciones digitales han aumentado, pero solo 20% de los usuarios las hacen [en línea]. Bogotá D.C 09 mayo de 2020 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible https://www.larepublica.co/especiales/el-boom-de-los-pagos-en-linea/transacciones-digitales-han-aumentado-pero-solo-20-de-los-usuarios-las-hacen-3036049

BBVA. Phishing', 'vishing', 'smishing', ¿qué son y cómo protegerse de estas amenazas? [en línea]. España abril 25 de 2019 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible en https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

BRANCH. Estadísticas de la situación digital de Colombia en el 2020-2021. [en línea]. -. [Fecha de consulta: 11, de abril 2022]. Disponible en https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2020-2021/#:~:text=Dispositivos%20que%20m%C3%A1s%20utilizan%20los%20usuarios%20de%20Internet&text=%E2%80%93%20Tel%C3%A9fonos%20inteligente%20(smartphone)%3A%2097.5,%E2%80%93%20Tablets%3A%2035.6%25.

CIBERSEGURIDAD. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. [en línea]. Bogotá D.C 09 mayo de 2020 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible en https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

CCIT. Estudio tendencias del cibercrimen 2019-2020 [en línea]. Bogotá D.C. 2019-. [Fecha de consulta: 05 de octubre 2020]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf.

CCIT. Estudio tendencias del cibercrimen 2019-2020 [en línea]. Bogotá D.C. 2019-. [Fecha de consulta: 10 de abril 2022]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CCIT. Informe Tendencias del cibercrimen primer trimestre 2020 [En línea]. Bogotá D.C. 2019-. [Fecha de consulta: 05 de octubre 2020]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-abril-2020-final.pdf.

CCIT. Informe de tendencias de cibercrimen [en línea]. Bogotá D.C. 2019-. [Fecha de consulta: 25 de noviembre 2020] Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CONCEPTODEFINICION. Social [en línea]. 13 enero de 2017 -. [Fecha de consulta: 29, de noviembre2020]. Disponible en https://conceptodefinicion.de/social

FISCALÍA GENERAL DE LA NACIÓN. [En línea]. [Fecha de consulta: 21 de mayo 2022]. ¡Disponible en https://www.fiscalia.gov.co/colombia/servicios-de-informacion-al-ciudadano/donde-y-como-denunciar/#:~:text=En%20el%20Centro%20de%20contacto,sistema%20de%20denuncia%20virtual%20%C2%A1ADenunciar!

FORBES STAFF. En 2020 Colombia tendría 50,3 millones de habitantes. [En línea]. Bogotá D.C 31 enero de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://forbes.co/2020/01/31/actualidad/en-2020-colombia-tendria-503-millones-de-habitantes

FORBES STAFF. 'Tenemos que lograr que Colombia sea el Silicon Valley de América Latina'. [en línea]. Bogotá D.C 02 septiembre de 2020 -. [Fecha de consulta: 08, de octubre 2020]. Disponible en https://forbes.co/2020/09/02/tecnologia/tenemos-que-lograr-que-colombia-sea-el-silicon-valley-de-america-latina/

FUNDACION KARISMA. Vulnerabilidades reportadas por el K+LAB de Karisma a entidades públicas en 2020 [En línea]. 27 enero de 2021 -. [Fecha de consulta: 15 de marzo 2022]. Disponible en https://web.karisma.org.co/vulnerabilidades-reportadas-por-el-klab-de-karisma-a-entidades-publicas-en-2020/#ancla2

GRANJAS MATÍAS, Simón. Colombia, uno de los países con más dificultades en acceso a internet [en línea]. Bogotá D.C 28, mayo de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/internet-calidad-de-conexion-en-colombia-con-mas-dificultades-en-el-mundo-529850

INTERNETPASOAPASO. ¿Cuáles son las principales vulnerabilidades de los dispositivos móviles y cómo podemos protegernos antes diversas amenazas? [En línea] -. [Fecha de consulta: 11 de abril 2022]. Disponible en https://internetpasoapaso.com/vulnerabilidades-dispositivos-moviles/

INTERPOL. Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad. [en línea]. 11 agosto de 2020 -. [Fecha de consulta: 20, de noviembre2020]. Disponible en https://www.interpol.int/es/Delitos/Ciberdelincuencia.

IDGRUP). ¿Qué es un Firewall? [en línea].14 octubre de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://idgrup.com/firewall-que-es-y-como-funciona/

KASPERSKY. Amenazas de seguridad móvil dirigidas a dispositivos Android. [en línea]. [Fecha de consulta: 13, de marzo 2022]. Disponible en https://latam.kaspersky.com/resource-center/threats/mobile

JIMENEZ. Javier Consejos de seguridad y privacidad para mensajería instantánea. [en línea]. Bogotá D.C 13 septiembre de 2019 -. [Fecha de consulta: 17, de marzo 2022]. Disponible en https://www.redeszone.net/tutoriales/seguridad/mensajeria-instantanea-sustituye-email-seguridad/

JIMENEZ. Javier. Principales amenazas de seguridad en una web. [en línea]. Bogotá D.C 23 junio de 2021 -. [Fecha de consulta: 17, de marzo 2022]. Disponible en https://www.redeszone.net/tutoriales/seguridad/principales-amenazas-seguridad-web/

KASPERSKY. ¿Qué es la ciberseguridad? [en línea]. Agosto de 2019-. [Fecha de consulta: 24 de noviembre 2020]. Disponible en https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

LEADER. 10 consejos de seguridad para dispositivos móviles. [en línea]. B -. [Fecha de consulta: 17, de marzo 2022]. Disponible en https://www.leader-network.com/movilidad/10-consejos-de-seguridad-para-dispositivos-moviles/

MEDINA Rosgaby. Estadísticas de la situación digital de Colombia en el 2019 y 2020. [en línea]. Colombia 17 abril de 2020 -. [Fecha de consulta: 25, de noviembre 2020]. Disponible en https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2019-y-2020/#:~:text=de%20redes%20sociales-,El%2069%25%20de%20la%20poblaci%C3%B3n%20total%20de%20Colombia%20es%20usuaria,de%203.4%20millones%20de%20personas.

MINTIC. Investigación, desarrollo e innovación. [en línea]. Bogotá D.C 07 septiembre de 2020 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible en https://www.mintic.gov.co/portal/inicio/Micrositios/I+D+I/Nodos/6120:Ciberseguridad

MONTERROSA BLANCO, Heidy. Este es el costo en el que incurren las empresas al no detectar a tiempo un ciberataque. [en línea]. Bogotá D.C 19 septiembre de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.larepublica.co/internet-economy/este-es-el-costo-de-no-detectar-a-tiempo-un-ciberataque.

MOLANO TORRES, Natalia. Colombia es el tercer país con más ataques de ingeniería social en América Latina. [en línea]. 06 noviembre de 2019 -. [Fecha de consulta: 29, de noviembre2020]. Disponible en https://www.larepublica.co/empresas/colombia-es-el-tercer-pais-con-mas-ataques-de-ingenieria-social-en-america-latina

MORALES, Juan David. Las redes sociales, un nuevo universo para emprendedores. [En línea]. Bogotá D.C 28, mayo de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible https://www.eltiempo.com/tecnosfera/novedades-tecnologia/las-redes-sociales-un-nuevo-universo-para-emprendedores-500800

NEOATTACK. (15 de 10 de 2020). Redes sociales, ventajas y desventajas [en línea].15 octubre de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://neoattack.com/ventajas-y-desventajas-de-las-redes-sociales

OBESO, Paula. Redes sociales: qué son, cómo funcionan, qué tipos existen y cómo influyen en las estrategias de Marketing. [en línea].12 diciembre de 2019 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://rockcontent.com/es/blog/que-son-las-redes-sociales/

PAREJA. Deicy. . ¿Pueden hackear tus datos biométricos con fotos de internet? [en línea]. agosto 08 de 2019 -. [Fecha de consulta: 13, de octubre 2020]. Disponible en https://www.pragma.com.co/blog/pueden-hackear-tus-datos-biometricos-con-fotos-de-internet

PEREZ, Enrique. Todo lo que podemos hacer en Instagram sin instalar la app: subir stories, guardar fotos y más. [en línea]. MountinView, CA 22 febrero de 2018 -. [Fecha de consulta: 25, de noviembre 2020]. Disponible en https://www.xatakandroid.com/aplicaciones-android/como-utilizar-instagram-desde-la-web-sin-instalar-la-aplicacion

PERALLIS SECURITY. 7 amenazas a la seguridad de los dispositivos móviles que debe tomar en serio en 2019. [en línea]. [Fecha de consulta: 13, de marzo 2022]. Disponible en https://www.perallis.com/noticias/7-amenazas-a-la-seguridad-de-los-dispositivos-moviles-que-debe-tomar-en-serio-en-2019

PORTAFOLIO. Cifras de ciberseguridad en Colombia prenden alarmas al cierre de 2020 [en línea]. Diciembre 10 2020 Bogotá D.C. [Fecha de consulta: 10 de abril 2022]. Disponible en https://www.portafolio.co/tendencias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020-547412

RAE**.** Ataque [en línea]. [Fecha de consulta: 29, de noviembre2020]. Disponible en https://dle.rae.es/ataque

RAMIREZ, Ivan. Cómo guardar un chat entero de WhatsApp con sus imágenes, stickers y demás. [en línea]. Bogotá D.C 06 noviembre de 2020 -. [Fecha de consulta: 25, de noviembre 2020]. Disponible en https://www.xatakandroid.com/tutoriales/como-guardar-chat-entero-whatsapp-sus-imagenes-stickers-demas

RAYA, Adrian. Así es la función para borrar mensajes enviados de Facebook Messenger [en línea]. 20 abril de 2018 -. [Fecha de consulta: 11 de diciembre 2020]. Disponible en https://www.elespanol.com/omicrono/software/20180420/funcion-borrar-mensajes-enviados-facebook-messenger/301221188_0.html

SECURE KIDS.¿Qué es el control parental y para qué sirve?
[en línea].25 agosto de 2015 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://securekids.es/que-es-el-control-parental-y-para-que-sirve/

SOFISTIC. La breve historia de la ciberseguridad. [En línea]. Bogotá D.C 30 noviembre de 2019 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

SPUTNI PACHON, Andrés. Las redes sociales, un nuevo universo para emprendedores [en línea]. Costa Rica 06 de junio 2020-. [Fecha de consulta: 05 de octubre 2020]. Disponible en https://www.elpais.cr/2020/06/06/otra-pandemia-en-colombia-se-expande-por-correo-electronico/

TECNICOM. Los 6 daños psicológicos y emocionales más comunes tras un robo, según Tecnicom [En línea]. 22 mayo de 2018 -. [Fecha de consulta: 29 de noviembre 2020]. Disponible en https://www.merca2.es/los-6-danos-psicologicos-y-emocionales-mas-comunes-tras-un-robo-segun-tecnicom/

TECNOSFERA. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. [en línea]. Bogotá D.C 20, octubre de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

TECNOSFERA. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. [en línea]. Bogotá D.C 20, octubre de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

TECNOLOGIA. Delitos informáticos aumentaron en Colombia durante la cuarentena. [en línea]. Bogotá D.C 04 agosto de 2020 -. [Fecha de consulta: 05, de octubre 2020]. Disponible en https://www.semana.com/on-line/tecnologia/articulo/delitos-informaticos-aumentaron-en-colombia-durante-la-cuarentena/662686/

UNITY. Consejos de seguridad en Redes Sociales. [en línea]. -. [Fecha de consulta: 18, de marzo 2022]. Disponible en https://www.unitypromotores.com/consejos-seguridad-redes-sociales/

UNIVERSIDAD PAMPLONA. Instructivo_ICONTEC_1486. {En línea}. {Consultado el 17 de marzo 2022}. Disponible en: https://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

RAE

Fecha de Realización:	28 de Agosto del 2020
Programa:	Especialización Seguridad Informática
Línea de Investigación:	Investigación Gestión de Sistemas
Título:	Ciberataques, riesgos y consecuencias que han afectado a la población colombiana entre los años 2018 y 2020.
Autor(es):	Tatiana Esperanza Figueroa Cubillos
Palabras Claves:	Cibercrimen, ciberdelincuentes, phishing redes Sociales y Ransomware
Descripción:	A través de este trabajo se pretende generar en la población colombiana conciencia respecto al tema de Ciberataques entre los años 2018 al 2020, exponiendo las estrategias más comunes utilizadas por los cibercriminales a nivel nacional, que burlan la protección de las plataformas digitales y dispositivos tecnológicos, logrando obtener información personal y así cumplir con su objetivo.

Fuentes bibliográficas destacadas:

ÁTICO 34. Suplantación de identidad. Tipos y causas [En línea]. 25 julio de 2019 -.
[Fecha de consulta: 10 de octubre 2020]. Disponible en https://protecciondatoslopd.com/empresas/suplantacion-de-identidad/

ASMAR SOTO Salomón Transacciones digitales han aumentado, pero solo 20% de
los usuarios las hacen [en línea]. Bogotá D.C 09 mayo de 2020 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible
https://www.larepublica.co/especiales/el-boom-de-los-pagos-enlinea/transacciones-digitales-han-aumentado-pero-solo-20-de-los-usuarios-lashacen-3036049

BBVA. Phishing', 'vishing', 'smishing', ¿qué son y cómo protegerse de estas amenazas? [en línea]. España abril 25 de 2019 -. [Fecha de consulta: 17, de noviembre 2020]. Disponible en https://www.bbva.com/es/phishing-vishingsmishing-que-son-y-como-protegerse-de-estas-amenazas/
BRANCH. Estadísticas de la situación digital de Colombia en el 2020-2021. [en línea]. -. [Fecha de consulta: 11, de abril 2022]. Disponible en

https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-decolombia-en-el-2020-2021/#:~:text=Dispositivos%20que%20m%C3%A1s%20utilizan%20los%20usuarios%20de%20Internet&text=%E2%80%93%20Tel%C3%A9fonos%20inteligente%20(smartphone)%3A%2097.5,%E2%80%93%20Tablets%3A%2035.6%25.

CIBERSEGURIDAD. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. [en línea]. Bogotá D.C 09 mayo de 2020 -. [Fecha de consulta:17, de noviembre 2020]. Disponible en https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibecolombia/276556

CCIT. Estudio tendencias del cibercrimen 2019-2020 [en línea]. Bogotá D.C. 2019-. [Fecha de consulta: 05 de octubre 2020]. Disponible en https://www.ccit.org.co/wpcontent/uploads/informe-tendencias-final.pdf.

CCIT. Estudio tendencias del cibercrimen 2019-2020 [en línea]. Bogotá D.C. 2019-. [Fecha de consulta: 10 de abril 2022]. Disponible en https://www.ccit.org.co/wpcontent/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Contenido del documento:	Debido a la gran influencia tecnológica que se tiene en los últimos años, la ola de ciberataques crece al mismo nivel, permitiendo que los cibercriminales generen una ganancia económica derivada por diferentes delitos como hurto por medios informáticos, violación de datos personales, acceso abusivo a un sistema informático, transferencia no consentida de activos y el uso de software malicioso. El factor humano sabe de la existencia de este tipo de delitos, pero no hay conciencia del gran peligro al que se encuentra expuesto. La importancia de esta monografía radica en explicar los métodos más comunes que los ciberdelincuentes utilizan para realizar ciberataques a la población colombiana y sus consecuencias en lo económico y moral, revelando estadísticas

	de estudios y análisis realizados por diversas fuentes a nivel nacional. Estos ataques son ejecutados por diversos medios virtuales o telefónicos ocasionando daños irreversibles en una empresa o en una persona. En este trabajo se exponen los ciberataques, riesgos y consecuencias que han afectado a los colombianos en los últimos 2 años.
Marco Metodológico:	La falta de conocimiento de las personas respecto al tema de ciberseguridad ha permitido que muchos ciber atacantes utilicen diversas técnicas para cometer sus actos delictivos, por diversos medios, sea por redes sociales, modalidad telefónica, envió de correos electrónicos entre otros. Al abordar el elemento de ciberseguridad más inestable: las personas. Al incumplir las buenas prácticas de seguridad, por error una persona puede dejar entrar un virus en cualquier dispositivo electrónico
Conceptos adquiridos :	Análisis: Es la manera de entender un tema en específico, minuciosamente. Ciberataques: Es un ataque informático organizado por una o un grupo de personas que provoca daños En un sistema informático o una Red. Estos ataques aprovechan alguna vulnerabilidad del recurso humano para acceder al software de algún dispositivo. Método Phishing: El BBVA como entidad financiera, invierte en de ciberseguridad para que sus clientes se sientan confiados en los procesos que realiza en dicho banco. Para el BBVA es importante ayudar a las personas y brindar de forma clara, información de algunos métodos. Ransomware: Es un método que se utiliza para infectar un equipo y de manera remota, bloquear y robar información para controlarla y así pedir un pago para el

	rescate de esta.
Conclusiones:	El presente trabajo identificó las diferentes técnicas de ciberataques más frecuentes que se han presentado entre el 2018 al 2020 en Colombia, la importancia de conocer las técnicas que utilizan los ciberdelincuentes que afectan a la población colombiana, ya que, recurrentemente estos ataques se han convertido en un dolor de cabeza para la comunidad. Los colombianos no están preparados para este tipo de ataques por falta de conocimiento, esta información se brinda teniendo en cuenta la encuesta realizada a un grupo selecto de personas que desconocen varios factores de esta índole, ya que, todos se conectan a internet y manejan sus respectivas redes, pero, no cuentan con instrucciones técnicas de redes, S.O, ciberdelincuentes, páginas no seguras, entre otros.