UNIVERSIDAD MIGUEL HERNÁNDEZ

Facultad de Ciencias Sociales y Jurídicas de Elche

GRADO EN SEGURIDAD PÚBLICA Y PRIVADA - SEPP

Curso académico 2021- 2022

ESTUDIO SOBRE CIBERSEGURIDAD EN EL MUNICIPIO DE RELLEU

Trabajo Fin de Grado

Alumno: José Manuel Salamanca Barragán

Tutor: José Luis Sainz- Pardo Auñón

"Estudio sobre ciberseguridad
en el municipio de Relleu"
Trabajo Fin de Grado

ÍNDICE

b) Resumen o abstract.

Resumen:

Desde años inmemorables ha existido el espionaje y los delitos ilegales, pero con los avances de las tecnologías y la facilidad de mantener el anonimato a través de ellas, se han potenciado en gran medida. Promoviendo en la red la ciberdelincuencia, el ciberterrorismo y el cibercrimen, mediante ataques de diferentes formas. El método más empleado en el ciberespionaje es el Malware y/o la ingeniería social, los cuales permiten adquirir información sobre el lugar que se pretende invadir, y así, generar distintos ataques y conseguir sus objetivos. De aquí surge la necesidad de la ciberseguridad, para proteger el entorno cibernético y asegurar la integridad de la persona que hay detrás de la pantalla. Sin embargo, la invasión en la red no se puede predecir, por lo que sería conveniente la implementación de diversos programas para prevenir los ciberataques y combatirlos. Por ello, se plantea una investigación cuantitativa de corte probabilístico, acerca de la vulnerabilidad de la ciudadanía frente a los posibles ataques en la red. Del mismo modo, se ha profundizado en las diferentes redes sociales más utilizadas, el uso en el que las emplean y la protección de los dispositivos electrónicos. Así como, descubrir la frecuencia en la que realizan copias de seguridad y medir el conocimiento que poseen sobre la inteligencia informática.

Palabras claves: ciberseguridad; espionaje; ingeniería social; malware; ataques.

Abstract:

Espionage and illegal crimes have existed since time immemorial, but with advances in technology and the ease of maintaining anonymity through them, they have been greatly enhanced. Promoting cybercrime, cyberterrorism and cybercrime on the network, through attacks in different ways. The most widely used method in cyberespionage is Malware and/or social engineering, which make it possible to acquire information about the place that is intended to be invaded, and thus, generate different attacks and achieve their objectives. From here arises the need for cybersecurity, to protect the cyber environment and ensure the integrity of the person behind the screen. However, the invasion of the network cannot be predicted, so it would be advisable to implement various programs to prevent cyberattacks and combat them. For this reason, a quantitative probabilistic investigation is proposed, about the vulnerability of citizens in the face of possible attacks on the network. In the same way,

the different most used social networks have been deepened, the use in which they are used and the protection of electronic devices. As well as, discover the frequency in which they make backup copies and measure the knowledge they have about computer intelligence.

Key words: cybersecurity; espionage; social engineering; malware; attacks.

c) Introducción

El espionaje aparece con el ser humano desde tiempos inmemoriales, donde se ojeaba las estrategias del pueblo vecino, así como, en multitud de guerras importantes de este país. Asimismo, los medios de comunicación y los avances de las Tecnologías de la Información y Comunicación han servido de vía para emplear el espionaje, amenazas, suplantamiento de identidad, entre otras.

Debido a los avances tecnológicos y la cantidad de piratas informáticos existentes se pueden clasificar varias clases de ataques. Por un lado, se encuentra la Clase I, centrada en la seguridad personal, así como, la privacidad de información. La Clase II, centrada en el espionaje entre organizaciones, tanto entre empresas como entre estados. Por último, la Clase III, enfocada en los ataques tecnológicos, como, por ejemplo, la propaganda de mensajes para promover daños. Además, es de vital importancia conocer el término *malware* y sus métodos de ataque. Los ciberdelincuentes o piratas informáticos, son capaces de recopilar información de gran valor a través del malware o de la ingeniería social.

Todos estos movimientos en la red causan la necesidad de protección e integridad de la información a todas las escalas, de este modo nace la ciberseguridad. Para garantizar y aplicar la seguridad en el ciberespacio, proteger la privacidad y libertad se convierte en la principal estrategia de los países desarrollados. El mundo de la red exige un compromiso continuo frente a la evolución de las tecnologías, por lo que se crea la necesidad de una continua protección de información junto a un entorno seguro y fiable. Asimismo, surgen programas de protección frente a las amenazas, empleo preventivo de ciberataques, disminución y/o eliminación de la vulnerabilidad y medidas de reducción de daños.

Por lo que el objeto de investigación que se va a abordar, engloba a las personas que utilizan la red, específicamente, a un muestrario de ciudadanos del municipio de Relleu. Se trata de un análisis de la vulnerabilidad frente a los posibles ataques del ciberespacio. El estudio de investigación se ha llevado a cabo desde un enfoque cuantitativo, a través de una encuesta. Herramienta de investigación por la cual se obtiene y analiza datos mediante unas variables preestablecidas.

En un primero momento, y apesar de ser una encuesta anónima se han recogido ciertos datos básicos para organizar y analizar las estadísticas, así como el sexo y la edad. Seguidamente, se ha centrado en el nivel de protección de los dispositivos electrónicos de los ciudadanos, el uso de los medios de comunicación y descubrir la red social más utilizada.

Con toda la información recogida y analizada, se quiere tener una visión más concreta y objetiva de la realidad que viven las personas de un municipio pequeño, respecto a la ciberseguridad y las amenazas en la red, y con ello, se pretende incitar a la población al uso adecuado de sus dispositivos electrónicos y una concienciación individual o colectiva respecto a las amenazas existentes y sus consecuencias.

La idea de esta investigación surge a raíz de la experiencia adquirida a través de estudios realizados sobre la ciberseguridad, además de ser un hecho verídico y problemática que se observa a diario en los medios de comunicación. El ciberespionaje o amenazas, surgen indiferentemente de la persona que sea, se adentran en aquella que le de paso a entrar. Asimismo, los jóvenes comienzan con el uso de dispositivos electrónicos a una edad más temprana, por lo que la concienciación sobre una buena protección en la red va dirigida a todas las edades.

d) Estado de la cuestión y marco teórico.

Estado de la cuestión

Tras la búsqueda bibliográfica en fuentes secundarias, nos disponemos a hacer una descripción de algunos estudios realizados sobre el tema en cuestión.

En primer lugar, destacar un estudio de Javier Díaz, Paula Venosa y Nicolás Macia, entre otros (2021) denominado *"Investigación en ciberseguridad en un año de pandemia"*. Se trata de una investigación formada por un grupo determinado de personas que forma parte del LINTI (Laboratorio de Investigación de Nuevas Tecnologías Informáticas). En este artículo se describe un trabajo realizado para frenar la vulnerabilidad frente al malware, detección de ataques y gestión de incidentes. El pilar fundamental para el equipo de trabajo es centrar los proyectos en la formación de recursos humanos, es decir, formación para la comunidad. Por lo que, este grupo de personas no solo poseen conocimientos necesarios sobre la ciberseguridad, sino que emplean mecanismos y herramientas para implementar una defensa eficaz, ayudando a la población de manera directa u indirecta.

Otro estudio encontrado de Astorga-Aguilar y Schmidt- Fonseca (2019) titulado *"Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad"*

analiza el estado de conocimiento de los peligros en las redes sociales en línea y maneras de protegerse por medio de buena prácticas de ciberseguridad para menores. Se adentra en la evaluación de los términos de seguridad y privacidad, el rol de los padres frente a esta educación y algunos elementos de ciberseguridad de las redes sociales más populares. Se descubrió que los peligros más eventuales en la red son el ciberbullying, grooming, sexting y adicción. Además, las redes sociales más utilizadas son Facebook, Instagram, Whatsapp y Snapchat. Todas ellas poseen una serie de herramientas para velar por la privacidad, la cual se tiene que configurar en el control de herramientas, esto es lo que se conoce como ciberseguridad. Asimismo, en primer lugar tendrán que ser los propios padres los que se nutran de las normas de seguridad en las redes sociales para que sus hijos no sean un blanco fácil frente a los ataques. Por otro lado, aconseja el acompañamiento del menor y su supervisión del uso correcto de las redes sociales con el fin de brindar acciones preventivas.

Encontramos otro estudio de Carmen Sabater Fernández (2014) y recibe el título de *"La vida privada en la sociedad digital. La exposición pública de los jóvenes en internet."* Consta de una investigación realizada a una muestra de 400 estudiantes en la Comunidad Autónoma de La Rioja, a través de entrevistas y encuestas. Este estudio surge mediante la observación en la que los jóvenes entre 14 y 20 años, exteriorizan cada vez más su vida privada, personal e intima por las redes sociales y diferentes aplicaciones. Asimismo, los resultados de la investigación indican que los jóvenes siguen manteniendo un espacio para su vida privada, sin embargo, en las redes sociales han incrementado la exposición de datos personales, fotografías y en el relato de los momentos cotidianos, compartiendo así, dicha información a sus contactos virtuales en un tablón público o semipúblico de las redes sociales.

Por otro lado, encontramos un estudio de Francisco Xavier Alvear Reinoso (2019) titulado "*Análisis y diseño de una propuesta para mitigar ataques cibernéticos a correos electrónicos utilizando técnicas de hacking ético*". En el mismo, detalla los ataques a correos electrónicos y cual es la información que el pirata informático necesita. Por lo que, basándose en casos reales, este estudio analiza los pasos que ha realizado el atacante hasta conseguir lo deseado. Además, analiza las posibles soluciones que ofrecieron las empresas ante este tipo de acontecimiento para que no se vuelva a repetir.

A Través de *Hacking Ético*, se realizaron ataques de diferentes tipo como: spoofing, mailing y correos híbridos con todos los ataques, de este modo por medio de Amazon Web Service llegó a atacar a 200 personas mediante correos reales, para conseguir una estadística y detectar qué personas son más vulnerables y qué información han dado al atacante. Para esto, plantea una solución para que las personas o empresas, no sean víctimas de ataques de robo de información, financiero o de otros tipos.

Encontramos también un artículo titulado: *"La influencia de las nuevas tecnologías: videojuegos, redes sociales e internet, en los consumidores seniors en España"* de Ana Sebastián y Gema Martínez " (2013). En él, se observa como la penetración a internet de las personas mayores va a un ritmo más lento que los del resto, aunque cada vez hay más personas mayores en la red. Asimismo, las autoras realizan una investigación cualitativa centrada en un análisis documental y en el estudio de casos sobre la influencia, beneficios y diferentes aplicaciones de las TICS. Todos los estudios analizados en esta investigación, demuestran que tanto el uso de videojuegos como de internet en general, por parte de las personas mayores favorecen sus habilidades cognitivas, afectivas y sociales. Además, facilita la integración social de dicho colectivo y aumenta su autoestima y creatividad, entre muchos otros aspectos más. Destacar, que este tipo de investigación con este colectivo, es poco usual en España y hay escasez de teoría científica sobre la temática, por lo que proporciona ricos conocimientos.

Otra investigación de Aina Giones- Valls y Marta Serrat-Brustenga (2010) denominada "*La gestión de la identidad digital: una nueva habilidad informacional y digital"*, describe la identidad digital en internet, resaltando las ventajas de una buena gestión, como son : la visibilidad, la reputación y la privacidad en la red; además, de las principales dificultades de una identidad. Del mismo modo, sitúa la gestión de la identidad digital como una nueva habilidad fundamental dentro de la información. Este nuevo método de comunicación, distingue dos clases de individuos, el que pertenece a la sociedad informatizada y la que no, creando una brecha digital entre ambos. La construcción de la identidad digital en la red implica un aprendizaje y una participación dentro de la cultura digital, en la que es absolutamente necesario conocer las tecnologías actuales y la forma de emplearla para brindar a toda la sociedad las herramientas fundamentales.

Por último, destacaremos un estudio titulado: *"Técnica de protección para credenciales de autenticación en redes sociales y correo electrónico ante ataques phishing*" de Paola Andrea Noreña y Sergio Calderón (2018). La investigación desarrollada en este artículo se centra en observar una necesidad en la industria y desarrollar la solución. Es decir, detener y prevenir ataques phishing en redes sociales y correos electrónicos, mediante técnicas para prevenir los riesgos, a partir del conocimiento, atención y cuidado visual del usuario. La técnica preventiva congrega 4 fases como son: Prevención al ingresar a la red social o al correo electrónico, Verificación del nombre del dominio, Prevención en la administración de credenciales al inicio de sesión, Análisis de indicadores de Seguridad.

Marco teórico

Los medios de comunicación y avances que brindan las Tecnologías de la Información y Comunicación (TIC) son incuestionables, del mismo modo que la dependencia que los ciudadanos poseen sobre ellas y los peligros y amenazas a los que están expuestos (Centro Criptológico, 2020).

Origen

El origen del espionaje ha acompañado al ser humano desde tiempos inmemorables, ya que conocer información de pueblos cercanos produce ciertas ventajas sociales. Asimismo, utilizaban diferentes métodos para encriptar la información escrita. El telégrafo y la radio han sido métodos pioneros en la encriptación de información, y junto a esto el espionaje (Maroto, 2009).

Un ejemplo de ello, es la máquina *Enigma* empleada por el Ejército alemán durante la Segunda Guerra Mundial. Según González (2018) dice que Enigma era: "una máquina de rotores utilizada por la armada alemana tanto para cifrar como para descifrar mensajes".(p.40)

Además, consistía en: Un sistema de comunicaciones capaz de saltar entre frecuencias para la transmisión de información, una técnica de modulación de señales en espectro expandido que usaban un par de tambores perforados y sincronizados para cambiar entre 88 frecuencias. Este sistema se diseñó y utilizó para construir torpedos teledirigidos por radio que no pudieran detectar los enemigos. (p.39)

Por otro lado, existen muchos ejemplos antiguos de ataques a gran escala como, *Ninda* de 2001. Se empleó el ataque "gusano", el cual Maroto (2009) define como: "Programa diseñado para aplicarse en gran número y distribuirse de un equipo a otro automáticamente. El resultado puede ser un intenso tráfico de red que hace más lentas las redes empresariales o Internet. También pueden permitir que otro usuario tome el control del equipo de forma remota". Este ataque no recibió la grandeza deseada, pero es un ejemplo de ataque automatizado de gran peso. Se difundió por Estados Unidos en una hora y su infección duró días, alcanzando a 86.000 ordenadores. Dos meses después, surgió el ataque Código Rojo, el cual se propagó a 150.000 ordenadores en 14 días aproximadamente.

Acontecimientos como los mencionados, hicieron que, en Estados Unidos, los especialistas en inteligencia y defensa pusieran la ciberseguridad al frente de la Seguridad Nacional (Maroto, 2009).

Conceptos de interés

Para una mayor comprensión se muestra una serie de definiciones esenciales para entender el mecanismo tan avanzado que coexisten en la red y que influye en nuestro día a día.

Según Curtis (2011) describe al e**spacio cibernético o ciberespacio**, como: "dominio artificial construido por el hombre, diferenciado de los otros cuatro dominios de guerra (tierra, aire, mar y espacio)". Se trata de un término aislado de otros dominios, aún así completamente vinculado y reforzado por otros medios físicos, como por ejemplo, las redes eléctricas. Si sufren ataques en sus interconexiones, esto puede derivar en repercusiones severas en cuanto a las estrategias de seguridad. (Gamón, 2017).

Por otro lado, el Departamento de Defensa de los Estados Unidos (2016) define al **ciberespacio** como: "un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información (incluyendo internet), redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores" (p.58).

El avance de las tecnologías y del uso a Internet no solo ha traído un nuevo descubrimiento hacia la información, sino también, hacia el lado oscuro, donde nacen nuevos términos como: cibercrimen, ciberespionaje, ciberdelincuencia, ciberterrorismo, entre otros.

El Consejo de Europa define el **ciberterrorismo** como: "terrorismo que utiliza las tecnologías de la información para poder intimidar, coaccionar o causar daños a grupos sociales con fines políticos-religiosos". (Subijana Zunzunegui, 2008).

Por otro lado, la **ciberdelincuencia** es definida por Ureña (2015) como: "toda aquella acción ilegal que se da por las vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet".

Otro concepto a destacar es el **cibercrimen** el cual:

Abarca desde el delito económico, como el fraude informático, el robo, la falsificación, el *computer hacking,* el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos ilegales (...) (Sánchez, 2012).

A diferencia de cualquier otro delito, el cibercrimen se nutre del ciberespacio, de la red, para realizar actividades ilegales. Por otro lado, el ciberterrorismo y la ciberdelincuencia tiene una gran conexión, aun así, el ciberterrorismo sobrepasa los límites de la delincuencia, debido a que buscan beneficios distintos, acentuando la ilegalidad a un rango superior. El ciberterrorismo busca generar un daño mayor por motivos políticos-religiosos, mientras que el beneficio del cibercrimen, por ejemplo, se centra en aspectos económicos (Sánchez, 2012).

Estos términos mencionados, poseen cuatro características genéricas, verbalizadas por Subijana (2008):

-Se cometen fácilmente.

-Requieren escasos recursos en relación al perjuicio que causan.

-Pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma.

-Se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas. (p. 171)

Clases de ataque

El ciberespacio une a todos los países del mundo, permitiendo a personas con mala intención adentrarse y actuar en sistemas a miles de kilómetros. Estos ataques en la red se ejecutan con gran rapidez, lo cual dificulta encontrar su origen. Asimismo, es fundamental defender los sistemas frente a cualquier asalto (Maroto, 2009). Para ello, y para un mejor análisis en profundidad de los posibles daños, se presentan las tres formas de ataques que Sánchez (2012) a descrito por clases:

- Clase I, *Personal Information Warfare*: área relacionada con las cuestiones y la seguridad personal, así como la privacidad de los datos y del acceso a las redes de información.
- Clase II, *Corporate/Organizational Level Information*: área del espionaje clásico entre organizaciones de diferente nivel (de la empresa al Estado) o al mismo nivel (de Estado a Estado).
- Clase III, *Open/Global Scope Information Warfare*: área relacionada con las cuestiones de ciberterrorismo a todos los niveles, como pueden ser: los ataques realizados desde computadoras a centros tecnológicos; la propaganda como forma para enviar sus mensajes y para promover el daño ocasionado por sus ataques; y/o la planificación logística de atentados tradicionales, biológicos o tecnológicos. (p.245-246)

Lo primero que hace cualquier hacker es examinar y visitar alguna zona donde se encuentren ***scripts***. Siguiendo con el mismo autor, Sánchez (2012) define a los *scripts* como: "ficheros de comando, que permiten agrupar órdenes que se dan a través del teclado. Los scripts son ampliamente utilizados en Internet y en programación atomizada de tareas". Mediante estos ficheros se escanea el sitio que se pretende invadir, con la finalidad de descubrir cuál es su arquitectura tecnológica básica. Es decir, indagan para descubrir qué sistema operativo utilizan y qué tipo de servidor de software ejecutan. Seguido, se realiza la parte más difícil: "encontrar "agujeros" o fallas en la versión específica del software de ese sitio, ya que éste puede proporcionar las "entradas" que permita romper su código"(Sánchez 2012, 246). Una vez encontrado lo deseado, esa información pasa a ser conocimiento público dentro de la comunidad hacker.

Malware y métodos de ataque

Como se ha mencionado anteriormente, los ciberdelincuentes o los hackers, son capaces de recopilar información de gran valor, mediante tipos de *malware.* La evolución de los mismos ha causado una mayor propagación en los últimos años. Sánchez (2012) hace referencia a *malware* como: "un virus, un caballo de Troya, una puerta trasera (backdoor), un programa espía (spyware), o un gusano". (p.262). Se compone principalmente de dos técnicas. La primera consiste en un análisis mediante un examen de comportamiento, y la segunda en la aplicación de técnicas para destapar el código en cuestión, técnica más compleja debido a que suele estar encriptado a través de un archivo binario. Además, según el Centro Criptológico (2020) a causa de un malware pueden generarse otros ataques como pueden ser:

- APT (Amenazas Persistentes Avanzadas). Se trata de ataques específicos de ciberespionaje o ciber sabotaje. Su destinatario puede ser la industria, la Administración o un particular. Este ataque lleva a cabo diferentes técnicas para realizar el delito, robo de información, de la manera más oculta posible.

- Ataques DDoS (Denegación de Servicios Distribuidos). Los cuales son realizados por un colectivo de personas o bots que atacan a un sistema a la vez. Esta acción provoca un colapso del sistema y deja de funcionar. Estos ataques son muy comunes y con fines propagandísticos.

- Ransomware. Este ataque se trata de un código nocivo, en el que el hacker cifra los datos a la víctima y exige cierta cantidad económica para la recuperación de la clave. Se considera una de las técnicas de malware que más ha evolucionado junto con la minería oculta de criptomonedas.

- Internet de las Cosas (IoT - Internet of Things). Recolecta información de todo tipo a través de objetos físicos. Los dispositivos IoT se utilizan a día de hoy para realizar ciberataques, además de para el espionaje y manipulación.

- Cryptojacking: Se trata de una estrategia para ganar dinero de manera delictiva conocida como *cryptojacking.* Técnica muy empleada también debido a su anonimato y monedas virtuales.

- Ataques a la cadena de suministros. Como es el caso de CCleaner (software de limpieza). Se trata de diferentes malware escondidos en las descargas del servicio.

- Cibercrimen como servicio (CaaS). La mayoría de sus servicios se realizan mediante *depp web.* Se trata de ataques digitales como si se tratara de una prestación legal mediante fraude, malware, ataques DDoS, ransomware, etc. A veces, incluso ataques mediante marketing y plataformas de compraventa.

- Hacktivismo. Se emplea mediante herramientas digitales ilegales para fines sociopolíticos. Se basa principalmente en la desfiguración de páginas webs, redirecciones y ataques al servidor, para realizar sabotajes y el robo de información.

- Desinformación. Son ciberamenazas en las que la información está manipulada y es totalmente falsa, difundida a la opinión pública con intenciones dañinas.

Identidad digital

Otro concepto a destacar e importante en este estudio es la Identidad Digital, la cual se define por Aparici y Osuna Acedo (2013) como: "todo lo que un individuo manifiesta en el ciberespacio e incluye tanto sus actuaciones como la forma en la que este es percibido por los demás en la Red".

Ingeniería social

La ingeniería social es una técnica esencial para el ciberespionaje. Se define como: "procedimiento mediante el cual un hacker engaña a otros para que revelen datos valiosos que le benefician de alguna forma" (Maroto 2009, 57).

"La Ingeniería Social es ampliamente utilizada por creadores de malware y delincuentes informáticos debido al alto nivel de eficacia logrado engañando al usuario" (Borghello 2009, 4).

Por otro lado, surge el término **Phishing,** el cual es la combinación de Ingeniería Social y exploits técnicos. Concretamente se trata de páginas web falsificadas donde se les redirecciona a los usuarios para extraer información confidencial. Estos ataques se pueden clasificar : según el servicio que ataquen o según el modus operandi. El primero respondería a bancos, pagos online y redes sociales, entre otras; mientras que el segundo se centraría en Software maliciosos, phishing engañosos,etc (Benavides, Fuertes, Sánchez y Nuñez, 2020).

Asimismo, es en la habilitación de un fraude en concreto, donde surge la ingeniería social, aplicada por los creadores de códigos y otro tipo de ataques. Cuanto más real se parece el mensaje, más posibilidad de engaño y así, alcanzar los propósitos propuestos (Borghello 2009, 4). Aunque los hackers emplean este método para obtener códigos o direcciones de correo para acceder a números de teléfono, los informes más actuales informan que se usan para actos como, la adquisición de números de tarjetas de créditos o otros daños financieros (Maroto, 2009).

Los fraudes más comunes a través de la red son el *mail spoofing* y la *web spoofing. "**Mail spoofing*** es un procedimiento mediante el cual se pretende suplantar el correo electrónico de un usuario o crear correos electrónicos supuestamente verídicos a partir de un dominio para poder enviar mensajes como si formasen parte de esa identidad" (Sánchez, 2012). Así mismo, cada vez es más habitual encontrar en la bandeja de entrada mensajes de entidades bancarias, con correos electrónicos creíbles y en los que, si aceptas estas ofreciendo tu dirección de correo electrónico, además de datos. Por otro lado, también existen mensajes en los que se solicita el número de las tarjetas de crédito y así realizar el fraude. ***Web spoofing*** trata de un engaño en el cual le hacen creer a la persona que está visitando una página web mientras que se trata de una réplica completamente controlada y monitorizada

por un ciberdelincuente. El cual pretende obtener toda la información y dinero posible (Sánchez, 2012).

Otro de los fraudes que se encuentran a la orden del día, destacablemente en menores son el **Grooming y el Sexting.** El **Grooming** se define por la Policía Nacional, específicamente, en el boletín de análisis de ciberseguridad, como:

La estrategia que una persona adulta desarrolla para ganarse la confianza de menores de edad a través de Internet, logra mantener una relación con el menor, haciéndose pasar por una persona de la misma edad, esto lo realiza con el fin de obtener material como imágenes o videos de índole sexual, generalmente inicia con un acercamiento lleno de empatía y engaños, y en una segunda fase inicia el chantaje para obtener mas contenidos que comprometan al niño, niña y/o adolescente (Policia Nacional, 2016).

En cuanto al **Sexting**, según el Instituto nacional de Tecnologías de la Comunicación (2011) lo define como: "una difusión o publicación de contenidos (principalmente fotografías y videos) de tipo sexual producidos por el propio remitente, utilizando para ello el teléfono móvil o cualquier otro dispositivo tecnológico". Existen diferentes riesgos a los que se exponen los practicantes de sexting, como: amenazas a la privacidad del menor, riesgos psicológicos, ciberbullying, sextorsión, grooming o riesgos físicos y geolocalización.

Añadir, que el Consejo de la Unión Europea expone mediante la siguiente infografía las principales ciberamenazas que ha sufrido la UE entre abril de 2020 y julio de 2021. La Unión Europea cada vez más, se está involucrando en estos ataques para proteger a las personas y empresas de la ciberdelincuencia y garantizar un ciberespacio seguro, abierto y protegido.

Gráfica N 1 - Infografía Consejo de la Unión Europea.

Violaciones de la seguridad de los datos y fugas de datos

Divulgación de datos sensibles, confidenciales o protegidos en un entorno no fiable.

*Se ha producido un **aumento de las violaciones de seguridad de datos sanitarios.***

Ataques distribuidos de denegación de servicio

Ataques que impiden a los usuarios de una red o sistema acceder a información, servicios u otros recursos pertinentes.

*Se han producido más de **10 millones de ataques distribuidos de denegación de servicio** debido a la COVID-19.*

Desinformación

Ataque intencionado consistente en crear o divulgar información falsa o engañosa para manipular a la opinión pública.

*La **COVID-19** es uno de los principales temas de los **ataques de desinformación**.*

Amenazas no malintencionadas

En su mayoría se deben a errores humanos, aunque también pueden darse como consecuencia de catástrofes naturales que causan daños en las infraestructuras informáticas.

*El **50 %** de estos ataques se deben a **fallos de configuración**.*

Gráfica N 1: Fuente Panorama de amenazas de ENISA (2021).

Por lo que, la Agencia de la Unión Europea para la Ciberseguridad (2021) recoge las principales ciberamenazas en un póster informativo, el cual se resume en:

- Programas de secuestro

  Encriptación de la información de una organización para solicitar rescate.

- Programas malignos

  Programas infiltrados en un dispositivo para impedir su buen funcionamiento y robar información.

- Cripto Secuestros o Criptomeria maliciosa

  Uso no autorizado del dispositivo electrónico para minar criptomonedas

- Ataques por correo electrónico

  Envío de mensajes o correos por el cual se intenta engañar al usuario y permita que accedan a su dispositivo (Phishing)

- Violaciones de la seguridad de los datos y fugas de datos

  Divulgación de datos sensibles en entornos no confiables

- Ataques distribuidos de denegación de servicio

  Ataques que impiden a los usuarios acceder a ciertos servicios en la red.

- Desinformación

  Divulgar noticias o información fake o falsa, para engañar y manipular la opinión pública.

- Amenazas no malintencionadas

  En su mayoría errores o causas no intencionadas que podrían impedir el buen funcionamiento de algunas estructuras informáticas

- Amenazas a la cadena de suministros

  Ataques a organizaciones a sus puntos vulnerables capaces de producir efectos en cascada.

Asimismo, el Centro Europeo de Delitos Cibernéticos de Europol pública la Evaluación de amenazas del crimen organizado en Internet (IOCTA). En su informe estratégico de 2021, se extraen una serie de conclusiones:

- El ransomware se ha aprovechado de las vulnerabilidades del teletrabajo.

- El aumento de mercado online lleva aparejado un incremento de las actividades intrusivas informáticas, como phishing, robos de identidad, banca online, etc.

- Creciente venta de productos médicos falsificados, como consecuencia de la la pandemia generada por la Covid-19.

- La Covid-19 ha provocado un mayor acceso de la población infantil a contenidos en línea, con los riesgos que ello conlleva.

- El comercio y la venta de datos privados, al amparo de accesos ilegales informáticos, es un mercado floreciente.

Doble factor de autenticación

Una forma de proteger los dispositivos electrónicos de los ataques o hackers informáticos, se trata de un sistema de autenticación basado en contraseñas de los usuarios. La información se protege mediante contraseñas privadas y seguras, a las que se le puede añadir un doble factor de autenticación. El cual se centra en emplear otro factor complementario a la contraseña, dándole una seguridad extra, dificultando así el paso de cualquier acceso inadecuado. En resumen, la autenticación básica suele ser una contraseña elegida por la persona en sus dispositivos electrónicos, y el doble factor de autenticación suele ser un código aleatorio generado por una aplicación externa (Alfonso, 2019).

Ciberseguridad

Para una mayor comprensión y cohesión del término ciberseguridad se recogen distintas definiciones que ofrecen diversos autores.

Para Newmeyer, Cubeiro y Sánchez (2015) la ciberseguridad es: "el conjunto de prácticas políticas, de entretenimiento y tecnología, diseñada para proteger el entorno cibernético con la finalidad de asegurar la integridad de la información y habilidad de conectar dispositivos para que operen según diseño".

Por otro lado, La Unión Internacional de Telecomunicaciones (2010) aprobó la Resolución 181, donde definió la seguridad como:

El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgo, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno.

Sin embargo, muchos autores expresan que no existe un consenso o una definición concreta del término ciberseguridad, es un tema aún por explotar. Estas definiciones se basan en la percepción de la amenaza en el ciberespacio, por lo que engloba diferentes técnicas y herramientas para hacer frente a los riesgos tecnológicos y de comunicación (UIT, 2010).

Asimismo, garantizar y aplicar la seguridad en el ciberespacio, y venerar la privacidad y libertad, es una de las primicias estratégicas de los países desarrollados. El mundo de la red exige un compromiso continuo ante la evolución de las tecnologías y de los

distintos ataques que van surgiendo. Por lo que, se crea la necesidad de protección de información junto con un entorno seguro y fiable (Centro Criptológico, 2020).

Programas frente a las amenazas

El ciberataque, el ciberespionaje y el cibercrimen desaparecen en la mayoría de los casos, debido a que están relacionados entre sí, por lo que uno es el paso previo de otro y sucesivamente. Sin embargo, no debemos obviar ningún paso para hacerles frente y combatirlos. Todas las estrategias diseñadas para combatir estas amenazas tienen que incluir la prevención de los ciberataques, un programa para la disminución y/o eliminación de la vulnerabilidad frente a ataques y medidas de reducción de daños.

Según Maroto (2009) *aparece El Programa Nacional de Reducción de Amenazas y Vulnerabilidades,* el cual intenta minimizar las amenazas y la vulnerabilidad para:

– Reducir y corregir las vulnerabilidades de *software*, identificando y arreglando las vulnerabilidades existentes que, si se explotaran, podrían causar la mayor parte del daño a los sistemas críticos.

– Impulsar el empleo de sistemas seguros de supervisión, control y adquisición de datos.

– identificar interdependencias de la infraestructura y mejorar la seguridad física de los sistemas vitales.

– Buscar vulnerabilidades en las nuevas tecnologías.

– Identificar y castigar actores maliciosos, mejorando las capacidades judiciales para la prevención y persecución de los ataques en el ciberespacio.

El mismo autor enseña *El Programa de Divulgación y Enseñanza sobre Seguridad del Ciberespacio,* debido a la necesidad de un desarrollo de prevención. Argumenta que las organizaciones que trabajan en la red deben tomar acciones proactivas para detener las posibles amenazas y arreglar sus vulnerabilidades, no esperar a que sean atacados. A pesar de ellos, es difícil descifrar cuándo surgirá un ciberataque, pero hay que estar preparados.

Cuando se utilice la red inalámbrica, se debe realizar una evaluación cuidadosa de los riesgos, ya que este tipo de comunicación puede sufrir ataques DoS, y pueden durar meses en volver a su estabilidad habitual (Maroto, 2009).

Marco legal

Todas las actividades e interacción en la red requieren de una serie de normas que regulen el comportamiento de todos los usuarios que practican en ella. Unas normas que avalen los derechos y deberes de los ciudadanos, pero que además ayude a un crecimiento y fortalecimiento de la actividad. Por lo que, en el ámbito de las TIC y la ciberseguridad, ha sido evidente la necesidad de protocolos y leyes que protejan a los ciudadanos, empresas y estados, de los diferentes ciberataques (Centro Criptológico, 2020).

Un avance importante en el desarrollo de las TIC ha sido la **Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos**. Dicha ley argumenta que la administración será la responsable de la eficacia del uso y estará bajo el principio de seguridad, respecto a la utilización de los medios electrónicos. Con la finalidad de preservar la integridad de los derechos fundamentales, específicamente con los principios de intimidad y protección de datos (Centro Criptológico, 2020).

Dicha Ley, también establece un Esquema Nacional de Seguridad (ENS), el cual se aprobó a través del **Real Decreto 3/2010, de 8 de enero**, actualizado posteriormente. Este esquema tiene como objetivo escoger la política de seguridad en la utilización de medios electrónicos, bajo una protección adecuada de la información (Centro Criptológico, 2020).

e) Objetivos/Hipótesis/Propósito.

Objetivos

En cuanto a los objetivos de la investigación, cabe mencionar los siguientes:

- Objetivo general:

Realizar un análisis de la vulnerabilidad frente a los posibles ataques del ciberespacio.

- Objetivos específicos:

- Descubrir el perfil más común
- Medir el nivel de protección de los dispositivos electrónicos
- Conocer la red social más utilizada.
- Analizar el uso de las redes sociales como medio de comunicación.
- Conocer la frecuencia en el que realizan copias de seguridad en los dispositivos.
- Descubrir el conocimiento que posee la población sobre los ciberataques.
- Medir la inteligencia informática que disponen.
- Conocer, si saben que es la identidad digital y cómo protegerla.

La presente investigación, tiene una serie de hipótesis que posteriormente se verificarán o, por el contrario, disentirán:

- Las personas que se encuentran en una franja de edad entre los 15 y los 30 descuidan la protección de sus dispositivos electrónicos.
- Contrariamente, el avance de las nuevas tecnologías informa sobre los ataques en ciberseguridad.
- El 80% de personas no realizan copias de seguridad.
- Muchas personas son conscientes de diferentes espionajes como las cookies, pero no le dan la importancia necesaria.
- Compartir diferentes finalidades en un mismo dispositivo, como lo laboral y lo personal, genera una vía libre para el ciberdelincuente para extraer información privada de ambas vías.
- La suplantación de identidad en menores de edad, ha desembocado en suicidios y/o problemas psicológicos.

Por tanto, el propósito de esta investigación se centrará en verificar si las hipótesis descritas están en lo cierto o no, a través de los resultados extraídos en la encuesta, que ha sido creada a través de una serie de objetivos que rigen el estudio.

f) Metodología.

A continuación, se da pie a contextualizar la metodología utilizada para examinar el objeto de investigación. Para ello, se encuentra recogido en él, el enfoque, el diseño, el procedimiento que se ha llevado a cabo, la técnica de recogida de datos y la ubicación y tiempo.

Enfoque

Respecto a la investigación que se ha llevado a cabo ha sido de enfoque cuantitativo, mediante un muestreo probabilístico, en el que se hace generalización de la población a partir de un muestreo. Esta recolección de datos nos ha permitido obtener una visión generalizada del municipio de Relleu y observar la vulnerabilidad existente frente a los posibles ataques en la red. Asimismo, mediante una encuesta proporcionada mediante un enlace a un gran número de ciudadanos han podido acceder a ella y completarla.

Además, este estudio se caracteriza por ser deductivo, como todos los estudios de investigación cuantitativos. Fernández (2002) dice que:

El hecho de que la metodología cuantitativa sea la más empleada no es producto del azar sino de la evolución del método científico a lo largo de los años. Creemos en ese sentido que la cuantificación incrementa y facilita la comprensión del universo que nos rodea y ya mucho antes de los positivistas lógicos o neopositivistas.

Población de estudio

Con lo que respecta a esta investigación, los participantes no han sido seleccionados a través de un muestreo no probabilístico de conveniencia, si no que se ha pretendido pasar un enlace con la encuesta de este estudio, a las personas suficientes para que representen mediante un muestreo a la totalidad de los ciudadanos de Relleu..

Diseño metodológico

El diseño metodológico empleado en esta investigación, parte con la elección del tema de estudio. Tras la elección de éste, se ha centrado en una búsqueda exhaustiva de documentación teórica y/o práctica a gran escala, y una lluvia de ideas para poder delimitar los temas tratados en esta investigación. Una vez elegidos los conceptos a tratar han sido desarrollados para contextualizar y obtener una mejor comprensión del estudio. Esta búsqueda y recopilación de documentación, ha sido extraída mediante fuentes secundarias de manuales, y artículos científicos de Google Académico y Dialnet.

Una vez obtenida toda la teoría en la que se basa esta investigación, se ha delimitado qué se quería mediar y conseguir, y cómo hacerlo. Por lo que se realizó una serie de objetivos, a través de hipótesis del estudio y se formuló unas preguntas que conforman la encuesta.

Procedimiento

Las encuestas de la investigación, fueron enviadas a través de las redes sociales, como email y WhatsApp, a un colectivo de personas que viven en Relleu, con la finalidad de que las mismas fueran propagando la encuesta hasta que recogiera a un gran número de participantes. La encuesta empieza con una pregunta abierta, además de informar que el cuestionario sería totalmente anónimo, en base a la Ley Orgánica de 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, y conformada por 18 preguntas cuantitativas.

Los participantes de esta investigación han sido un total de 161, por lo que este ha sido el total del muestreo frente a 1.173 habitantes en el municipio. Datos extraídos del 2021 a través del Instituto Nacional de Estadística.

Por último, cabe mencionar que los datos estadísticos de las encuestas han sido transcritos en un documento Excel y en Power BI junto con sus respectivas gráficas, para una mayor comprensión y un posterior análisis de resultados.

Técnica de recogida de datos/instrumentos

La técnica de recogida de datos empleada en esta investigación ha sido la encuesta. La encuesta se trata de un procedimiento estandarizado de recolección de información a una muestra o población (Blanco, 2011). Asimismo, se trata de un método estructurado de una población sobre determinados temas.

Diversos autores sostienen que la encuesta es la técnica que permite abarcar un elevado número de información y contribuir a la realización de investigaciones cualitativas, de carácter descriptivo, es decir, como marco diagnóstico.

Según Blanco (2011) dice que la encuesta es:

Uno de los métodos más apropiados para el logro de tal objetivo puesto que permite estudiar a muchas unidades de análisis en relativamente poco tiempo, y a un menor costo que si se utilizaran métodos cualitativos tales como las entrevistas en profundidad y/o antropológicas.

Por último, destacar, que al ser un instrumento de recolección de datos y al ser estandarizado permite una mayor interpretación de datos y posterior evaluación.

Ubicación y tiempo

La ubicación espacial de los participantes no es exacta ya que al ser realizadas en la red, fenómeno estudiado en esta investigación y del cual recae cierta responsabilidad, no se puede medir la ubicación exacta debido al estar conectados a una red inalámbrica. También influye el tiempo empleado en la realización de la encuesta. Al ser una encuesta de 18 preguntas, esto posibilita la realización de la misma en cualquier momento del día y en cualquier lugar, ya que no es necesario realizarla en un ordenador y se puede hacer en un minuto en el propio teléfono móvil. Esto era muy importante para la investigación, ya que se pretendía que los participantes mantuvieran un feedback positivo con la propia y la contestaran con honestidad. Por lo contrario, si se tratase de una encuesta compuesta por muchas preguntas los resultados podrían ser otros.

g) Análisis y discusión.

Esta investigación tiene como finalidad detectar la vulnerabilidad que posee una muestra de la población de Relleu, frente a los posibles ataques en el ciberespacio. El método empleado en esta investigación es cuantitativo, por lo que se extraen datos a través de encuestas. Los participantes son un total de 161 y de forma anónima.

En esta investigación, también se han extraído otros datos, es decir, otros ítems. Los cuales han sido: la marca temporal de la realización de la encuesta, el sexo y la edad de los participantes. La marca temporal de realización se centra en el mes de noviembre. Por otro lado, el resto de ítems serán explicados en profundidad a continuación.

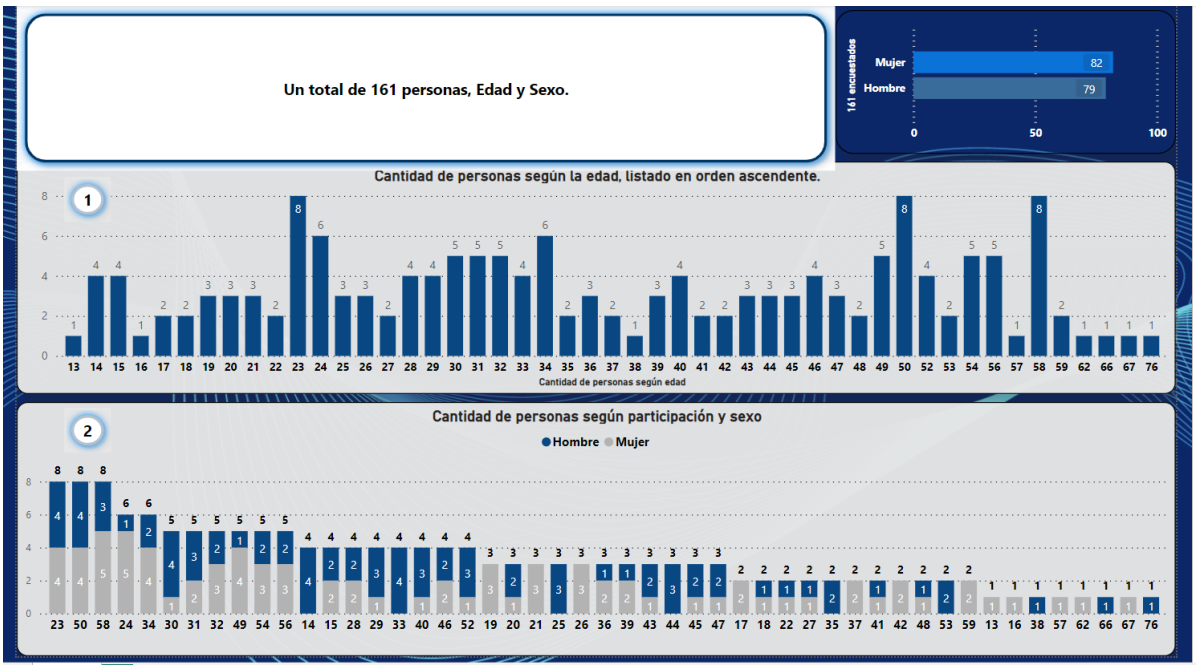
Por último, cabe destacar que una vez realizada la encuesta y observar la situación de manera global, se lleva a cabo un análisis de la situación objeto de estudio. Por ello, la información extraída más relevante para esta investigación, se centra en las siguientes dimensiones:

- Sexo de los participantes
- Edad más destacada
- Red más utilizada
- Uso de los medios de comunicación
- Conocimientos e inteligencia informática
- Responsabilidad y seguridad en la red

Estas dimensiones, se centran en los objetivos específicos elaborados y por lo tanto, son los que verifican si las posibles hipótesis se aproximan a la realidad o no.

A continuación, se expone un análisis de cada una de las preguntas generadas en la entrevista junto a unas gráficas realizadas en Power BI, para una mayor comprensión mediante una muestra más específica de los resultados.

Preguntas 1 y 2: Sexo y edad de los encuestados.

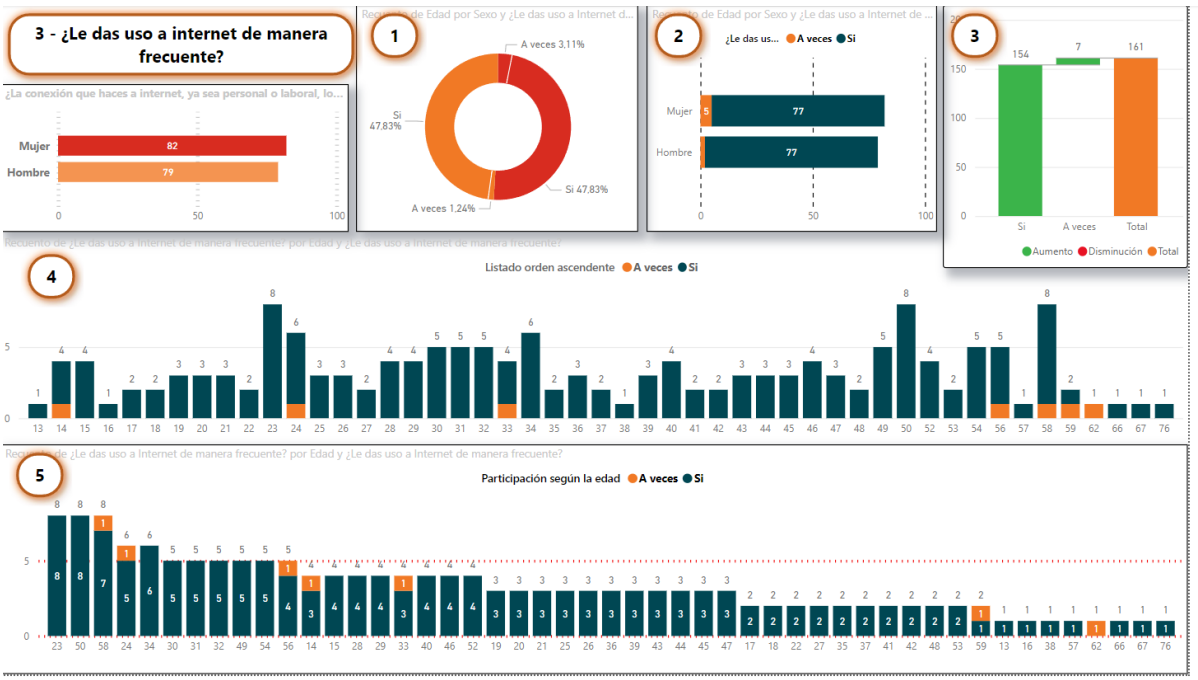


Gráfica 2 : Fuente primaria

Estas gráficas recogen las preguntas 1 y 2, en las cuales se puede observar que han sido un total de 161 participantes, siendo 82 mujeres con una edad mínima de 13 y una edad máxima de 67 años. Los hombres son un total de 79, con una edad mínima de 14 y una edad máxima de 76 años. En la segunda gráfica (2.2) se observa una distribución por edad relativamente equilibrada solo unas pocas columnas son ya sea de solo mujeres (19, 26, 17, 37 y 59, sin contar las individuales) o solo hombres (14, 33, 25, 44, 35 y 53).

(*En los listados de excel, figuran 162 participantes, se anula la fila 35, por no tener la información requerida para el estudio de la encuesta).*

Pregunta 3: ¿Ejerces el uso de Internet de manera frecuente? Sí/ No/ A veces



Gráfica 3: Fuente primaria

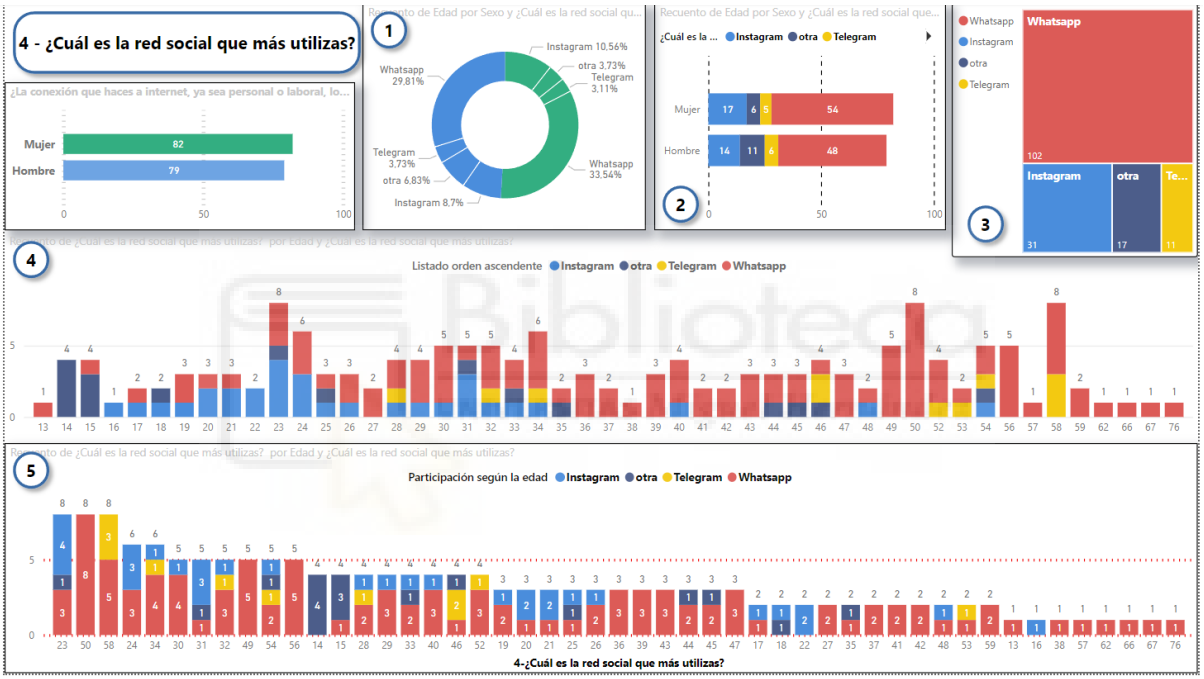
Esta gráfica recoge la información necesaria para conocer con que frecuencia los ciudadanos de Relleu dan uso al internet, saber de qué forma se implican las personas, conocer su rango de edad y su implicación según su edad y sexo. Además, de conocer el porcentaje de las personas que sí dan uso de manera frecuente, las que no hacen uso frecuente y las personas que lo utilizan de manera esporádica.

También, se observa que han respondido a la pregunta un total de 161 personas, por lo que, la participación fue total. Siendo 82 mujeres y los 79 restantes hombres. Según el contenido de la encuesta, las mujeres están en un rango de edad de 13 a 67 años, siendo una niña de 13 años como la menor y una señora de 67 como la mayor entre las mujeres. Los hombres encuestados, se encuentran en un rango de edad de 14 a 76, siendo un niño de 14 años el menor de los hombres y un señor de 76 el mayor de los hombres que han participado en la encuesta.

Se observa que la participación ha sido igual tanto en las mujeres, como en los hombres, con una votación igualada de 77 hombres y 77 mujeres con un porcentaje cada grupo de 47,83% (g3.1 y g3.2), siendo el total de los encuestados del 95,66% (g3.3) que tienen claro que usan con frecuencia internet. Por otro lado, se observa un porcentaje mucho más reducido de las personas que emplean el uso de una manera esporádica de internet, siendo este de un 4,34% entre ambos sexos. Siendo 3,11% mujeres y 1,24% hombres (g3.1).

Este resultado da a conocer que un porcentaje muy alto de ciudadanos de esta población navegan constantemente en internet. Teniendo en cuenta este porcentaje, al relacionarlo con las otras encuestas, se puede observar que tan expuestos o no, están a los posibles ataques que deambulan constantemente por el mundo virtual. En las gráficas 3.4 y 3.5 se observa que la mayoría del grupo que afirma no usar con frecuencia el internet está entre los 56 a 62 años.

Pregunta 4: ¿Cuál es la red social que más utilizas?. Whatsapp, Instagram, Telegram, Otras.



Gráfica 4: Fuente primaria

La información que se extrae mediante estas gráficas, es el conocimiento sobre cuáles son las redes sociales más utilizadas por los ciudadanos de Relleu. Asi como, conocer el porcentaje de cada una de ellas, la cantidad exacta de las personas según el sexo que utilizan cada red social y saber el número total saber de personas que utilizan cada una de las redes sociales teniendo en cuenta las edades. Además, se perciben los rangos de edad donde existe mayor o menor participación en las diferentes redes sociales.

Los resultados obtenidos en la gráfica 4, a rasgos generales son: la participación de 82 mujeres de diferentes edades y la participación de 79 hombres de diferentes edades.

Por un lado, en la categoría de las mujeres se observa un porcentaje un poco más alto en el uso de la red social más utilizada, pero los dos grupos coinciden en que la red social más utilizada es ***Whatsapp***, siendo las mujeres un 33,54% y los hombres un 3,37% menos, o sea, con un 29,81% (g4.1). Por lo que, ambos sexos se decantan por la red social ***Whatsapp*** como primera red con más uso. La segunda red social más opcionada por los dos grupos es ***Instagram***. Se observa al grupo de mujeres de este estudio, formando parte de un 10,56% y el grupo de hombres con un poco menos, es decir, un 8,7%. En el caso de la tercera red social propuesta por la encuesta, las mujeres escogieron la opción de ***otras***, con un 3,73%, pero los hombres en esta ocasión han calificado como tercera opción la red social ***Telegram*** con un 3,73%, justo el mismo porcentaje que las mujeres pero diferente red social. Por último y cuarta opción, las mujeres han seleccionado a la red social Telegram con un 3,11% y los hombres han dejado como cuarta opción ***otras***, con un 6,83%.

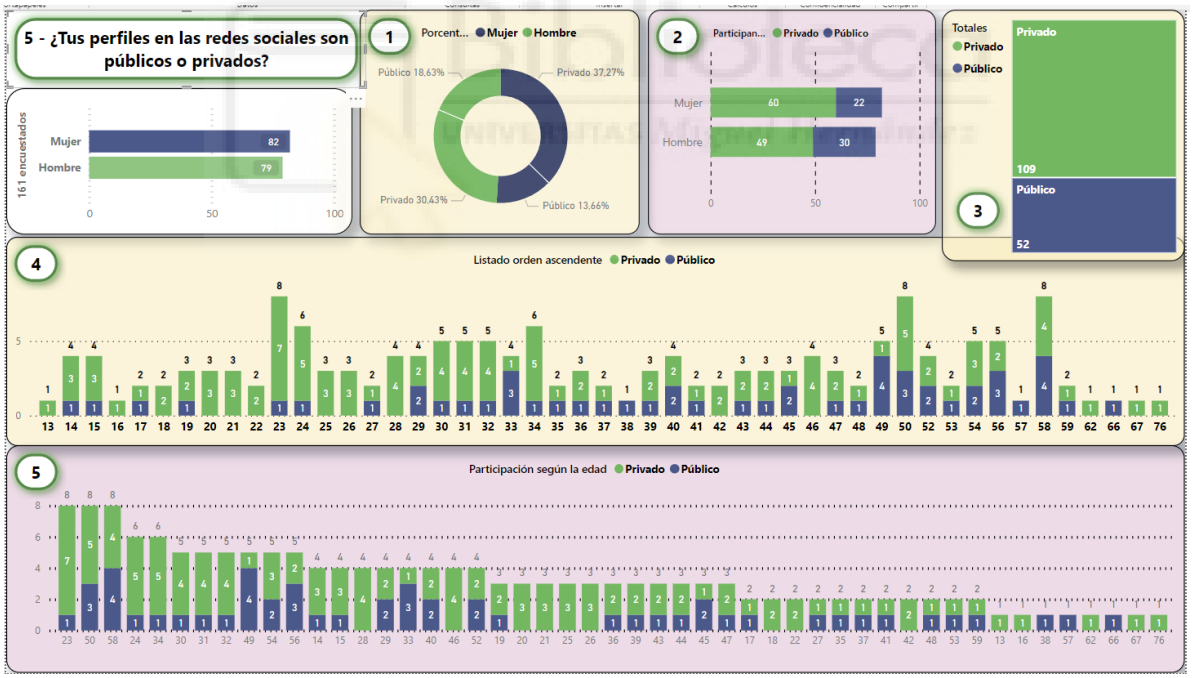
En general, los datos proporcionados por las personas que participaron en la elección de cada una de estas redes sociales, no poseen cifras con grandes diferencias en ninguno de los grupos. Por ejemplo, en el caso de la red social ***Whatsapp*** que ha sido la de mayor elección, la diferencia entre estos dos grupos de personas, se limita únicamente a 6 personas de diferencia, en el grupo de las mujeres. Una cantidad no muy relativa que no ocasiona desajustes o ninguna brecha entre ambos grupos. En el caso de **Instagram**, ocurre como en el anterior, son las mujeres las que reciben más cifras que los hombres, siendo 17 mujeres y 14 hombres. La siguiente opción, **Telegram**, recibe la participación de 6 hombres y 5 mujeres. Por último, aparece seleccionado por los participantes la opción de **otras redes sociales**, esta fue elegida por 11 hombres frente a 6 mujeres. Con estos resultados podemos observar que los hombres tienen una inclinación más llamativa hacia otras redes sociales, ya que en las más seleccionadas, las mujeres son las que dan datos más elevados, de manera general. Además, también se evidencia debido a la última opción de otras redes sociales, ya que han sido los hombres los participantes que más la han seleccionado. Por lo que, de manera global los hombres emplean tiempo en diferentes redes sociales que no se han tenido en cuenta para esta investigación.

Siguiendo con los marcadores en total, sin tener en cuenta el sexo, únicamente centrandonos en el número de los participantes, se observa que la red social **Whatsapp,** supera el 50% del total de los encuestados, llegando a un 63,35%, es decir, han seleccionado esta opción 102 encuestados. Por otro lado, **Instagram** recibe un 19,26%, siendo esta cifra un total de 31 encuestados, datos visibles en la Gráfica 4.3.

En el listado ascendente, gráfica 4,4 y 4.5, se observa qué zonas predominan más una red social u otra. Asimismo, la red social **Whatsapp**, se observa a lo largo de todo el listado, con diferencia en la zona de los 14 a los 25 años, donde hay un poco menos de participación. Asimismo, la red social que se visualiza con más participación es Instagram, sin embargo, ese protagonismo va disminuyendo hasta casi desaparecer entre las personas de 35 a 76 años de edad. Otra figura destacable de estas gráficas con listado ascendente, es la inclinación de los hombres hacia otras redes sociales, hecho ya mencionado Además, es destacable esta opción por jóvenes de 14 y 15 años.

Añadir, que la edad es un factor importante para esta gráfica, ya que se observa que según la franja de edad en la que se encuentren los participantes, emplearán el uso de una red social u otra.

Pregunta 5: ¿Los perfiles o cuentas que utilizas en redes sociales son de carácter privado o público? Privado/ Público



Gráfica 5: Fuente primaria.

Esta gráfica, nos muestra si las redes sociales que poseen los participantes de la investigación, tienen las redes sociales con un perfil público o privado y el porcentaje que aporta cada grupo a la encuesta, es decir, hombres y mujeres. Además, de conocer la

participación de ambos sexos en las opciones público o privado, o la participación total, según la edad y los rangos de edad según las dos opciones visibles.

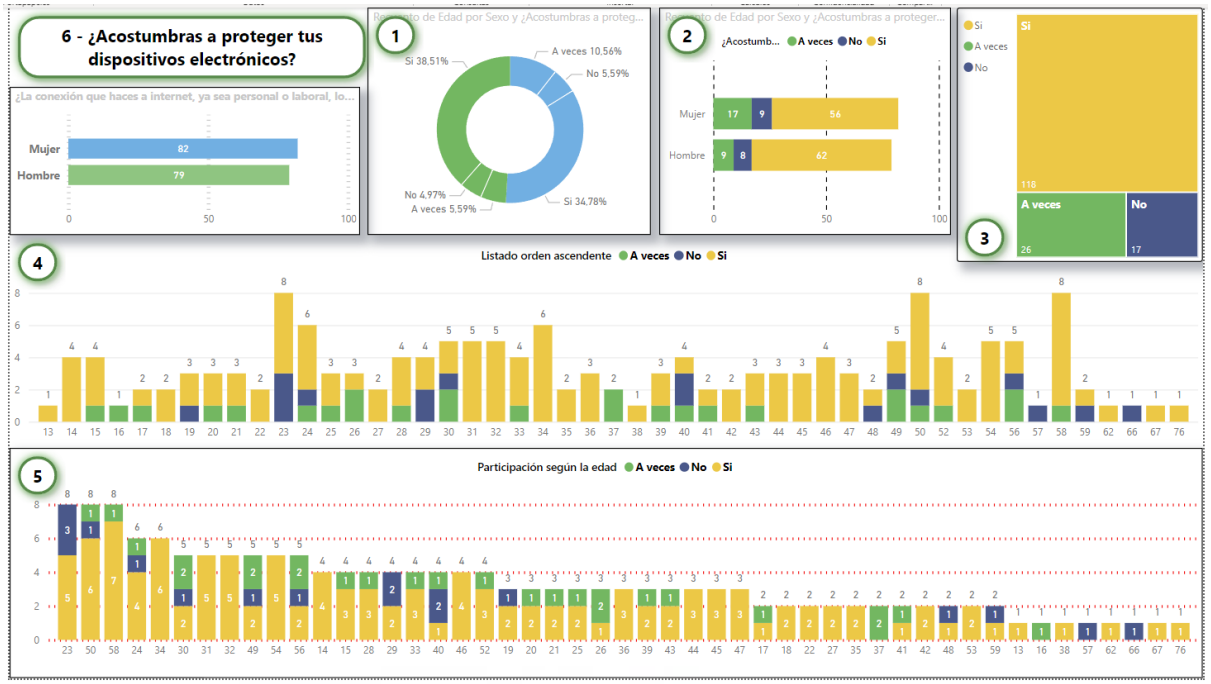
La participación de la encuesta es la misma que en las anteriores gráficas, 82 mujeres y 79 hombres, para un total de 161 participantes.

En esta ocasión, se tiene un porcentaje (g5.1) total de participación de las mujeres del 50,93%, con un desglose de 37.27% para las mujeres que han escogido tener sus redes sociales privadas y un 13,66% para las mujeres que consideran que sus redes sociales sean públicas.

En en caso de los hombres, la participación a tener las redes sociales privadas, es de un 30,43%, aproximadamente un 7% menos que las mujeres, es decir, 11 personas menos que el grupo de las mujeres. Con esos valores, se percibe que el grupo de las mujeres se preocupan más por la privacidad de sus redes sociales que los hombres. En general, la participación total, observable en la gráfica 5.3 es de un 67,7%,es decir , 109 personas que consideran como mejor opción, tener sus redes sociales privadas, ante un 32,29% (52 personas), que optaron por la opción de tener sus redes sociales públicas.

El listado ascendente, gráfica 5.4, nos permite ver desglosado la totalidad del listado, y datos como, que de los 49 años a los 58 años hay más personas que han optado por tener las redes sociales públicas. Por otro lado, el listado de participación por edad (g5.5), muestra una participación un poco más dispersa, especialmente en las redes sociales públicas. De los 13 años a los 28 años, son un total de 16 columnas, las cuales son formadas por 51 personas, y únicamente 7 personas han seleccionado la opción de redes sociales públicas. Este hecho, nos muestra que los jóvenes de 13 a 28 años, se preocupan más por la seguridad y privacidad de sus redes sociales.

Pregunta 6: ¿Acostumbras a proteger tus dispositivos electrónicos? Sí/No/ A veces



Gráfica 6: Fuente primaria.

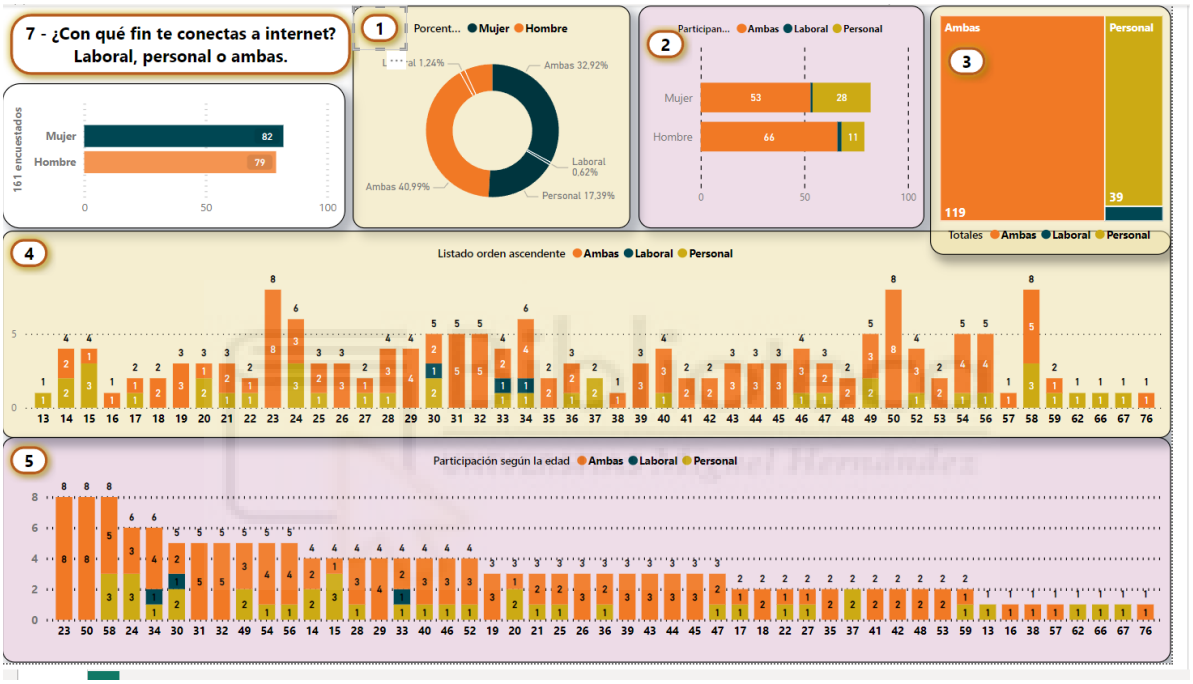
Con la pregunta generada en la encuesta, se quiere descubrir si las personas protegen o no sus dispositivos electrónicos, hecho que se puede observar en las gráficas, ya que , estas recogen toda la información necesaria. Asimismo, estas gráficas muestran que grupo de personas están seguras y consideran correcto o necesario proteger sus dispositivos electrónicos, y también, observar el porcentaje de personas que no lo consideran tan necesario y su decisión se encuentra más intermitente. Además, se ve el rango de edad en el que se encuentra la persona y que franja de edad es más cuidadosa con sus dispositivos electrónicos y quienes menos.

Centrándonos, en los datos específicos de la gráfica 6.1 y 6.2, se observa en el grupo de mujeres que 56 de ellas, es decir, el 34,78% acostumbran a proteger sus dispositivos electrónicos. Por otro lado, en el grupo de los hombres, es un porcentaje un poco más alto, el 38,51% para un total de 62 hombres. En este caso, 6 personas más que el grupo de las mujeres, sí acostumbran a proteger sus dispositivos electrónicos. Entre los dos grupos hacen un total de 118 personas (g6.3), es decir, un 73.29% de personas sí que acostumbran a proteger sus dispositivos electrónicos. Sin embargo, aparece un grupo de personas formado por 17 personas, es decir, el 10,56% las cuales no protegen sus dispositivos electrónicos. Por

último, se encuentran las personas que dicen proteger sus dispositivos de vez en cuando, estos forman un total de 26 personas entre ambos sexos, y equivalen a un 16,15%.

Añadir, que en la gráfica 6.4 se observan dos pequeños grupos de franjas de edad, uno de ellos es desde los 13 años hasta los 22 años, donde solo una persona de 19 años afirma no proteger su dispositivo, el otro grupo, se encuentra entre los 31 años hasta los 47 años, donde solo 2 personas de 40 años no protegen sus dispositivos.

Pregunta 7: ¿Con qué fin te conectas a internet? Laboral/ Personal/ Ambas



Gráfica 7: Fuente primaria.

Desconocer el riesgo al que se podría estar expuesto por no conocer los peligros en la red, ya es mucho, pero exponer también información laboral podría ser mucho peor, de ahí surge la elaboración de dicha pregunta.

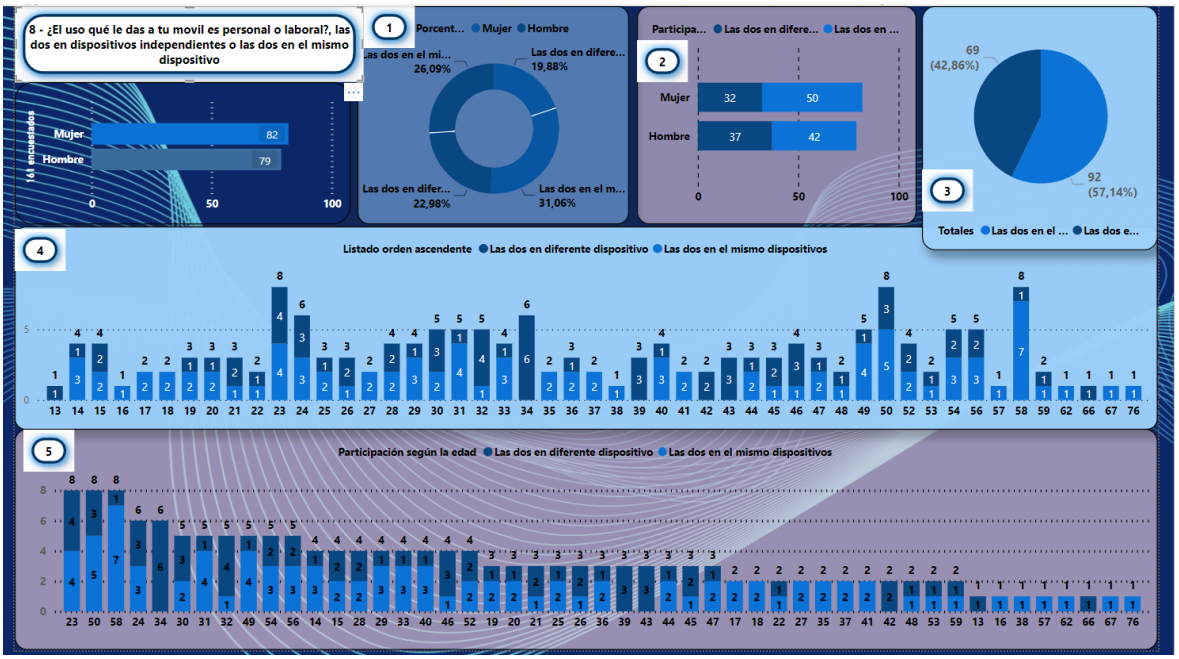
Esta gráfica, da a conocer los porcentajes y cantidad de personas que interactúan entre lo laboral y lo personal con un mismo dispositivo, del mismo modo, muestra el porcentaje y las personas que interactúan en estas dos modalidades, cada una en su respectivo dispositivo. Además, de mostrar los datos por rango de edad y por diferentes sexos de las personas que utilizan los dispositivos para conectarse a internet ya sea para lo personal, laboral o ambas cosas.

En las gráficas 7.1 y 7.2, en el grupo de hombres, un 40,99% han contestado que se conectan a internet para lo laboral y lo personal, es decir, ambas cosas en un mismo dispositivo. Siendo un total de 66 hombres. En el caso de las mujeres, el porcentaje al conectarse a internet para ambas cosas fue un poco más bajo, siendo de un 32,92% , lo que equivale a 53 mujeres. Además, únicamente el 1,24% de los hombres reconocen conectarse a internet solo por temas laborales, mientras que en el grupo de las mujeres afirman conectarse a internet para temas laborales un 0,62%. Por otro lado, se encuentra a un grupo de hombres de 11 personas, con un 6,83%, los cuales exponen que solo se conectan a internet por temas personales, mientras que el grupo de las mujeres, han contestado con un 17,39%, es decir, 28 mujeres, que solo se conectan a internet por temas personales, un porcentaje mucho más alto que el de los hombres

En datos generales, (g7.3) se observa que 119 personas se conectan a internet para ambas cosas, para lo personal y lo laboral, 39 personas afirman conectarse a internet solo para temas personales y una cifra mucho más reducida, de 3 personas se conectan solo para temas laborales.

Referente al rango de edad (g7.4 y 7.5), se observa que las personas que se conectan a internet para ambas cosas y para lo personal, no es un rango puntual, es un rango muy disperso sin tener en cuenta a los de 13, 14 y 15 años, edades en las que los jóvenes aún no poseen un puesto de trabajo y se puede considerar normal, pero para las personas que han contestado que solo se conectan a internet para temas laborales, el rango de edad, oscila entre los 30 y 35 años.

Pregunta 8: ¿El uso que le das a tu móvil es personal o laboral? Personal/ Laboral/ Las dos en dispositivos independientes/ Las dos en el mismo dispositivo



Gráfica 8: Fuente primaria.

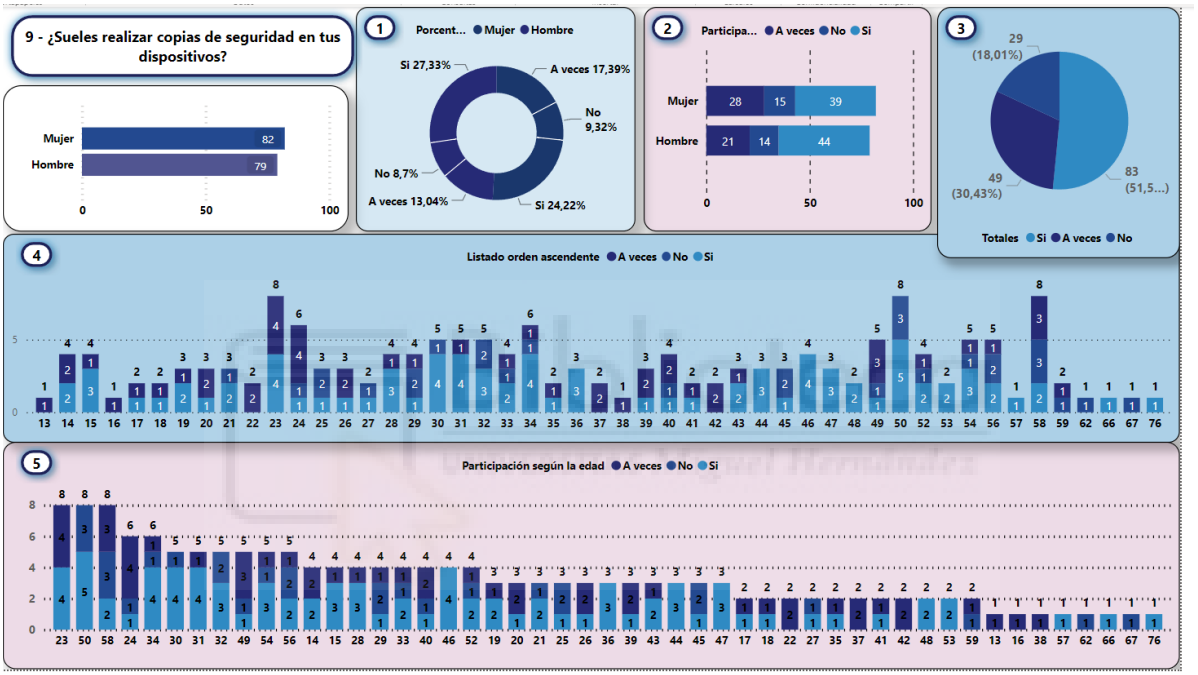
Teniendo en cuenta la anterior gráfica, se observa que los hombres se conectan para lo laboral, y laboral y personal un total de 42,23% (la suma de lo laboral y ambas cosas), es decir, un total de 68 hombres. Del mismo modo, la respuesta de esos 68 hombres es importante para analizar esta gráfica.

En la gráfica 8.2 se visualiza que solo 37 hombres tienen la precaución de conectarse a internet desde dispositivos independientes,es decir, un dispositivo para lo laboral y otro dispositivo para lo personal. Mientras que, 42 hombres lo hacen todo desde el mismo dispositivo. Por lo que, sólo 37 de esos 68 hombres, tienen la precaución de no mezclar lo laboral con lo personal. Asimismo, esa diferencia de 31 hombres estaría incluida entre los 42 hombres de la gráfica 8. Por lo que, en el caso de un hackeo o ataque virtual, estarían colocando en peligro no solo lo personal si no también lo laboral, por utilizar el mismo dispositivo para las dos cosas.

En el caso de las mujeres varía un poco el resultado final, ya que las mujeres en la gráfica anterior, la suma entre ambas cosas y lo laboral es del 33,54%, es decir, un total de 54 mujeres, de las cuales solo 32 mujeres confirman utilizar un dispositivo para lo laboral y otro diferente para lo personal. Esto deja una cifra de 50 (g8.2) mujeres, a las que les es indiferente utilizar el mismo dispositivo para lo personal y laboral, y en caso de un hackeo se verían perjudicados las dos vías como en el caso de los hombres.

Por último, haciendo mención a la edad, en las gráficas 8.3 y 8.4, no existe un rango de edad que predomine en ninguno de los dos grupos, lo que sí se observa es la falta de precaución por parte de las 92 personas (incluido los dos perfiles) al combinar estas dos prácticas en un mismo dispositivo, teniendo en cuenta que el ámbito laboral podría ser de información delicada y puede afectar a la empresa en la que trabajan si les llegaran a hackear el dispositivo.

Pregunta 9: ¿Sueles realizar copias de seguridad en tus dispositivos? Sí/ No/A veces



Gráfica 9: Fuente primaria.

Con esta pregunta se pretende conocer qué tan responsables y/o cuidadosos son los habitantes de Relleu con la seguridad de la información de sus dispositivos electrónicos.

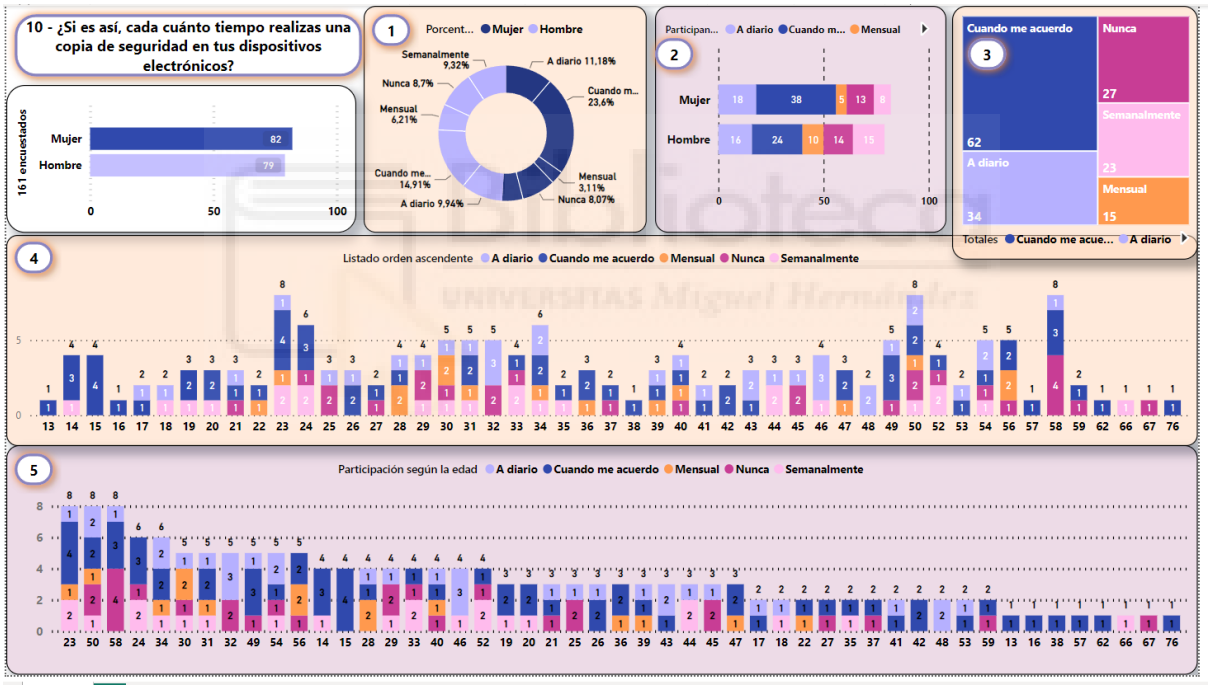
En esta gráfica se observa que un porcentaje muy alto reconoce no realizar copias de seguridad a sus dispositivos electrónicos (g 9.1, 9.2, 9.3). Hecho perjudicial y negativo para la persona si sufriera un hackeo en sus dispositivos electrónicos, ya que para solucionarlo, uno de los principales pasos que tendría que realizar sería borrar todo lo que tenga en él, perjudicando a cualquiera de los ámbitos (personal o laboral) por la pérdida de los datos.

Según las gráficas extraídas de la investigación, se observa que un 18,02% (entre ambos sexos) no realizan copias de seguridad, lo cual equivale a 29 personas. Por otro lado, encontramos a un 30,43%, los cuales confirman realizar copias de seguridad "a veces". La

suma de estas dos opiniones equivalen a un 48,45% (78 personas), casi el 50 % de todos los encuestados, una cifra muy alta teniendo en cuenta que después de un hackeo a uno de los dispositivos, es una de las mejores opciones para recuperar casi el 100% de la información digital perdida con el hackeo.

En conclusión, se visualiza que los valores de esta encuesta no varían mucho entre los dos grupos, del mismo modo, que la respuesta de no realizar copias de seguridad por rango de edad.

Pregunta 10: Si es así, ¿Cada cuánto tiempo realizas una copia de seguridad en tus dispositivos electrónicos? A diario/ Semanalmente/Mensualmente/ Anualmente/ Cuando me acuerdo.



Gráfica 10: Fuente primaria.

En la anterior gráfica, se ha observado la participación del total de los encuestados y se ha tenido en cuenta el porcentaje de personas que si realizan copia de seguridad, para la realización de esta gráfica, número 10. En esta ocasión, se observa la información de los porcentajes y cantidad de personas que hacen las copias de seguridad, además, de cada cuánto tiempo la hacen. Del mismo modo, también los que no realizan copias de seguridad.

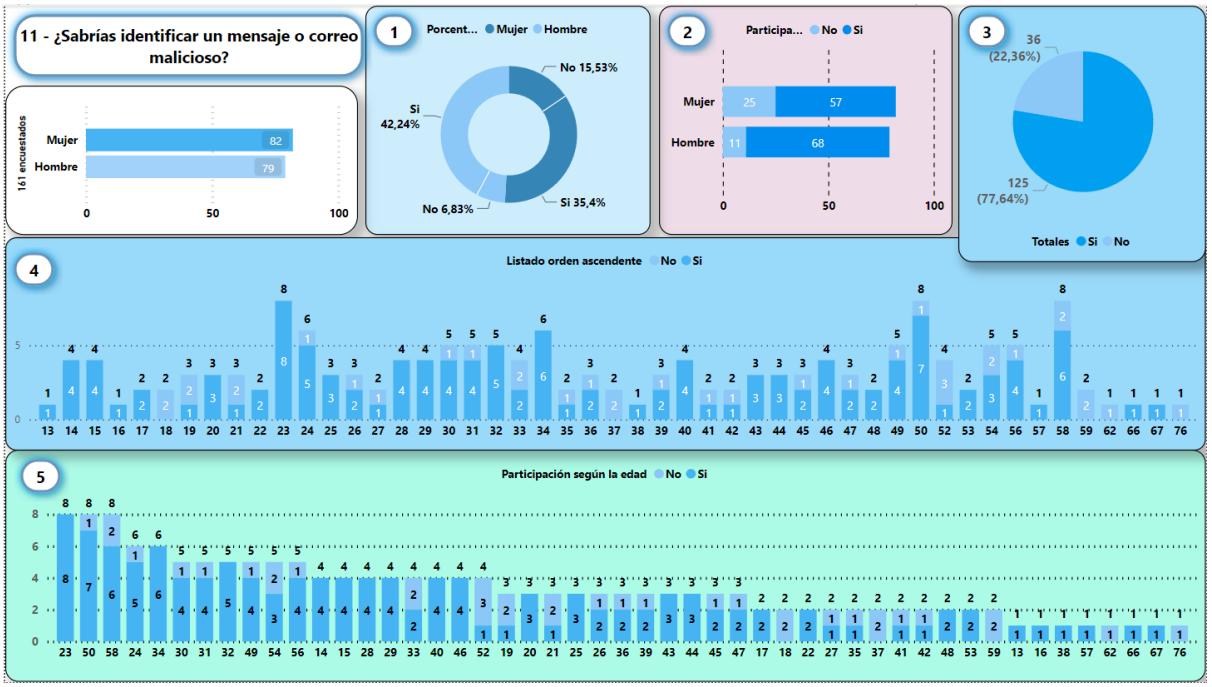
En la gráfica 10.1 y 10.2, el 40,38% (65 hombres), afirman hacer copias de seguridad, mientras que el 8,7% dicen nunca hacer copias de seguridad, coincide un 100% con la gráfica N 9 en el caso de los hombres.

A diferencia de la gráfica anterior, en la gráfica N 10, y con la pregunta expuesta, se pretende saber cada cuánto tiempo se hacen esas copias de seguridad, a una distancia próxima entre copias de seguridad, supondrá un mayor control de la información. Asimismo, solo el 9,94% (16 hombres) están haciendo copias de seguridad a diario, lo cual garantiza que si en algún momento sus dispositivos son hackeados, la información que se pueda perder es mínima porque tiene copia guardada del día anterior, por lo que, solo tendrían que resetear el dispositivo y configurar con la copia del día anterior.

De forma similar, ocurre con el grupo de las mujeres, nunca guardan copia de seguridad el 8,07% (13 mujeres), el resto 37,89% has contestado sí guardar copia de seguridad. Sin embargo, únicamente el 11,18% (18 mujeres) guardan copias de seguridad a diario.

En total, (g10.3) son 34 personas entre los dos grupos los que guardan copias de seguridad a diario, frente a 27 personas que nunca guardan copias de seguridad. Añadir, que 62 personas guardan copias cuando se acuerdan, el 38,51%. Es una cifra alta y según el listado y participación (g10.4 y 10.5), se observa que no hay un rango en concreto al cual se les pueda adjudicar estos valores, es una participación muy dispersa.

Pregunta 11: ¿Sabrías identificar un mensaje o correo malicioso? Sí / No



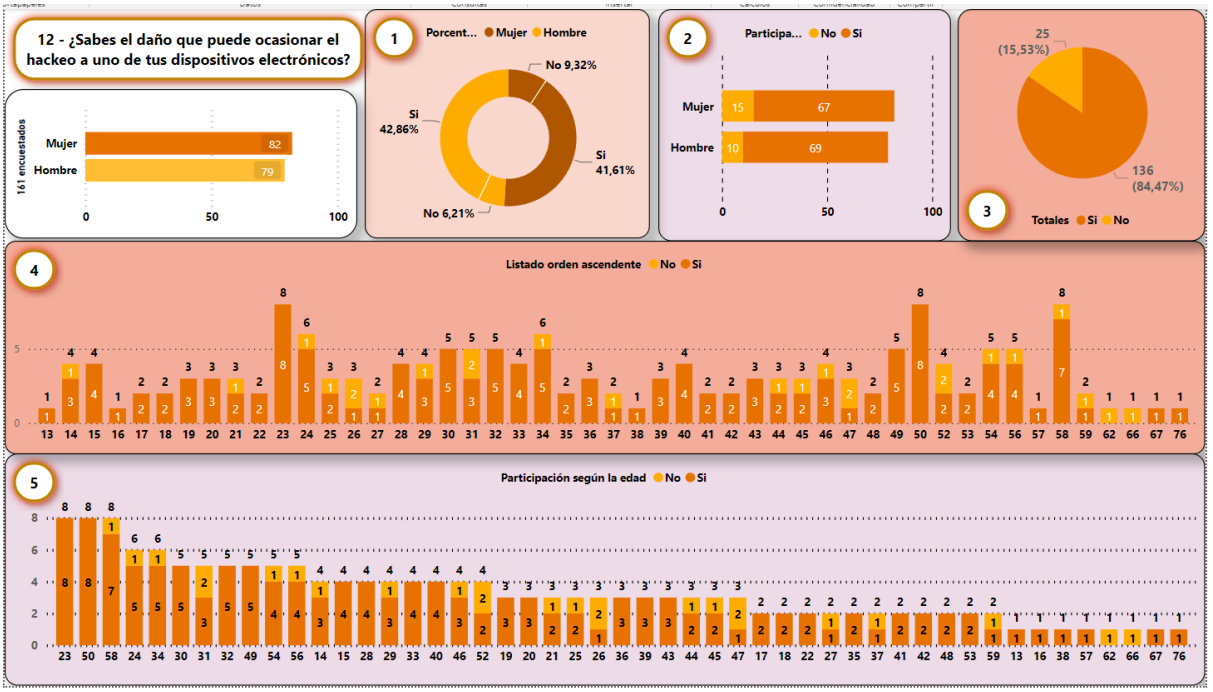
Gráfica 11: Fuente primaria

Esta gráfica nos muestra qué tan preparados están los habitantes de Relleu en el momento de un posible hackeo.

Según la misma, la participación es de 161 personas de las cuales el 77,64%, es decir, 125 personas, (g11.1 y g11.2) dicen reconocer un posible intento de hackeo a sus dispositivos, contra un 22,36%, 36 personas, que no sabrían identificarlo. Sin embargo, al observar los grupos por separado, se puede decir que los hombres con un 42,24% reconocen mejor un ataque virtual que las mujeres con un 35,4%.

Por último, en los listado por edad (g11.4) se observa dos pequeños grupos, de los 23 a 32 años y de los 43 a 50 años, los cuales lo tienen claro a la hora de reconocer un posible ataque virtual. La mayor participación está en las edades de 23, 50 y 58 (24 personas), de las cuales solo 3 personas dicen no reconocer un mensaje o correo malicioso (g11.5).

Pregunta 12: ¿Sabes el daño que puede ocasionar el hackeo a uno de tus dispositivos electrónicos? Sí/ No.



Gráfica 12: Fuente primaria

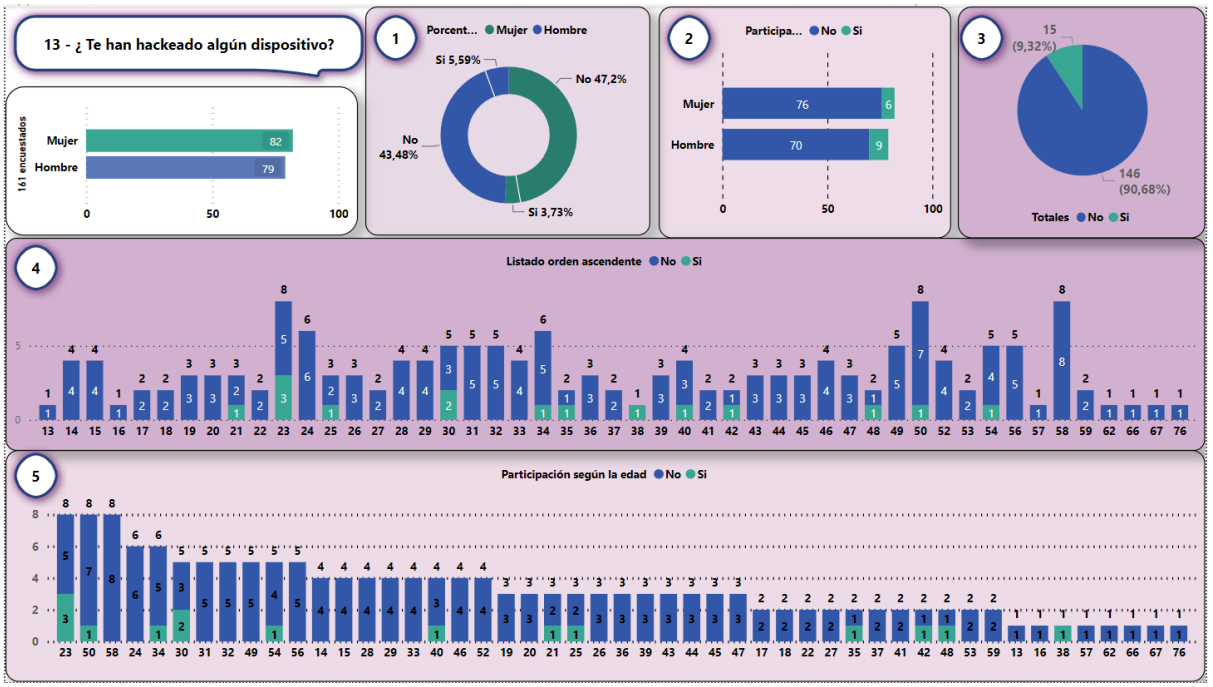
Con la muestra de estas gráficas se pretende descubrir el conocimiento que la población de Relleu tiene sobre los daños ocasionados por un hackeo informático. Asimismo, da a conocer el porcentaje y la cantidad de personas según su edad y sexo, que confirman saber el daño que les puede ocasionar un hackeo a sus dispositivos.

En la encuesta participaron 161 encuestados, como se ha ido mencionando durante este análisis, 82 mujeres y 79 hombres. El 42,86%, 69 hombres, han contestado saber el daño que les puede ocasionar el hackeo a sus dispositivos electrónicos (gráficas 12.1 y 12.2). Siendo un porcentaje de 6,21% los hombres que desconocen las repercusiones de un ataque informático.

Por otro lado, en el grupo de las mujeres se presenta un 41,61% ,67 mujeres dicen que son conocedoras de los daños de un posible hackeo, frente a un 9,32% que lo desconocen. En los dos grupos se observa dato elevado, por lo que la gran mayoría son conscientes del problema, específicamente 136 personas, es decir, el 84,47% .

Por último, mencionar que en los listados por edad y participación no se observa ningún grupo que destaque más que otro ni datos resultantes (gráficas 12.4 y 12.5).

Pregunta 13: ¿Te han hackeado algún dispositivo? Sí / No



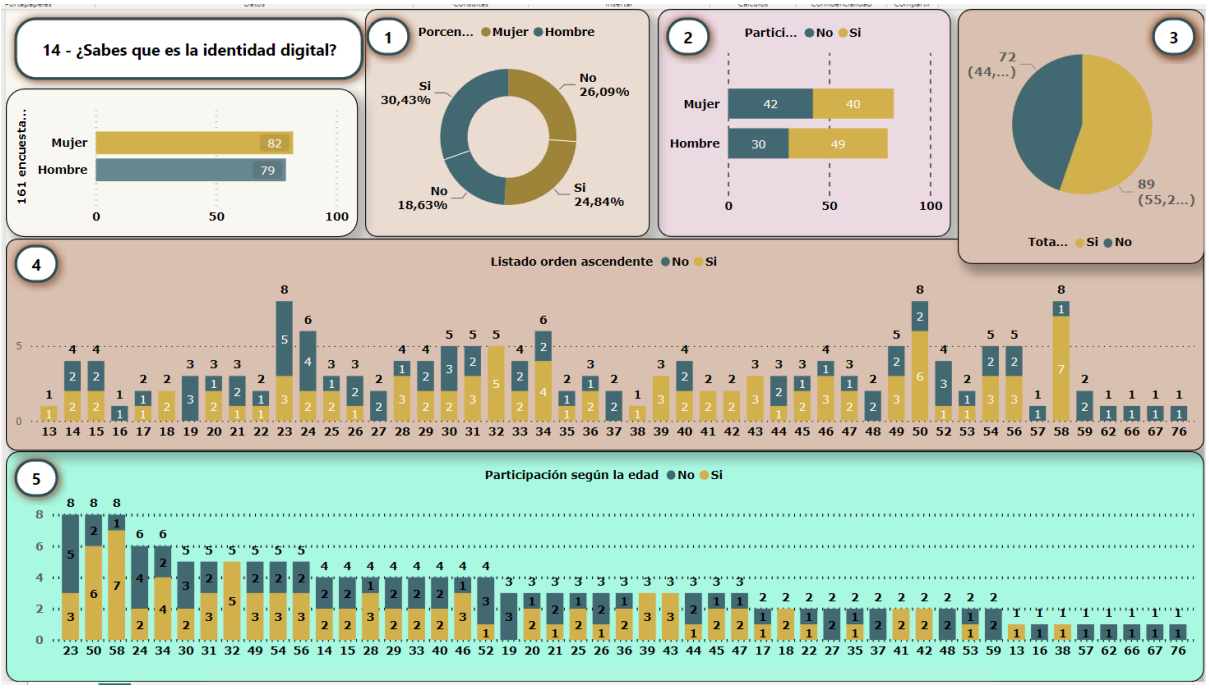
Gráfica 13: Fuente primaria

Esta gráfica, muestra la pregunta de si les han hackeado algún dispositivo alguna vez (g13.1). Sin embargo, solo un 5,59% de los hombres y un 3,73% de las mujeres reconocen que les han hackeado algún dispositivo. Por lo que, los datos observables muestran que solo el 9,32% ha sufrido algún ataque, frente al 90,68%, los cuales han contestado que no han sido hackeados. Teniendo en cuenta estos valores y observando las dos anteriores gráficas, se podría decir que el porcentaje es similar, en la gráfica número 11, el 22,36% no identifican un posible hackeo, en la gráfica número 12 el 15,53% no saben el daño que les podría ocasionar un hackeo a alguno de sus dispositivos y en la gráfica número 13 sólo el 9,32% ha sido hackeado.

Teniendo en cuenta los datos mencionados anteriormente, se observa que los habitantes de Relleu si distinguen un ataque virtual. El porcentaje de personas que no han sido hackeados es alto, un 90,68% , es decir, 146 personas.

En los listado por edad y participación (g13.4 y 13.5), se observa que las personas que han sido hackeadas están ubicadas entre los 21 y 25 años, otro de los sectores se encuentra entre los 34 a los 42 (g13.4). Por último, aparecen rasgos individuales como el de 30, 48, 50 y 54 años. También se observan zonas muy marcadas que no han sido hackeadas como son de los 13 a los 20 años y de los 56 a los 76 años, o sea, que se podría decir que no es cuestión de edad (g13.5).

Pregunta 14: ¿Sabes que es la identidad digital? Sí/ No

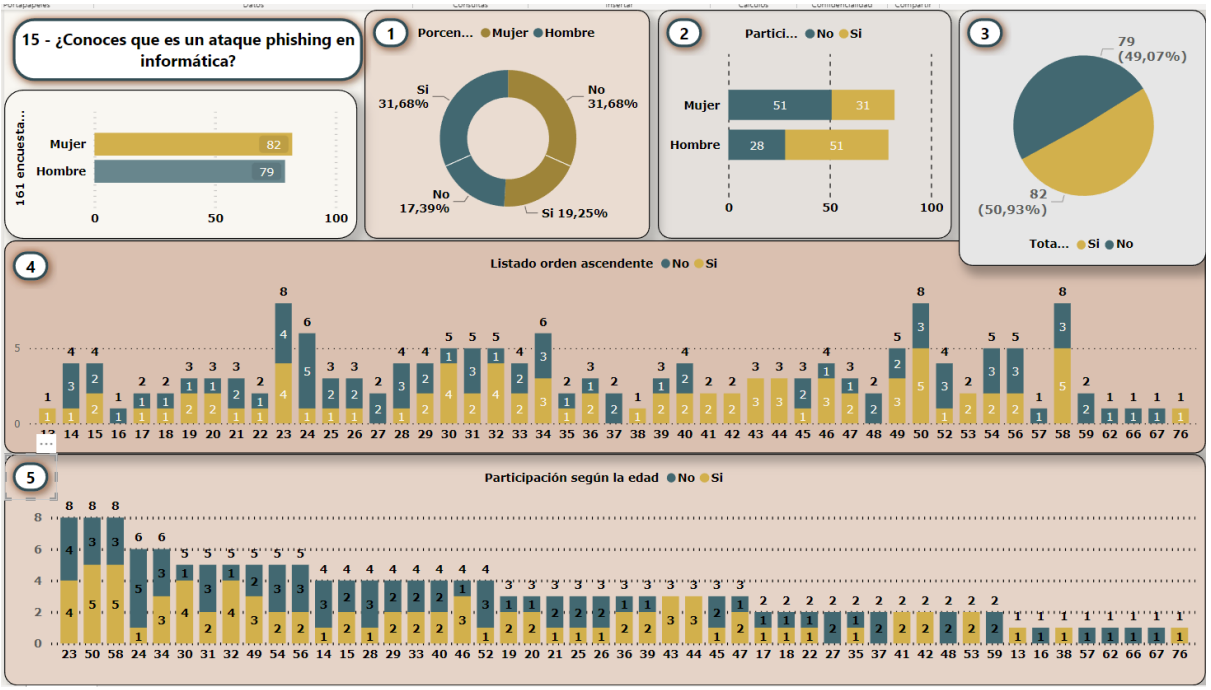


Gráfica 14: Fuente primaria

En esta gráfica, se da a conocer que conocimiento tiene la población de Relleu sobre la Identidad Digital. Según la participación de los hombres encuestados (gráficas 14.1, 14.2 y 14.3), el 30,43%, 49 hombres, saben lo que es la identidad digital mientras que casi el 20% no lo conocen (30 hombres). En el grupo de las mujeres el porcentaje es un poco más equilibrado entre las que lo saben y las que no lo saben, el 24,84% (40 mujeres), dicen saber que es la identidad digital, el 26,09% (42 mujeres), dicen no saberlo. En total, entre ambos sexos son 72 personas y reciben un porcentaje de 44,72%, las que no saben lo que es la inteligencia digital, mientras que 89 personas que equivalen al 55,28% han contestado que sí saben que es la identidad digital.

En relación con las gráficas del listado por edad y participación gráficas (14.4 y 14.5), se observa que de los 14 a los 27 años, su porcentaje en desconocer que es la identidad digital es un poco más bajo, por otro lado, en el rango de los 59 años en adelante, han contestado no conocer la identidad digital, en esta ocasión sí se puede decir que hay más desconocimiento en ciertos rango de edad.

Pregunta 15: ¿Conoces que es un ataque phishing en informática? Sí /No

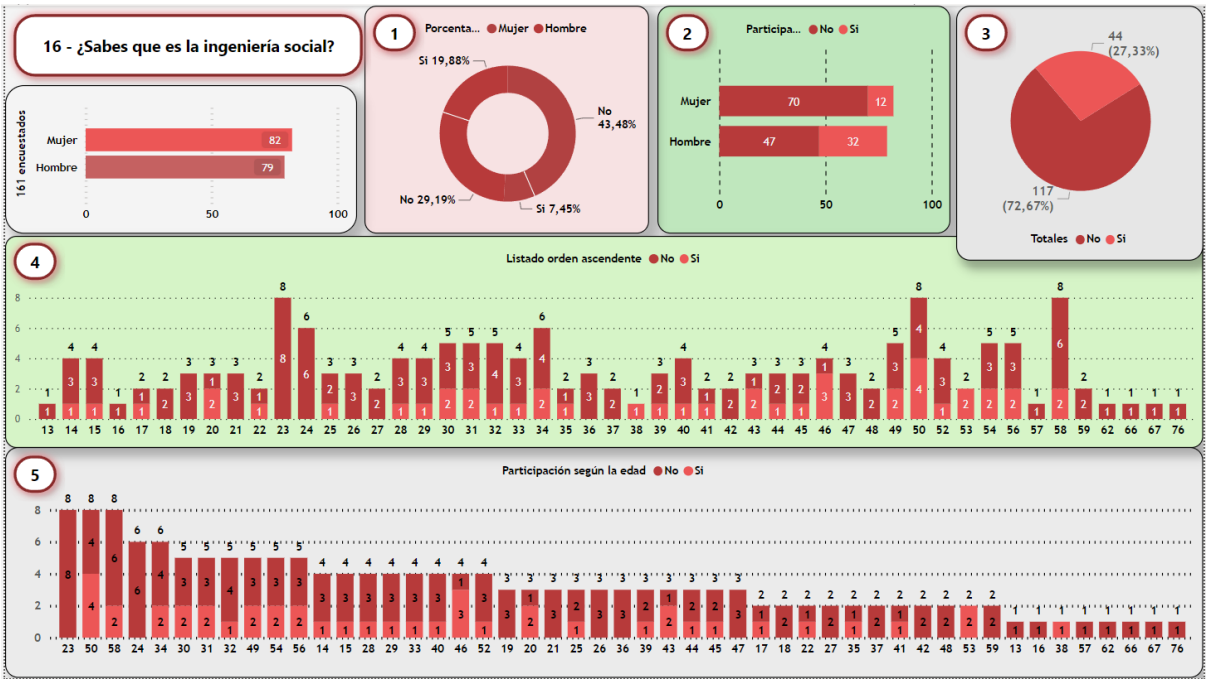


Gráfica 15: Fuente primaria

Esta gráfica también se centra en el conocimiento de una terminología dentro de la seguridad informativa, como es un ataque phishing. En esta ocasión se observa una gran diferencia entre las encuestas de las mujeres y la de los hombres, gráficas 15.1 y 15.2. En las respuestas de las mujeres, el porcentaje que no saben lo que es un ataque phishing es más alto que las que lo saben, siendo las mujeres que lo saben un total de 31 mujeres, (19,25%), mientras las que no lo saben son un total de 51 mujeres (31,68%). Por otro lado, en el grupo de los hombres el porcentaje es totalmente contrario, el 31,68% (51 hombres) si saben lo que es un ataque phishing y el 17,39% (28 hombres) no lo saben.

Por último, en el listado por edad (g15.4) y el listado por participación (g15.5), se observan pequeños grupos con una inclinación muy concreta. Por ejemplo, el grupo de los 59 años en adelante, tienen claro saber que es un ataque phishing, además del grupo de los 24 a los 29 años, estos dos grupos tiene un porcentaje alto en saber que es un ataque phishing. A diferencia del grupo en el rango de edad de 38 a 47 años, posee un porcentaje alto de no saber que es un ataque phishing. A pesar de que, en la gráfica total (g15.3) se observa muy igualada con las personas que han elegido la opción de saber que es un ataque phishing y las que no lo saben. Muestra que un 50,93% (82 personas) saben lo que es un ataque phishing y un 49,07% (79 personas) no saben lo que es un ataque Phishing.

Pregunta 16: ¿Sabes que es la ingeniería social? Sí / No



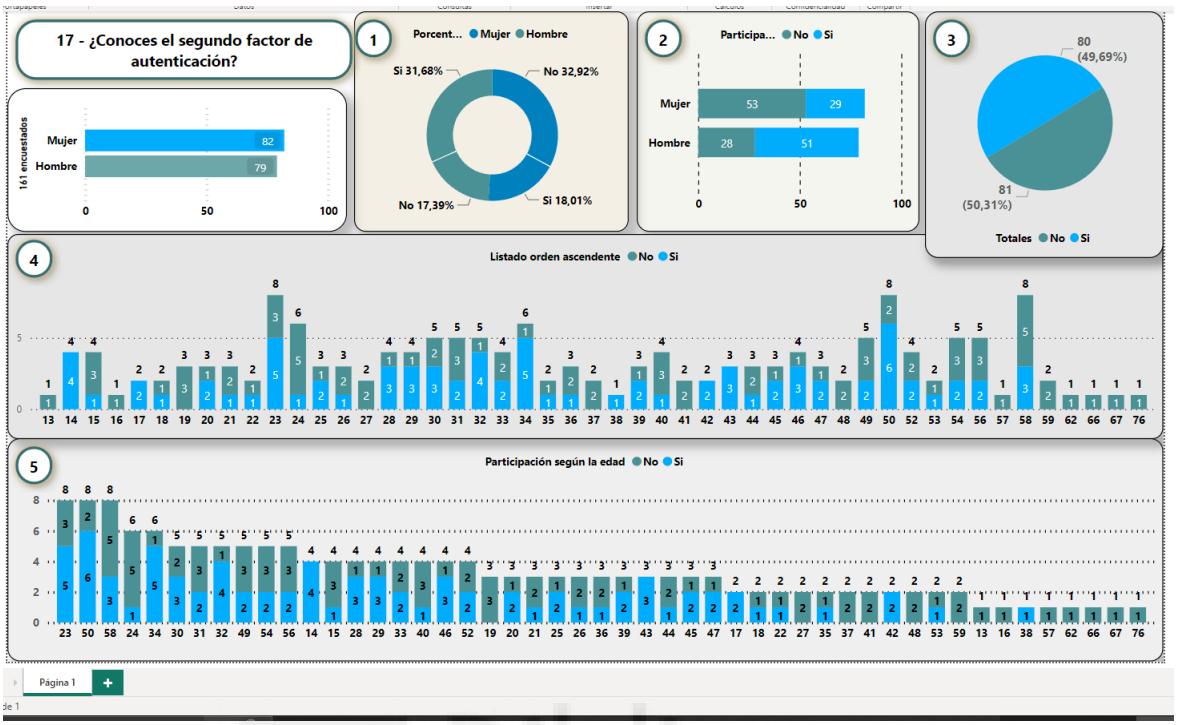
Gráfica 16: Fuente primaria

La gráfica 16 dará a conocer si los habitantes de Relleu conocen el significado de Ingeniería Social y en que les beneficia o afecta.

Solo un 27,33% (44 personas), datos observables en las gráficas 16.1 y 16.2 de todos los encuestados, saben lo que es la ingeniería social, mientras que el 72,67% (117 personas) restante, no saben lo que es la ingeniería social. De los hombres sólo un 19,88% (32 hombres) han contestado saber lo que es la ingeniería social, el otro 29,19% (47 hombres) lo desconocen. Por otro lado, en el grupo de las mujeres los porcentajes varían mucho con relación a los porcentajes de los hombres, solo 12 mujeres (7,45%) saben lo que es la ingeniería social, el resto de mujeres 70 (43,48%) han manifestado no saber qué es la ingeniería social.

Al observar el listado por edad y la participación (gráficas 16.4 y 16.5), las personas de 57 años en adelante han manifestado no conocer la ingeniería social, su representación es mínima en la encuesta al igual que algunas columnas individuales.

Pregunta 17: ¿Conoces el doble factor de autenticación?



Gráfica 17: Fuente primaria

El uso del doble factor de seguridad es de gran apoyo para la protección de la información, en esta ocasión se sabrá el uso que le dan los habitantes de Relleu por medio de esta encuesta.

Inicialmente (gráficas 17.1 y 17.2) se obtiene la información de los hombres que protegen sus dispositivos electrónicos con el doble factor de seguridad. El 31,68% (51 hombres) confirman mediante la encuesta conocer el factor de doble seguridad, los 28 hombres restantes 17,39% dicen no saber qué es el doble factor de seguridad.

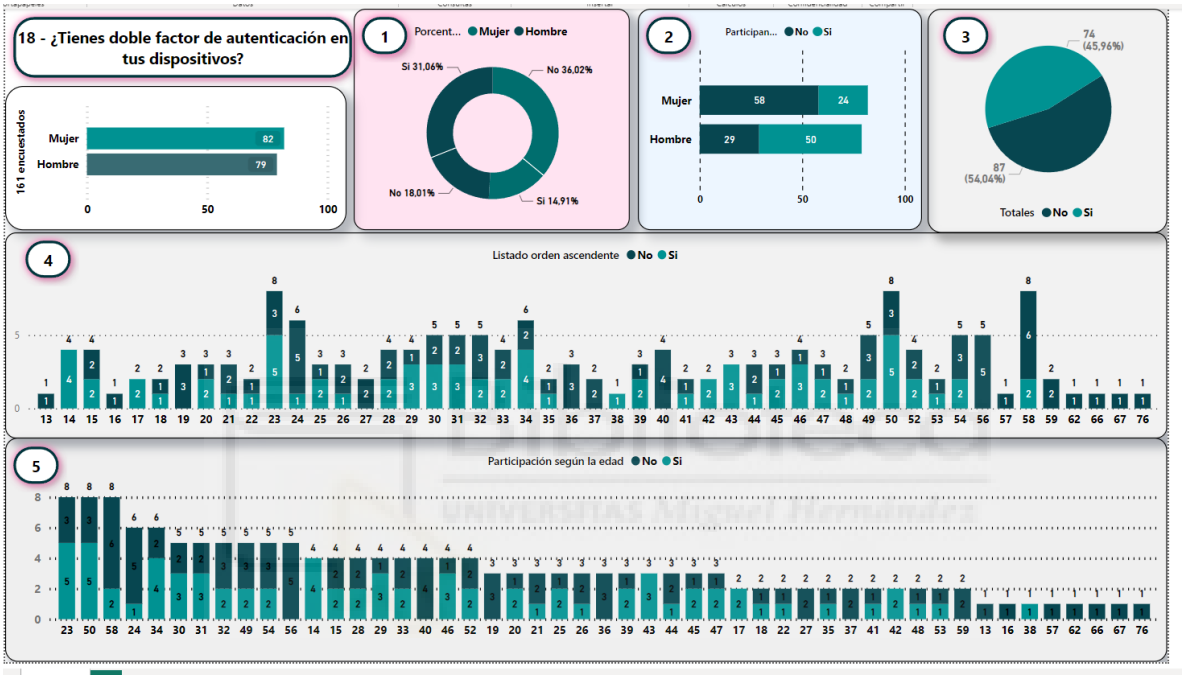
En el caso del grupo de las mujeres, es algo totalmente opuesto: el 32,92% (53 mujeres) han contestado que no conocen el doble factor de seguridad a diferencia del 18,01% (29 mujeres) que dicen si conocerlo, los porcentajes son muy diferentes frente al de los hombres. Teniendo en cuenta la gráfica de totales (g17.3) se observa que han seleccionado la opción **sí el** 49,69% (80 personas) y a **no** el 50,31% (81 personas). Por lo que, las cifras son muy igualadas pero si desglosamos esa gráfica en totales, se pueden observar que los porcentajes son diferentes.

Por último, en la gráfica 17.4 se puede observar que de los 59 años en adelante muestran que no conocen el doble factor de seguridad. Además, en la gráfica 17.5 de la

columna 23 años (primera columna) hasta la columna de los 22 años se observa más equilibrio en las respuestas, siendo:

No	62 personas
Sí	75 personas

Pregunta: 18: ¿Tienes un segundo factor de autenticación en tus dispositivos?



Gráfica 18: Fuente primaria

En esta última gráfica, se observa que personas conocen el doble factor de seguridad, y sobre todo si lo emplean. Siguiendo el orden de la gráfica 8, en la 18.1 expone unos porcentajes muy parecidos a la gráfica 17.1. Por otro lado, en cuanto a diferencia por sexos, el porcentaje de los hombres que dicen usar el doble factor de seguridad en sus dispositivos es del 31,06% (50 hombres). Sin embargo, el grupo de las mujeres recibe un 14,91%, 24 mujeres, las cuales dicen tener en sus dispositivos el doble factor de seguridad. Volviendo al grupo de los hombres, existe un porcentaje que muestra no tener el doble factor de seguridad, siendo un 18,01%, mientras que las mujeres que tampoco emplean el doble factor es de un 36,02%, los cuales recogen a 58 mujeres. Los totales entre ambos sexos poseen unos porcentajes bastante parecidos, por lo que se puede percibir cierta igualdad.

Del mismo modo, que en la gráfica anterior (N17), deja claro que el género o sexo es destacable en ciertas cuestiones, ya que, aunque se observe en la gráfica 18.5 cifras parejas, cabe recordar que los hombres son el grupo que más emplea el doble factor de seguridad con un 31,06% ,frente a un 14,91% de las mujeres.

h) Conclusiones y propuestas.

La ciberseguridad debería ser una enseñanza a nivel global debido a la repercusión que genera, aún más en la época cibernética en la que coexistimos. La ciberseguridad es un seguro de vida en muchos aspectos, además de una herramienta esencial diseñada para proteger el entorno de la red, asegurando la integridad de la información. El entorno cibernético exige un compromiso continuo ante la evolución de las TIC.

Como se ha mencionado en la fundamentación teórica diferentes autores crean programas como: El *Programa Nacional de Reducción de Amenazas y Vulnerabilidades*, el cual intenta minimizar las amenazas y vulnerabilidades y el *Programa de Divulgación y Enseñanza sobre Seguridad del Ciberespacio*, debido a la necesidad de un desarrollo de prevención, es decir, realizar acciones proactivas. Asimismo, se quiere hacer hincapié en la necesidad de estas acciones y métodos de prevención y conseguir una mayor concienciación, no solo a nivel micro como puede ser el muestreo de esta investigación, sino a nivel macro, es decir, a un nivel nacional.

Tras la investigación a nivel teórico, la elaboración de una encuesta a través de ciertas hipótesis y el correspondiente análisis, podemos afirmar que sí existe cierta vulnerabilidad en la población frente a los ataques del ciberespacio, posiblemente por el desconocimiento de las consecuencias que pueden ser generadas.

Una vez analizado todos los datos y realizar esta investigación se puede concluir respecto a varios aspectos:

- Que las personas que se encuentran en una franja de edad entre los 15 y los 30 no son el grupo que más descuida sus dispositivos electrónicos. Como se puede comprobar en la encuesta en la que se centra la investigación no existe una franja de edad específica, ni centrada en los jóvenes, incluso en una de las cuestiones aparece que las personas entre 49 y los 58 utilizan sus redes sociales con perfiles públicos, lo cual genera tener menos control, seguridad y

privacidad en sus redes sociales, y por tanto, en sus dispositivos electrónicos. Añadir, que ni el sexo ni la edad ha sido un factor resaltante en esta investigación ya que, 77 hombres y 77 mujeres usan internet de manera frecuente. Asimismo, su uso se encuentra completamente igualado.

- Otra de las conclusiones a las que se ha llegado a través de este estudio, es que el avance de las nuevas tecnologías ha servido para informar a la población de diversos ataques en internet, incluso de un aprendizaje respecto terminologías importantes dentro de la seguridad cibernética. El 77,64% de los encuestados en este estudio, es decir, 125 personas de 161, sabría identificar un mensaje o un correo malicioso. Además, 136 personas son conocedoras del daño que puede ocasionar un hackeo o un ataque en sus dispositivos electrónicos. Se corrobora esta información extraída ya que el porcentaje de personas que han sido hackeadas no alcanza ni al 10%. Por otro lado, en cuanto al conocimiento de diferentes conceptos de la ciberseguridad existen unos más trabajados que otros. El concepto de identidad digital y el doble factor, está arraigado en la población de este estudio ya que más del 50% conocen el término identidad digital y casi el 50% el doble factor. Este último, se trata en rasgos generales, pero si se desglosa se observa que de esos casi 50%, el 31,68% que emplean el doble factor son hombres. Sin embargo, solo el 27,33%, es decir, 44 personas son conocedores de la ingeniería social, y del ataque phishing, existen 79 personas que lo desconocen.
- No existe un nivel total de desprotección en este municipio, pero sí destacable. Una vez extraídos los datos se observa que el 73,29% de personas sí que acostumbran a proteger sus dispositivos electrónicos. Sin embargo, aparece una pequeña línea que dejan sin protección. 119 personas se conectan a internet para la utilización del ámbito laboral y del personal, pero 92 de estos emplean el mismo dispositivo para ambos ámbitos. Esto quiere decir, que si presencian el ataque o un hackeo cibernético, no sólo están desprotegiendo uno de los ámbitos, sino que ambos quedarían contaminados. Pudiendo generar problemas frente a información delicada de la empresa o información personal.
- Otro aspecto importante a destacar sobre la desprotección de los ciudadanos de este estudio, es que, a pesar de manifestar que el 73,29% sí protege sus dispositivos, después se observa que un porcentaje alto reconoce no realizar

copias de seguridad, casi el 50%. Y sólo, 34 personas de la investigación las realizan diariamente.

- Por último, destacar la red social más utilizada de este muestreo. Se trata de Whatsapp, siendo sus cifras de un 63,35%, es decir 102 encuestados. Sin embargo, esta cifra está compuesta gran parte por mujeres, ya que los hombres se han inclinado más por la opción de otras redes sociales, por lo que, dedican más tiempo a otras redes que no son las expuestas en la encuesta: Whatsapp, Instagram o Telegram. Sin embargo, al pertenecer Whatsapp a más del 50% sería el principal medio para poner en marcha la ciberseguridad, mediante acciones preventivas o paliativas, para no poner en riesgo la privacidad de la persona, teniendo en cuenta toda la información que dicha aplicación puede dar a los piratas informáticos.

Para finalizar, una vez obtenidas las conclusiones de la propia investigación surgen varias recomendaciones en las que se podría intervenir desde la Seguridad Pública y Privada. Estas intervenciones son para mejorar el bienestar y calidad de vida de las personas que utilizan la red, prevenir posibles consecuencias o ayudarles a intervenir frente a amenazas. Las recomendaciones planteadas son las siguientes:

- Charlas de concienciación, en las que se exponen casos reales de amenazas de este país, y como llegaron a una extrema intimidación de la persona, o casos reales de empresas que lo han perdido todo a causa de no proteger sus dispositivos o software.
- Cursos de uso adecuado de las redes sociales. Fomentando desde el principio la privacidad y protección de ellas. Saber detectar amenazas, disfrazadas de spam, enlaces de fraude, etc. Además, de enseñarles el lado contrario de un mal uso, para que observen las consecuencias.
- Talleres para jóvenes y adultos sobre la educación en la red. Teniendo en cuenta que la Covid-19 ha dejado una serie de hábitos y el más destacado ha sido el uso masivo de los dispositivos electrónicos . En el que se ha dado pie al teletrabajo, exámenes online y un acceso desmedido de la población infantil, entre otros. Este uso poco habitual hasta entonces, ha hecho que prolifere de cierta forma la aceptación de las *cookies,* en las cuales se podría filtrar métodos de extracción de información, como puede ser el *phishing* o algún Malware. Asimismo, el propósito será evitar un uso descontrolado de los móviles u ordenadores, aspecto que da pie a un uso de las redes sociales con riesgo. Además, se centrarán en la privacidad y el buen uso.

- Fomentar la investigación a través de videos informativos sobre la problemática. Se recomendarán videos de *Youtube* o medio similar, accesibles para todo el mundo en el que se explica la importancia de proteger los dispositivos electrónicos y por lo tanto, sobre ciberseguridad.

i) Bibliografía.

Díaz, F. J., Venosa, P., Macia, N., Lanfranco, E. F., Sabolansky, A. J., Durante, M., ... & Pretto, J. (2021) Investigación en ciberseguridad en un año de pandemia. In *XXIII Workshop de Investigadores en Ciencias de la Computación (WICC 2021, Chilecito, La Rioja)*.

Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare*, *23*(3), 339-362.

Fernández, C. S. (2014). La vida privada en la sociedad digital. La exposición pública de los jóvenes en internet. *Aposta. Revista de Ciencias Sociales*, (61), 1-32.

Alvear Reinoso, F. X. (2019). *Análisis y diseño de una propuesta para mitigar ataques cibernéticos a correos electrónicos utilizando técnicas de hacking ético* (Bachelor's thesis).

Sebastián-Morillas, A., & Martínez-Navarro, G. (2013). La influencia de las nuevas tecnologías: videojuegos, redes sociales e internet, en los consumidores seniors en España.

Giones-Valls, A., & Serrat-Brustenga, M. (2010). La gestión de la identidad digital: una nueva habilidad informacional y digital.

Cardona, P. A. N., & Restrepo, S. C. (2018). Técnica de protección para credenciales de autenticación en redes sociales y correo electrónico ante ataques phishing. *Publicaciones e Investigación*, *12*(2), 23-34.

Blanco, C. (2011). *Encuesta y estadística: modelos de investigación cuantitativa en Ciencias Sociales y Comunicación*. Brujas.

Ruiz Díaz, Joaquín. 2016. "Ciberamenazas: ¿el terrorismo del futuro?",http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Subijana Zunzunegui, Ignacio José. 2008. "Elciberterrorismo: Una perspectiva legal y judicial". Eguzkilore, 22 (2008): 169-187.http://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf

Departamento de Defensa de los Estados Unidos. (2016). Dictionary of Military and Associated Terms. Recuperado de: https://fas.org/irp/doddir/dod/jp1_02.pdf.

Urueña Centeno, Francisco Javier. 2015. "Ciberataques, la mayor amenaza actual", http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf.

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93.

Curtis E. Lemay Center. 2011. "Introduction to cyberspaceoperations", https://doctrine.af.mil/download.jsp?filename=3-12-D01-CYBER-Introduction.pdf.

Pita Fernández, S., & Pértegas Díaz, S. (2002). Investigación cuantitativa y cualitativa. *Cad aten primaria*, *9*, 76-78.

del Centro Criptológico, S. D. C. (2020). La ciberseguridad y su relevancia en el Sector Público: El papel del Centro Criptológico Nacional. *Revista española de control externo*, *22*(64), 66-87.

Unión Internacional de Telecomunicaciones (UIT). (2010). Resolución 181. Recomendación UIT–T X.1205. *UIT*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Newmeyer, K., Cubeiro, E., & Sánchez, M. (2015). Ciberespacio, Ciberseguridad y Ciberguerra.

Unión Internacional de Telecomunicaciones (UIT). (2010). Resolución 181. Recomendación UIT–T X.1205. *UIT*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Sánchez Medero, G. (2012). Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del s. XXI.

Unión Internacional de Telecomunicaciones (UIT). (2010). Resolución 181. Recomendación UIT–T X.1205. *UIT*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Borghello, C. (2009). El arma infalible: la Ingeniería Social. *ESETLatinoamérica*.

Maroto, J. P. (2009). El ciberespionaje y la ciberseguridad. In *La violencia del siglo XXI. Nuevas dimensiones de la guerra* (pp. 45-76). Instituto Español de Estudios Estratégicos.

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y - ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93.

González, G. (2018). El legado tecnológico de la Segunda Guerra Mundial. *Revista Prisma Tecnológico, IX*, *1*, 39-41.

Bubukayr, M. A. S., & Almaiah, M. A. (2021, July). Cybersecurity concerns in smart-phones and applications: A survey. In *2021 International Conference on Information Technology (ICIT)* (pp. 725-731). IEEE.

Informe sobre la cibercriminalidad en España. (2021). Ministerio del Interior. Gobierno de España. https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/Informe-Cibercriminalidad-2021.pdf

Principales ciberamenazas en la UE. (2022, 29 agosto). European Council. https://www.consilium.europa.eu/es/infographics/cyber-threats-eu/

Internet Organised Crime Threat Assessment (IOCTA). (2021). Europol. https://www.europol.europa.eu/publications-events/main-reports/iocta-report

Aparici, R., & Osuna Acedo, S. (2013). La cultura de la participación. *Revista Mediterránea enComunicación, 4*(2), 137-148.doi:https://doi.org/10.14198/MEDCOM2013.4.2.07

Benavides, E., Fuertes, W., Sanchez, S., & Nuñez-Agurto, D. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia y Tecnología*, *13*(1), 97-104.

Alfonso Pagán, I. M. (2019). Sistema de autenticación robusto.

Policía Nacional . (12 de mayo de 2016). Boletín de análisis en Ciberseuridad NNA. Obtenido de https://caivirtual.policia.gov.co/sites/default/files/boletin_grooming03_0.pdf

"Guía sobre adolescencia y sexting: ¿qué es y cómo prevenirlo?", Instituto Nacional de Tecnologías de la Comunicación, Observatorio de la seguridad de la Información", febrero de 2011.Disponible en *http://www.educacion.navarra.es/portal/digitalAssets/49/49142_20110337.pdf*.

Sánchez, I. (2014). Protección de niños en la red: sexting, ciberbullying y pornografía infantil. *Universidad Nacional Autónoma de México*, 83-115

j) Anexos.

Preguntas encuesta:

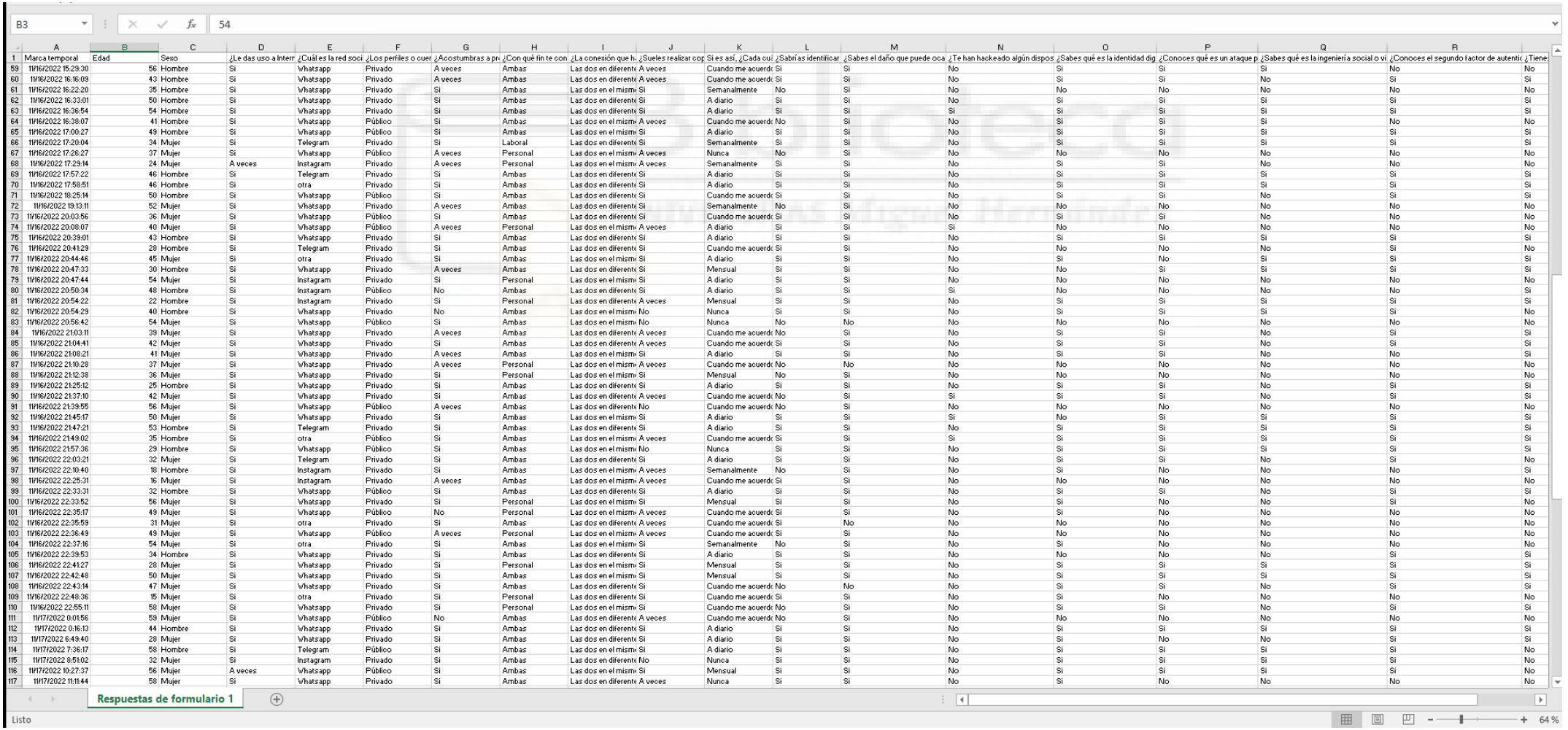
1. Edad:
2. Sexo: hombre/mujer /otro
3. ¿Ejerces el uso de Internet de manera frecuente? Sí/ No/ A veces/Casi nunca
4. ¿Cuál es la red social que más utilizas? (pregunta abierta)
5. ¿Los perfiles o cuentas que utilizas en redes sociales son de carácter privado o público? Privado/ Público
6. ¿Acostumbras a proteger tus dispositivos electrónicos? Sí/No
7. ¿Con qué fin te conectas a internet? Laboral/ Personal/ Ambas
8. ¿El uso que le das a tu móvil es personal o laboral? Personal/ Laboral/ Las dos en dispositivos independientes/ Las dos en el mismo dispositivo
9. ¿Sueles realizar copias de seguridad en tus dispositivos? Sí/ No/A veces/Casi nunca
10. Si es así, ¿Cada cuánto tiempo realizas una copia de seguridad en tus dispositivos electrónicos? A diario/ Semanalmente/Mensualmente/ Anualmente/ Cuando me acuerdo
11. ¿Sabrías identificar un mensaje o correo malicioso? Sí / No/ Tal vez
12. ¿Sabes el daño que puede ocasionar el jaqueo a uno de tus dispositivos electrónicos? Sí/ No /Sí, me ha ocurrido/ No, nunca me ha ocurrido
13. ¿Te han hackeado algún dispositivo? Sí / No
14. ¿Sabes que es la identidad digital? Sí/ No
15. ¿Conoces que es un ataque phishing en informática? Sí /No
16. ¿Sabes que es la ingeniería social? Sí / No
17. ¿Conoces el segundo factor de autenticación?
18. ¿Tienes un segundo factor de autenticación en tus dispositivos?

Datos extraídos encuesta:

B3 | 54

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
1	Marca temporal	Edad	Sexo	¿Le das uso a Internr	¿Cuál es la red soci	¿Los perfiles o cuer	¿Acostumbras a pr	¿Con qué fin te con	¿La conexión que h	¿Sueles realizar cop	Si es así, ¿Cada cuá	¿Sabrías identificar	¿Sabes el daño que puede oca	¿Te han hackeado algún dispos	¿Sabes qué es la identidad dig	¿Conoces qué es un ataque p	¿Sabes qué es la ingeniería social o vi	¿Conoces el segundo factor de autentic	¿Tiene
2	11/14/2022 17:57:30	47	Hombre	Si	Whatsapp	Público	Si	Personal	Las dos en el mism	Si	Mensual	Si	No	No	No	No	No	No	No
3	11/15/2022 4:42:48	54	Hombre	Si	Telegram	Público	Si	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	Si	Si	No	Si	Si	Si	Si	Si
4	11/15/2022 9:35:40	24	Mujer	Si	Instagram	Privado	Si	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	Si	No	No	No	No
5	11/15/2022 9:40:45	26	Mujer	Si	Whatsapp	Privado	A veces	Ambas	Las dos en diferente	Si	A diario	No	Si	No	No	No	No	No	No
6	11/15/2022 9:43:30	21	Mujer	Si	Instagram	Privado	Si	Ambas	Las dos en diferente	Si	Cuando me acuerdo	Si	Si	No	Si	Si	No	Si	Si
7	11/15/2022 9:43:55	19	Mujer	Si	Instagram	Público	No	Ambas	Las dos en el mism	Si	Cuando me acuerdo	No	Si	No	No	No	No	No	No
8	11/15/2022 9:44:26	31	Hombre	Si	Instagram	Privado	Si	Ambas	Las dos en el mism	Si	Mensual	Si	Si	No	Si	Si	Si	Si	Si
9	11/15/2022 9:49:25	46	Mujer	Si	Whatsapp	Privado	Si	Personal	Las dos en el mism	Si	A diario	Si	No	No	No	No	No	No	No
10	11/15/2022 9:49:47	58	Mujer	A veces	Whatsapp	Privado	A veces	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	No	No	No	No	No	No	No	No
11	11/15/2022 9:56:25	18	Mujer	Si	otra	Privado	Si	Ambas	Las dos en el mism	Si	A diario	No	Si	No	Si	Si	No	Si	No
12	11/15/2022 9:58:10	20	Mujer	Si	Whatsapp	Privado	A veces	Personal	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	No	Si	No	No	No
13	11/15/2022 10:07:24	34	Mujer	Si	Whatsapp	Público	Si	Personal	Las dos en diferente	Si	A diario	Si	Si	No	Si	No	No	No	No
14	11/15/2022 10:54:57	23	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	Si	No	No	No	Si	Si
15	11/15/2022 11:19:31	39	Mujer	Si	Whatsapp	Público	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	No	No	No	No
16	11/15/2022 11:57:38	26	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	No	No	Si	No	No	No	No
17	11/15/2022 12:00:46	23	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	Si	Semanalmente	Si	Si	No	No	No	No	Si	Si
18	11/15/2022 12:47:41	15	Mujer	Si	otra	Privado	Si	Personal	Las dos en diferente	Si	Cuando me acuerdo	Si	Si	No	No	No	No	No	Si
19	11/15/2022 13:58:50	23	Hombre	Si	otra	Privado	Si	Ambas	Las dos en diferente	A veces	Mensual	Si	Si	Si	Si	Si	No	Si	Si
20	11/15/2022 14:04:33	25	Hombre	Si	otra	Privado	Si	Personal	Las dos en el mism	No	Nunca	Si	No	Si	Si	No	No	No	Si
21	11/15/2022 14:07:36	31	Hombre	Si	Instagram	Privado	Si	Ambas	Las dos en el mism	Si	Semanalmente	Si	Si	No	Si	Si	Si	Si	Si
22	11/15/2022 14:28:37	25	Hombre	Si	Instagram	Privado	A veces	Ambas	Las dos en el mism	No	Nunca	Si	Si	No	No	No	Si	Si	No
23	11/15/2022 16:15:56	24	Mujer	Si	Whatsapp	Privado	No	Personal	Las dos en diferente	No	Nunca	Si	Si	No	No	No	No	No	No
24	11/15/2022 19:05:47	24	Mujer	Si	Instagram	Privado	Si	Personal	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	No	No	No	No	No
25	11/15/2022 22:13:30	24	Mujer	Si	Whatsapp	Público	Si	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	No	No	No	No	No	No	No	No
26	11/15/2022 23:30:24	17	Mujer	Si	Instagram	Privado	Si	Personal	Las dos en el mism	Si	A diario	Si	Si	No	No	Si	Si	Si	Si
27	11/16/2022 0:03:28	26	Mujer	Si	Instagram	Privado	A veces	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	Si	No	No	No	Si	No	Si	Si
28	11/16/2022 0:23:53	52	Hombre	Si	Whatsapp	Público	Si	Personal	Las dos en el mism	No	Nunca	No	No	No	No	No	No	No	No
29	11/16/2022 0:40:46	50	Hombre	Si	Whatsapp	Privado	A veces	Ambas	Las dos en el mism	No	Nunca	No	Si	No	No	No	No	No	No
30	11/16/2022 0:49:41	49	Mujer	Si	Whatsapp	Público	A veces	Ambas	Las dos en el mism	No	Nunca	No	Si	No	No	Si	No	No	No
31	11/16/2022 0:52:04	15	Hombre	Si	Whatsapp	Privado	A veces	Personal	Las dos en el mism	Si	Cuando me acuerdo	Si	Si	No	No	Si	No	No	No
32	11/16/2022 0:53:56	14	Hombre	Si	otra	Privado	Si	Personal	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	No	No	No	Si	Si
33	11/16/2022 0:54:34	20	Hombre	Si	Instagram	Privado	Si	Personal	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	Si	No	Si	Si	Si
34	11/16/2022 0:54:59	14	Hombre	Si	otra	Privado	Si	Personal	Las dos en diferente	Si	Cuando me acuerdo	Si	Si	No	Si	Si	No	Si	Si
35	11/16/2022 1:02:02	tu puta madre!!	Hombre	Si	otra	Público	Si	Ambas	Las dos en el mism	Si	Semanalmente	Si	No	No	No	No	Si	Si	Si
36	11/16/2022 1:10:40	50	Mujer	Si	Whatsapp	Privado	No	Ambas	Las dos en el mism	No	Nunca	Si	Si	No	Si	No	No	No	No
37	11/16/2022 1:22:37	19	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	No	Si	No	No	Si	No	No	No
38	11/16/2022 1:26:58	58	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	No	Nunca	Si	Si	No	Si	Si	Si	No	Si
39	11/16/2022 1:31:06	76	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	Si	Cuando me acuerdo	No	Si	No	No	No	No	No	No
40	11/16/2022 1:31:41	48	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	Si	A diario	Si	Si	No	No	No	No	No	No
41	11/16/2022 1:42:45	66	Hombre	Si	Whatsapp	Público	No	Personal	Las dos en diferente	Si	Semanalmente	Si	No	No	No	No	No	No	No
42	11/16/2022 3:20:21	33	Hombre	Si	otra	Público	Si	Ambas	Las dos en diferente	Si	Semanalmente	No	Si	No	No	No	No	No	No
43	11/16/2022 3:54:29	27	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	No	Nunca	No	No	No	No	No	No	No	No
44	11/16/2022 3:56:09	21	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	No	Si	No	No	No	No	No	No
45	11/16/2022 4:01:10	31	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	Si	Cuando me acuerdo	No	No	No	No	No	No	No	No
46	11/16/2022 4:10:25	31	Hombre	Si	Instagram	Público	Si	Ambas	Las dos en el mism	Si	A diario	Si	Si	No	Si	No	No	No	Si
47	11/16/2022 7:10:17	20	Hombre	Si	Instagram	Privado	Si	Ambas	Las dos en diferente	Si	Semanalmente	Si	Si	No	Si	Si	Si	Si	Si
48	11/16/2022 10:55:29	13	Mujer	Si	Whatsapp	Privado	Si	Personal	Las dos en diferente	A veces	Cuando me acuerdo	Si	Si	No	Si	Si	No	No	No
49	11/16/2022 10:56:27	14	Hombre	A veces	otra	Privado	Si	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	Si	No	No	Si	No
50	11/16/2022 12:57:03	29	Hombre	Si	Whatsapp	Privado	No	Ambas	Las dos en el mism	Si	A diario	Si	Si	No	No	No	No	Si	Si
51	11/16/2022 14:55:32	30	Mujer	Si	Instagram	Privado	Si	Personal	Las dos en el mism	Si	Semanalmente	No	Si	Si	No	No	No	No	No
52	11/16/2022 15:11:22	50	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en diferente	Si	Semanalmente	Si	Si	No	Si	Si	Si	Si	Si
53	11/16/2022 15:13:38	47	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	Si	Cuando me acuerdo	Si	Si	No	Si	Si	No	Si	Si
54	11/16/2022 15:16:30	30	Hombre	Si	Whatsapp	Público	No	Laboral	Las dos en el mism	Si	A diario	Si	Si	Si	No	Si	Si	Si	Si
55	11/16/2022 15:16:44	49	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	Si	Si	No	Si	Si	Si	Si	Si
56	11/16/2022 15:20:44	52	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en diferente	Si	Cuando me acuerdo	No	No	No	No	No	No	Si	Si
57	11/16/2022 15:23:47	46	Mujer	Si	Telegram	Privado	Si	Ambas	Las dos en diferente	Si	Semanalmente	Si	Si	No	Si	Si	Si	Si	Si
58	11/16/2022 15:28:19	53	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en el mism	Si	Cuando me acuerdo	Si	Si	No	No	Si	Si	No	No
59	11/16/2022 15:29:30	56	Hombre	Si	Whatsapp	Privado	A veces	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	Si	Si	No	Si	Si	Si	No	No
60	11/16/2022 16:16:09	43	Hombre	Si	Whatsapp	Privado	A veces	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	Si	Si	No	Si	No	Si	Si	Si

Respuestas de formulario 1



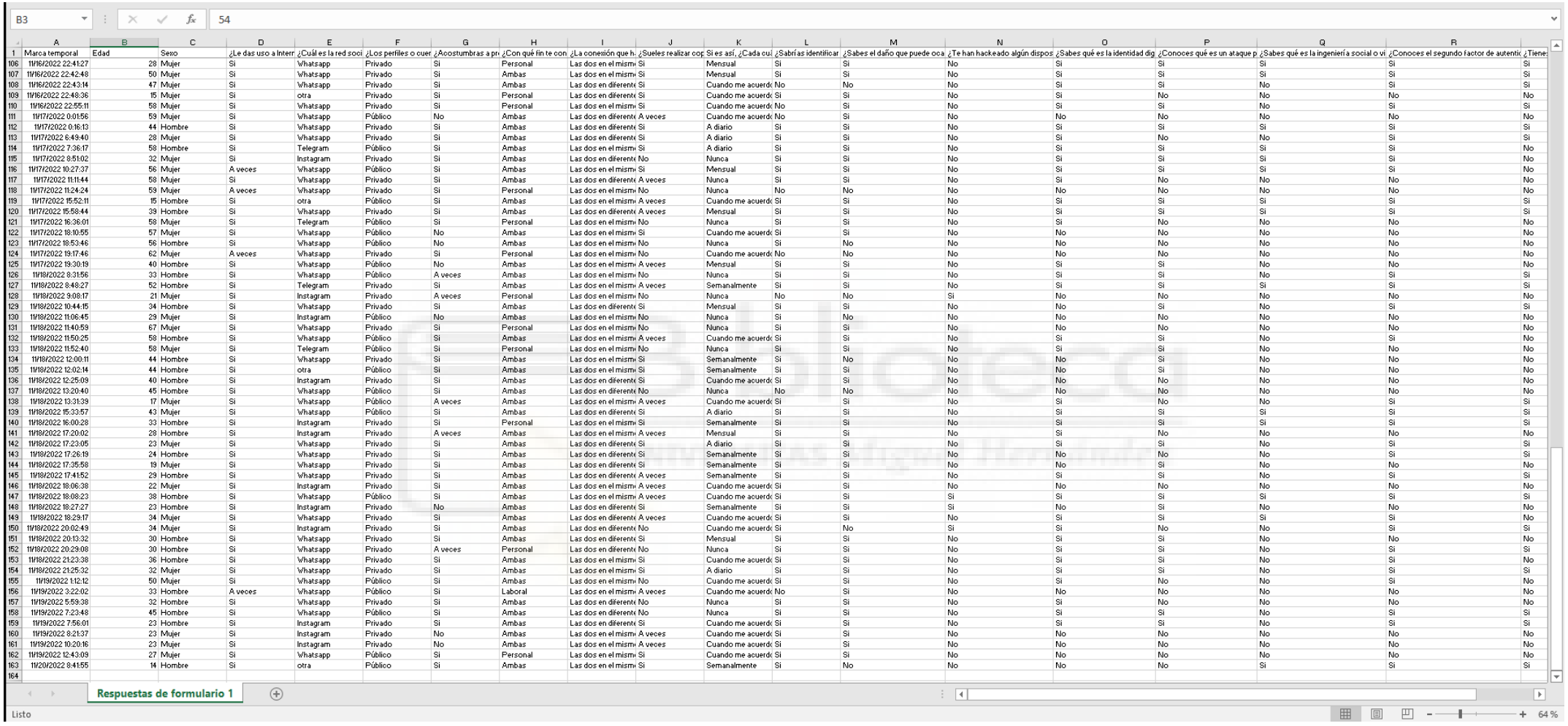
B3 54

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
1	Marca temporal	Edad	Sexo	¿Le das uso a Interr	¿Cuál es la red soci	¿Los perfiles o cuer	¿Acostumbras a pr	¿Con qué fin te con	¿La conexión que h	¿Sueles realizar cop	Si es así, ¿Cada cu	¿Sabrías identificar	¿Sabes el daño que puede oca	¿Te han hackeado algún dispos	¿Sabes qué es la identidad dig	¿Conoces qué es un ataque p	¿Sabes qué es la ingeniería social o vi	¿Conoces el segundo factor de autentic	¿Tiene
59	11/16/2022 15:29:30	56	Hombre	Si	Whatsapp	Privado	A veces	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	Si	Si	No	Si	Si	Si	No	No
60	11/16/2022 16:16:09	43	Hombre	Si	Whatsapp	Privado	A veces	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	Si	Si	No	Si	Si	No	Si	Si
61	11/16/2022 16:22:20	35	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en el misme	Si	Semanalmente	No	Si	No	No	No	No	No	No
62	11/16/2022 16:33:01	50	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	Si	Si	Si
63	11/16/2022 16:36:54	54	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	Si	Si	Si	Si	Si	Si
64	11/16/2022 16:38:07	41	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en el misme	A veces	Cuando me acuerdo	No	Si	No	Si	Si	Si	No	No
65	11/16/2022 17:00:27	49	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en el misme	Si	A diario	Si	Si	No	Si	Si	Si	Si	Si
66	11/16/2022 17:20:04	34	Mujer	Si	Telegram	Privado	Si	Laboral	Las dos en diferente	Si	Semanalmente	Si	Si	No	Si	Si	Si	Si	Si
67	11/16/2022 17:26:27	37	Mujer	Si	Whatsapp	Público	A veces	Personal	Las dos en el misme	A veces	Nunca	No	Si	No	No	No	No	No	No
68	11/16/2022 17:29:14	24	Mujer	A veces	Instagram	Privado	A veces	Personal	Las dos en el misme	A veces	Semanalmente	Si	Si	No	Si	Si	No	No	No
69	11/16/2022 17:57:22	46	Hombre	Si	Telegram	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	Si	Si	Si
70	11/16/2022 17:58:51	46	Hombre	Si	otra	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	Si	Si	Si
71	11/16/2022 18:25:14	50	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en diferente	Si	Cuando me acuerdo	Si	Si	No	Si	Si	No	Si	Si
72	11/16/2022 19:13:11	52	Mujer	Si	Whatsapp	Privado	A veces	Ambas	Las dos en diferente	Si	Semanalmente	No	Si	No	No	No	No	No	No
73	11/16/2022 20:03:56	36	Mujer	Si	Whatsapp	Público	Si	Ambas	Las dos en diferente	Si	Cuando me acuerdo	Si	Si	No	Si	Si	No	No	No
74	11/16/2022 20:08:07	40	Mujer	Si	Whatsapp	Público	A veces	Personal	Las dos en el misme	A veces	A diario	Si	Si	Si	No	No	No	No	No
75	11/16/2022 20:39:01	43	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	Si	Si	Si
76	11/16/2022 20:41:29	28	Hombre	Si	Telegram	Privado	Si	Ambas	Las dos en diferente	Si	Cuando me acuerdo	Si	Si	No	No	No	No	Si	No
77	11/16/2022 20:44:46	45	Mujer	Si	otra	Privado	Si	Ambas	Las dos en el misme	Si	A diario	Si	Si	No	Si	No	Si	Si	Si
78	11/16/2022 20:47:33	30	Hombre	Si	Whatsapp	Privado	A veces	Ambas	Las dos en diferente	Si	Mensual	Si	Si	No	No	Si	Si	Si	Si
79	11/16/2022 20:47:44	54	Mujer	Si	Instagram	Privado	Si	Personal	Las dos en el misme	Si	A diario	Si	Si	No	No	No	No	No	No
80	11/16/2022 20:50:34	48	Hombre	Si	Instagram	Público	No	Ambas	Las dos en diferente	Si	A diario	Si	Si	Si	No	No	No	No	Si
81	11/16/2022 20:54:22	22	Hombre	Si	Instagram	Privado	Si	Personal	Las dos en diferente	A veces	Mensual	Si	Si	No	Si	Si	Si	Si	Si
82	11/16/2022 20:54:29	40	Hombre	Si	Whatsapp	Privado	No	Ambas	Las dos en el misme	No	Nunca	Si	Si	No	Si	Si	Si	Si	No
83	11/16/2022 20:56:42	54	Mujer	Si	Whatsapp	Público	Si	Ambas	Las dos en el misme	No	Nunca	No	No	No	No	No	No	No	No
84	11/16/2022 21:03:11	39	Mujer	Si	Whatsapp	Privado	A veces	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	No	Si	No	Si	Si	No	Si	Si
85	11/16/2022 21:04:41	42	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	Si	Si	No	Si	Si	No	Si	Si
86	11/16/2022 21:08:21	41	Mujer	Si	Whatsapp	Privado	A veces	Ambas	Las dos en el misme	Si	A diario	Si	Si	No	Si	Si	No	No	Si
87	11/16/2022 21:10:28	37	Mujer	Si	Whatsapp	Privado	A veces	Personal	Las dos en el misme	A veces	Cuando me acuerdo	No	No	No	No	No	No	No	No
88	11/16/2022 21:12:38	36	Mujer	Si	Whatsapp	Privado	Si	Personal	Las dos en el misme	Si	Mensual	No	Si	No	No	No	No	No	No
89	11/16/2022 21:25:12	25	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	No	Si	Si
90	11/16/2022 21:37:10	42	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	No	Si	Si	Si	Si	No	Si	Si
91	11/16/2022 21:39:55	56	Mujer	Si	Whatsapp	Público	A veces	Ambas	Las dos en diferente	No	Cuando me acuerdo	No	Si	No	No	No	No	No	No
92	11/16/2022 21:45:17	50	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en el misme	Si	A diario	Si	Si	Si	No	Si	Si	Si	Si
93	11/16/2022 21:47:21	53	Hombre	Si	Telegram	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	Si	Si	Si
94	11/16/2022 21:49:02	35	Hombre	Si	otra	Público	Si	Ambas	Las dos en el misme	A veces	Cuando me acuerdo	Si	Si	Si	Si	Si	Si	Si	Si
95	11/16/2022 21:57:36	29	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en el misme	No	Nunca	Si	Si	No	Si	Si	Si	Si	Si
96	11/16/2022 22:03:21	32	Mujer	Si	Telegram	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	No	Si	No
97	11/16/2022 22:10:40	18	Hombre	Si	Instagram	Privado	Si	Ambas	Las dos en el misme	A veces	Semanalmente	No	Si	No	Si	No	No	No	Si
98	11/16/2022 22:25:31	16	Mujer	Si	Instagram	Privado	A veces	Ambas	Las dos en el misme	A veces	Cuando me acuerdo	Si	Si	No	No	No	No	No	No
99	11/16/2022 22:33:31	32	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	No	Si	Si
100	11/16/2022 22:33:52	56	Mujer	Si	Whatsapp	Privado	Si	Personal	Las dos en el misme	Si	Mensual	Si	Si	No	Si	No	No	Si	No
101	11/16/2022 22:35:17	49	Mujer	Si	Whatsapp	Público	No	Personal	Las dos en el misme	A veces	Cuando me acuerdo	Si	Si	No	Si	No	No	No	No
102	11/16/2022 22:35:59	31	Mujer	Si	otra	Privado	Si	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	Si	No	No	No	No	No	No	No
103	11/16/2022 22:36:49	49	Mujer	Si	Whatsapp	Público	A veces	Personal	Las dos en el misme	A veces	Cuando me acuerdo	Si	Si	No	No	No	No	No	No
104	11/16/2022 22:37:16	54	Mujer	Si	otra	Privado	Si	Ambas	Las dos en el misme	Si	Semanalmente	No	Si	No	Si	No	No	No	No
105	11/16/2022 22:39:53	34	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	No	No	No	Si	Si
106	11/16/2022 22:41:27	28	Mujer	Si	Whatsapp	Privado	Si	Personal	Las dos en el misme	Si	Mensual	Si	Si	No	Si	Si	Si	Si	Si
107	11/16/2022 22:42:48	50	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en el misme	Si	Mensual	Si	Si	No	Si	Si	Si	Si	Si
108	11/16/2022 22:43:14	47	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	Cuando me acuerdo	No	No	No	Si	Si	No	Si	Si
109	11/16/2022 22:48:36	15	Mujer	Si	otra	Privado	Si	Personal	Las dos en diferente	Si	Cuando me acuerdo	Si	Si	No	Si	No	No	No	No
110	11/16/2022 22:55:11	58	Mujer	Si	Whatsapp	Privado	Si	Personal	Las dos en el misme	Si	Cuando me acuerdo	No	Si	No	Si	Si	No	Si	Si
111	11/17/2022 0:01:56	59	Mujer	Si	Whatsapp	Público	No	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	No	Si	No	No	No	No	No	No
112	11/17/2022 0:16:13	44	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	Si	Si	Si
113	11/17/2022 6:49:40	28	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	No	No	Si	Si
114	11/17/2022 7:36:17	58	Hombre	Si	Telegram	Público	Si	Ambas	Las dos en el misme	Si	A diario	Si	Si	No	Si	Si	Si	Si	No
115	11/17/2022 8:51:02	32	Mujer	Si	Instagram	Privado	Si	Ambas	Las dos en diferente	No	Nunca	Si	Si	No	Si	Si	Si	Si	No
116	11/17/2022 10:27:37	56	Mujer	A veces	Whatsapp	Público	Si	Ambas	Las dos en el misme	Si	Mensual	Si	Si	No	Si	Si	Si	Si	No
117	11/17/2022 11:11:44	58	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	A veces	Nunca	Si	Si	No	Si	No	No	No	No

Respuestas de formulario 1

Listo

64 %



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
1	Marca temporal	Edad	Sexo	¿Le das uso a Intern	¿Cuál es la red soci	¿Los perfiles o cuer	¿Acostumbras a pr	¿Con qué fin te con	¿La conexión que h	¿Sueles realizar cop	Si es así, ¿Cada cui	¿Sabrías identificar	¿Sabes el daño que puede oca	¿Te han hackeado algún dispos	¿Sabes qué es la identidad dig	¿Conoces qué es un ataque p	¿Sabes qué es la ingeniería social o vi	¿Conoces el segundo factor de autentic	¿Tiene
106	11/16/2022 22:41:27	28	Mujer	Si	Whatsapp	Privado	Si	Personal	Las dos en el mism	Si	Mensual	Si	Si	No	Si	Si	Si	Si	Si
107	11/16/2022 22:42:48	50	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	Si	Mensual	Si	Si	No	Si	Si	Si	Si	Si
108	11/16/2022 22:43:14	47	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	Cuando me acuerdo	No	No	No	Si	Si	No	Si	Si
109	11/16/2022 22:48:36	15	Mujer	Si	otra	Privado	Si	Personal	Las dos en diferente	Si	Cuando me acuerdo	Si	Si	No	Si	No	No	No	No
110	11/16/2022 22:55:11	58	Mujer	Si	Whatsapp	Privado	Si	Personal	Las dos en el mism	Si	Cuando me acuerdo	No	Si	No	Si	Si	No	Si	Si
111	11/17/2022 0:01:56	59	Mujer	Si	Whatsapp	Público	No	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	No	Si	No	No	No	No	No	No
112	11/17/2022 0:16:13	44	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	Si	Si	Si
113	11/17/2022 6:49:40	28	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	No	No	Si	Si
114	11/17/2022 7:36:17	58	Hombre	Si	Telegram	Público	Si	Ambas	Las dos en el mism	Si	A diario	Si	Si	No	Si	Si	Si	Si	No
115	11/17/2022 8:51:02	32	Mujer	Si	Instagram	Privado	Si	Ambas	Las dos en diferente	No	Nunca	Si	Si	No	Si	Si	Si	Si	No
116	11/17/2022 10:27:37	56	Mujer	A veces	Whatsapp	Público	Si	Ambas	Las dos en el mism	Si	Mensual	Si	Si	No	Si	Si	Si	Si	No
117	11/17/2022 11:11:44	58	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	A veces	Nunca	Si	Si	No	Si	No	No	No	No
118	11/17/2022 11:24:24	59	Mujer	A veces	Whatsapp	Privado	Si	Personal	Las dos en el mism	No	Nunca	No	No	No	No	No	No	No	No
119	11/17/2022 15:52:11	15	Hombre	Si	otra	Público	Si	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	Si	Si	Si	Si	Si
120	11/17/2022 15:58:44	39	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	A veces	Mensual	Si	Si	No	Si	Si	Si	Si	Si
121	11/17/2022 16:36:01	58	Mujer	Si	Telegram	Público	Si	Personal	Las dos en el mism	No	Nunca	Si	Si	No	Si	No	No	No	No
122	11/17/2022 18:10:55	57	Mujer	Si	Whatsapp	Público	No	Ambas	Las dos en el mism	Si	Cuando me acuerdo	Si	Si	No	No	No	No	No	No
123	11/17/2022 18:53:46	56	Hombre	Si	Whatsapp	Público	No	Ambas	Las dos en el mism	No	Nunca	Si	No	No	No	No	No	No	No
124	11/17/2022 19:17:46	62	Mujer	A veces	Whatsapp	Privado	Si	Personal	Las dos en el mism	No	Cuando me acuerdo	No	No	No	No	No	No	No	No
125	11/17/2022 19:30:19	40	Hombre	Si	Whatsapp	Público	No	Ambas	Las dos en el mism	A veces	Mensual	Si	Si	No	Si	Si	No	No	No
126	11/18/2022 8:31:56	33	Hombre	Si	Whatsapp	Público	A veces	Ambas	Las dos en el mism	No	Nunca	Si	Si	No	Si	Si	No	Si	Si
127	11/18/2022 8:48:27	52	Hombre	Si	Telegram	Privado	Si	Ambas	Las dos en el mism	A veces	Semanalmente	Si	Si	No	Si	Si	Si	Si	Si
128	11/18/2022 9:08:17	21	Mujer	Si	Instagram	Privado	A veces	Personal	Las dos en el mism	No	Nunca	No	No	Si	No	No	No	No	No
129	11/18/2022 10:44:15	34	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	Mensual	Si	Si	No	No	Si	No	Si	Si
130	11/18/2022 11:06:45	29	Mujer	Si	Instagram	Público	No	Ambas	Las dos en el mism	No	Nunca	Si	No	No	No	No	No	No	No
131	11/18/2022 11:40:59	67	Mujer	Si	Whatsapp	Privado	Si	Personal	Las dos en el mism	No	Nunca	Si	Si	No	No	No	No	No	No
132	11/18/2022 11:50:25	58	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	Si	Si	No	Si	No
133	11/18/2022 11:52:40	58	Mujer	Si	Telegram	Público	Si	Personal	Las dos en el mism	No	Nunca	Si	Si	No	Si	Si	No	No	No
134	11/18/2022 12:00:11	44	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	Si	Semanalmente	Si	No	No	No	Si	No	No	No
135	11/18/2022 12:02:14	44	Hombre	Si	otra	Público	Si	Ambas	Las dos en el mism	Si	Semanalmente	Si	Si	No	No	Si	No	No	No
136	11/18/2022 12:25:09	40	Hombre	Si	Instagram	Privado	Si	Ambas	Las dos en diferente	Si	Cuando me acuerdo	Si	Si	No	No	No	No	No	No
137	11/18/2022 13:20:40	45	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en diferente	No	Nunca	No	No	No	No	No	No	No	No
138	11/18/2022 13:31:39	17	Mujer	Si	Whatsapp	Público	A veces	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	Si	No	No	Si	Si
139	11/18/2022 15:33:57	43	Mujer	Si	Whatsapp	Público	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	Si	Si	Si
140	11/18/2022 16:00:28	33	Hombre	Si	Instagram	Privado	Si	Personal	Las dos en el mism	Si	Semanalmente	Si	Si	No	Si	Si	Si	Si	Si
141	11/18/2022 17:20:02	28	Hombre	Si	Instagram	Privado	A veces	Ambas	Las dos en el mism	A veces	Mensual	Si	Si	No	Si	No	No	No	No
142	11/18/2022 17:23:05	23	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	A diario	Si	Si	No	Si	Si	No	Si	Si
143	11/18/2022 17:26:19	24	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	Semanalmente	Si	Si	No	No	No	No	Si	Si
144	11/18/2022 17:35:58	19	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	Semanalmente	Si	Si	No	No	Si	No	No	No
145	11/18/2022 17:41:52	29	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	A veces	Semanalmente	Si	Si	No	Si	Si	No	Si	Si
146	11/18/2022 18:06:38	22	Mujer	Si	Instagram	Privado	Si	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	No	No	No	No	No
147	11/18/2022 18:08:23	38	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	Si	Si	Si	Si	Si	Si
148	11/18/2022 18:27:27	23	Hombre	Si	Instagram	Privado	No	Ambas	Las dos en diferente	Si	Semanalmente	Si	Si	Si	No	Si	No	No	No
149	11/18/2022 18:29:17	34	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	A veces	Cuando me acuerdo	Si	Si	No	Si	Si	Si	Si	No
150	11/18/2022 20:02:49	34	Mujer	Si	Instagram	Privado	Si	Ambas	Las dos en diferente	No	Cuando me acuerdo	Si	No	Si	Si	No	No	Si	Si
151	11/18/2022 20:13:32	30	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	Si	Mensual	Si	Si	No	Si	Si	No	No	No
152	11/18/2022 20:29:08	30	Hombre	Si	Whatsapp	Privado	A veces	Personal	Las dos en diferente	No	Nunca	Si	Si	No	Si	Si	No	Si	Si
153	11/18/2022 21:23:38	36	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	Si	Cuando me acuerdo	Si	Si	No	Si	Si	No	Si	No
154	11/18/2022 21:25:32	32	Mujer	Si	Whatsapp	Privado	Si	Ambas	Las dos en el mism	Si	A diario	Si	Si	No	Si	Si	No	Si	Si
155	11/19/2022 1:12:12	50	Mujer	Si	Whatsapp	Público	Si	Ambas	Las dos en el mism	No	Cuando me acuerdo	Si	Si	No	Si	No	No	Si	No
156	11/19/2022 3:22:02	33	Hombre	A veces	Whatsapp	Público	Si	Laboral	Las dos en el mism	A veces	Cuando me acuerdo	No	Si	No	No	No	No	No	No
157	11/19/2022 5:59:38	32	Hombre	Si	Whatsapp	Privado	Si	Ambas	Las dos en diferente	No	Nunca	Si	Si	No	Si	No	No	No	No
158	11/19/2022 7:23:48	45	Hombre	Si	Whatsapp	Público	Si	Ambas	Las dos en diferente	No	Nunca	Si	Si	No	Si	Si	No	Si	Si
159	11/19/2022 7:56:01	23	Hombre	Si	Instagram	Privado	Si	Ambas	Las dos en diferente	Si	Cuando me acuerdo	Si	Si	No	Si	Si	No	Si	Si
160	11/19/2022 8:21:37	23	Mujer	Si	Instagram	Privado	No	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	No	No	No	No	No
161	11/19/2022 10:20:16	23	Mujer	Si	Instagram	Privado	No	Ambas	Las dos en el mism	A veces	Cuando me acuerdo	Si	Si	No	No	No	No	No	No
162	11/19/2022 12:43:09	27	Mujer	Si	Whatsapp	Público	Si	Personal	Las dos en el mism	Si	Cuando me acuerdo	Si	Si	No	No	No	No	No	No
163	11/20/2022 8:41:55	14	Hombre	Si	otra	Público	Si	Ambas	Las dos en el mism	Si	Semanalmente	Si	No	No	No	No	Si	Si	Si
164																			