UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Saldaña Díaz, Mauricio Nicolas (orcid.org/0000-0001-8829-985X)

ASESOR:

Dr. Visurraga Agüero, Joel Martin (orcid.org/0000-0002-0024-668X)

LÍNEA DE INVESTIGACIÓN:
Auditoria de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:
Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2022

Dedicatoria

Mi tesis se la dedico principalmente a mis padres por ser mi soporte y apoyo en esta parte de mi vida y quienes me han permitido desarrollarme profesionalmente. A mis hermanos, por estar a mi lado dándome su apoyo constante. Por último, a mi amiga “Kion” por brindarme su apoyo y amistad en esta parte de mi vida.

Agradecimiento

Agradezco a Dios por brindarme la oportunidad de culminar esta parte de mi vida. De igual manera, a mis padres y hermanos por estar a mi lado, dando su apoyo incondicional y amor.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

La presente investigación titulada Ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022; tiene el objetivo de determinar el impacto de la ciberseguridad y la prevención de ataques cibernéticos en los adultos mayores.

El tipo de investigación utilizada fue de tipo básica-no experimental de nivel transversal correlacional con un muestreo no probabilístico simple. Se obtuvo una muestra de 375 habitantes adultos mayores de 60 años; para la recolección de datos se utilizó la encuesta y el instrumento fue el cuestionario. Todos los datos obtenidos, fueron analizados mediante el programa estadístico SPSS.

Los resultados obtenidos en la investigación según la regresión ordinal fueron para la ciberseguridad y su impacto en la prevención de ataques cibernéticos un valor de sig. de 0.000 < 0.05. De la misma manera, la dimensión detección de vulnerabilidades, el valor sig. de 0.000 < 0.05. También, la dimensión prevención de robo de información el valor de sig. de 0.406 > 0.05. Finalmente, la dimensión identificación de tipos de ciberataques, el valor de sig. 0.017 < 0.05.

Se concluye finalmente que la ciberseguridad impacta en la prevención de ataques cibernéticos en los adultos mayores.

Palabras clave: Ciberseguridad, Prevención de ataques cibernéticos, Seguridad de la información

Abstract

This research entitled Cybersecurity and its impact on the prevention of cyber attacks on older adults in the district of Jesús María, Lima 2022; has the objective of determining the impact of cybersecurity and the prevention of cyber attacks on older adults.

The type of research used was basic-non-experimental type of correlational cross-sectional level with a simple non-probabilistic sampling. A sample of 375 adult inhabitants over 60 years of age was obtained; For data collection, the survey was used and the instrument was the questionnaire. All data obtained were analyzed using the statistical program SPSS.

The results obtained in the investigation according to the ordinal regression were for cybersecurity and its impact on the prevention of cyber attacks a value of sig. of 0.000 < 0.05. In the same way, the vulnerability detection dimension, the value sig. of 0.000 < 0.05. Also, the information theft prevention dimension the value of sig. of 0.406 > 0.05. Finally, the dimension identification of types of cyberattacks, the value of sig. 0.017 < 0.05.

It is finally concluded that cybersecurity has an impact on the prevention of cyber attacks in older adults.

Keywords: Cybersecurity, Prevention of cyber attacks, security of the information

I. INTRODUCCIÓN

El avance tecnológico en los últimos años ha ido evolucionado rápidamente, más aún debido a la pandemia, donde la gran mayoría de empresas tanto grandes como pequeñas tuvieron que pasar por una transformación digital drástica, haciendo que usuarios y clientes se vean afectados, por una parte, las empresas tuvieron que cambiar de manera acelerada los procesos de cada área, una de las áreas implicadas, en la cual tuvo un fuerte impacto fue el de la ciberseguridad, y por otra parte, los usuarios y clientes que comenzaron a trabajar remotamente y se conectaban desde sus redes domésticas y que al no estar en un espacio controlado, es decir, dentro de una conexión segura, eran más propensos a recibir ataques cibernéticos.

Es decir, la pandemia no afectó solo a la seguridad de información de las empresas, sino también a todas las personas que hacen uso de las tecnologías especialmente a los adultos mayores, que tienen pocos conocimientos, sobre cómo protegerse contra estos tipos de ataques, siendo víctimas de ataques como el phishing, estafas, dominios malignos, desinformación, entre otras más. Estos tipos de ataques, si bien ya eran conocidos, sus cifras se incrementaron debido a esta crisis mundial.

Como se mencionó previamente, los ciberdelincuentes a nivel mundial, centraron sus ataques en los trabajadores de las empresas, que realizaban trabajo remoto, reportándose en donde Protek (2022) indica que en el 2021 el robo de credenciales de los usuarios, ascendió en 20%, debido a esta modalidad, de igual manera, aprovechando el auge de las criptomonedas se realizaron estafas, donde muchas personas perdieron grandes cantidades de dinero, es importante mencionar que durante el 2021, el 80% de estos ataques fue por error humano y que un 35%, fueron casos de phishing o suplantación de identidad, adicionalmente, el 30% de los afectados por causas de fraude, son adultos mayores de 60 años, todo esto ocasiono grandes pérdidas económicas y de prestigio, para las empresas y de igual manera para los usuarios independientes los cuales se vieron afectados por falta de capacidad y conocimientos, sobre todo en los adultos mayores.

Por otro lado, a nivel nacional cuando la pandemia llegó al país y se declaró el estado de emergencia en marzo del 2020, el número de estafas se duplicaron, especialmente con el método de phishing en los dispositivos móviles, se detectaron un aumento entre los meses de febrero y marzo. Así mismo, según Pichihua (2021), durante el inicio de la pandemia los delitos informáticos se elevaron en 39.78%, la División de Investigación de Delitos de Alta Tecnología (Divindat) de la policía, tuvo un registro de 300 casos cada mes, los fraudes informáticos, suplantación de identidad, entre otros casos más, sumaron un total de 4, 162 casos durante el 2020, 84% de ellos fueron por delitos informáticos y un 10% haciendo uso de tecnologías de información.

De igual manera, como se mencionó más arriba, los adultos mayores son los que se vieron más afectados por dichos cambios, debido a que, al no tener conocimientos digitales, eran más vulnerables a caer en las estafas, fraudes y otros hechos delictivos. Debido a lo explicado hasta ahora, podemos entender que, en el distrito de Jesús María, el público más vulnerable a ataques cibernéticos son los adultos mayores de 60 años, es debido a que, no tienen conceptos sobre la ciberseguridad y no identifican o entienden, el significado de algunos de los nombres más comunes de estos ataques. Esto se debe a que, por no haber nacido en el auge de la tecnología, les cuesta más entender y aprender, por lo que la gran mayoría de estos adultos buscan ayuda en algún familiar más joven, para que los guie sobre estos temas.

Por lo tanto, como problema general se generó la siguiente pregunta, ¿De qué manera la ciberseguridad impacta en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022? Con respecto a los problemas específicos, se plantearon las siguientes preguntas específicas, a) ¿De qué manera la ciberseguridad impacta en la dimensión detección de vulnerabilidades en los adultos mayores en el distrito de Jesús María, Lima 2022?, b) ¿De qué manera la ciberseguridad impacta en la dimensión prevención de robo de información de los adultos mayores en el distrito de Jesús María, Lima 2022?, c)

¿De qué manera la ciberseguridad impacta en la dimensión identificación de tipos de ciberataques en los adultos mayores en el distrito de Jesús María, Lima 2022?

En esta investigación se justificó en diferentes aspectos los cuales son los siguientes. Dentro de la justificación epistemológica, se recopiló todos los conocimientos necesarios para desarrollar la problemática, así mismo, se expuso de manera detalladamente cada proceso realizado durante la investigación, de esta manera se buscó transmitir de manera clara el objetivo de la investigación y mediante la aplicación del método científico y los datos recogidos en nuestro instrumento de investigación se validó las hipótesis propuestas. Así mismo, en la justificación teórica, se buscó aumentar la información con relación a la ciberseguridad y la prevención de ataques cibernéticos, haciendo uso de un marco teórico y conceptual, donde se explicó las variables y dimensiones de la investigación, haciendo uso de la bibliografía recopilada con antelación, donde se explicó el enfoque de manera adecuada, de esta manera se busca aportar nuevos conocimientos para el desarrollo de investigaciones futuras. Con relación a la justificación práctica, se basa como la ciberseguridad brinda soluciones para identificar, proteger y prevenir el robo de información, a si de esta manera nos facilita en obtener los conocimientos necesarios en cómo impacta en la prevención de ataques cibernéticos. Por último, en la justificación metodológica, podemos mencionar que esta investigación está desarrollada bajo un diseño no experimental, debido a que las dos variables presentadas no están expuestas a un cambio. Se tiene como propósito obtener resultados verídicos, en donde recopilamos datos mediante un instrumento digno de confianza que ha sido validada por expertos en el tema.

Se planteó el siguiente objetivo general para resolver la problemática de esta investigación, determinar el impacto de la ciberseguridad en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022. En consecuencia, se planteó los siguientes objetivos específicos: a) Determinar el impacto de la ciberseguridad en la dimensión detección de

vulnerabilidades en los adultos mayores en el distrito de Jesús María, Lima 2022, b) Determinar el impacto de la ciberseguridad en la dimensión prevención de robo de información de los adultos mayores en el distrito de Jesús María, Lima 2022, c) Determinar el impacto de la ciberseguridad en la dimensión identificación de tipos de ciberataques en los adultos mayores en el distrito de Jesús María, Lima 2022.

Así mismo, luego de haber planteado los objetivos de la investigación, se plantea la siguiente hipótesis general, la ciberseguridad impacta significativamente en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022. Consecuentemente se plantean las siguientes hipótesis específicas: a) La ciberseguridad impacta significativamente en la dimensión detección de vulnerabilidades en los adultos mayores en el distrito de Jesús María, Lima 2022, b) La ciberseguridad impacta significativamente en la dimensión prevención de robo de información de los adultos mayores en el distrito de Jesús María, Lima 2022, c) La ciberseguridad impacta significativamente en la dimensión identificación de tipos de ciberataques en los adultos mayores en el distrito de Jesús María, Lima 2022.

II. MARCO TEÓRICO

Para el desarrollo de esta investigación, conviene destacar estudios previos relacionados a nuestras variables de modo que nos sirva como base para el desarrollo de esta, con respecto a los antecedentes internacionales nos podemos referir al estudio de Choejey (2018) con su investigación titulada Desafíos y prácticas de ciberseguridad: Un estudio de caso de Bután, realizado en la Universidad Murdoch, Perth, Australia Occidental, cuyo objetivo fue el de investigar la ciberseguridad en el contexto de las TIC países emergentes, principalmente para comprender cómo los países emergentes de TIC, como Bután un país de Asia del Sur, están gestionando los desafíos de ciberseguridad, utilizó un diseño de investigación secuencial de manera mixta, es decir, combinando cuantitativos y cualitativos. Llegando a la conclusión de que, la investigación mostró que Bután es vulnerable a los riesgos de ciberseguridad, como el malware, la piratería y la ingeniería social.

Asimismo, nos referimos a Bernashvili (2017) con su investigación titulada El impacto del cibercrimen y marco legal de los voluntarios en la ciberseguridad: caso de Georgia, realizado en la Universidad de Tecnología de Tallin, Estonia. Esta investigación tuvo como objetivo el de examinar el enfoque regulatorio actual para la seguridad cibernética a nivel nacional y considera la legislación aplicable para definir y establecer la naturaleza jurídica de ciberseguridad y voluntariado, utiliza un enfoque cuantitativo. Y concluye en que, el documento analiza si el enfoque georgiano de la seguridad cibernética es compatible con los estándares internacionales y de la UE.

Por otro lado, Fritzvold (2017) con su investigación titulada, Ciberseguridad en las Organizaciones, realizada en la Universidad de Stavanger, Noruega, cuyo objetivo fue la de encontrar similitudes en la industria, problemas clave y desafíos relacionados con la seguridad cibernética, y encontrar áreas de mejora, realizó un análisis cualitativo, los datos adquiridos fue a través de un proceso de entrevista. Concluye en que, las tres organizaciones en este estudio han aumentado su

enfoque en la seguridad cibernética y son conscientes de las vulnerabilidades y los riesgos asociados con la tecnología. Así mismo, la seguridad cibernética se ha convertido en un tema común.

Por otro lado, Anchundia-Betancourt (2017) con su investigación titulada Ciberseguridad en los sistemas de información de las universidades, realizada en la Revista Científica, dominio de las ciencias, Ecuador. El objetivo principal de esta investigación fue la de determinar el conocimiento actual de como intervienen las universidades en las enseñanzas sobre la ciberseguridad. La investigación concluye en que, las universidades juegan un papel importante para establecer una cultura en la ciberseguridad exigiendo una capacitación en cada sector dentro de la sociedad.

Por último, Camargo (2020) con su investigación denominada Ciberseguridad y teletrabajo en tiempos de covid-19, realizado en la Universidad del Rosario, Bogotá. Su objetivo principal fue realizar un estudio cuantitativo sobre la percepción y la actitud de los empleados hacia la ciberseguridad en diferentes organizaciones libias. Concluye demostrado a través del análisis que, de hecho, estas actitudes que se muestran hacia la ciberseguridad en los negocios son significativas en cuanto al impacto que tiene en los empleados con diferentes edades, géneros, así como diferentes puestos de trabajo y varios niveles de experiencia.

Así mismo. En cuanto antecedentes nacionales tenemos a Bohorquez (2021), con su investigación denominada Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020, realizado en la Universidad César Vallejo. Optaron por una investigación no experimental – correlacional, el objetivo principal fue determinar como la ciberseguridad se relaciona con la gestión de tecnologías de información en dicha empresa. En donde 87 empleados era la población, pero solo se les tomó a 71 empleados la encuesta realizada en esta tesis. Por el cual llegó a la conclusión que, la ciberseguridad se relaciona significativamente con la gestión de tecnologías de información en la

empresa realizada donde el coeficiente de Rho de Spearman es igual a 0.832, en el cual se evidencia una correlación de nivel muy fuerte.

Asimismo, Aliaga (2021), con su investigación denominada Implementación de un sistema de ciberseguridad para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza, realizada en la Universidad César Vallejo. Realizaron una investigación experimental – pre experimental, el objetivo principal fue determinar como la implementación de un sistema de ciberseguridad influye en la prevención de ataques cibernéticos. Tanto la población como la muestra fueron de 50, realizándoles una encuesta a cada empleado. Concluyeron que dicha implementación influyó de manera positiva en la prevención de estos ataques, en donde se comprobó que disminuyó las vulnerabilidades que sufría esta empresa así de esta manera aumentando el desempeño de esta.

Por otro lado, esta Morales (2020) con su investigación denominada Uso de tecnologías de información y comunicaciones en la seguridad ciudadana del distrito de Santiago de surco, realizada en la Universidad César Vallejo. El objetivo principal fue determinar cómo aplicar las tecnologías de información en la seguridad ciudadana en el distrito de Santiago de Surco. En esta investigación utilizaron la observación y las encuestas para obtener los resultados. Concluyendo así que, las tecnologías de la información en este distrito no están integradas, existiendo una dispersión y de igual manera el sistema de radiotransmisión emplea un servicio de contratado donde se requiere una inversión enorme restándole competencia frente a otros distritos en este campo de la seguridad a los ciudadanos.

Por otro lado, esta Medina (2021) con su investigación denominada Teletrabajo y la gestión de seguridad de la información en la empresa infoservicios, Lima-2020. Realizada en la Universidad César Vallejo, el objetivo principal fue determinar la relación del teletrabajo y la gestión de seguridad de información en la empresa infoservicios. Se realizó una investigación no experimental – correlacional, donde se utilizó la encuesta como instrumento a unos 70 trabajadores. Concluyeron en

que, se estableció una correlación positiva donde recalcaron que mientras exista un mayor uso del teletrabajo aumentará la gestión en la seguridad de la información.

Por último, tenemos a Díaz (2018) con su investigación denominada La auditoría informática y la seguridad de la información en el área de sistemas de la caja del Santa, Chimbote, realizada en la Universidad Privada del Norte, el objetivo principal fue determinar en qué medida la auditoría informática se relaciona con la seguridad de la información en la caja del Santa. Se realizó una investigación no experimental – correlacional, donde la población y muestra fueron de 10 trabajadores, a los cuales se utilizó la encuesta para recabar los datos necesarios. Concluyeron en que, cada dimensión utilizada en esta investigación se encontraba en un estado ineficiente, sin embargo, logrando de esta manera aceptar la hipótesis.

Con respecto a las teorías, esta investigación es respaldada a través de las siguientes descritas más adelante. En primer lugar, tenemos a la Teoría General de Sistemas (T.G.S.), tenemos en primer lugar a Ossa (2017), donde explica de manera amplia que la T.G.S., es el estudio de los sistemas de manera interdisciplinaria, que busca aplicar los principios en cualquier sistema. De igual manera tenemos a Hernández (2020), donde la TGS ofrece diferentes metodologías en diferentes ámbitos como arquitectura, diseño, de esta manera ofrece soluciones óptimas para el planteamiento de problemas variados. Por otro lado, Peralta (2016) nos indica que la TGS utiliza los modelos de organización de los sistemas, para explicar los fenómenos que se encuentran en la realidad, de esta manera se pueden aplicar a múltiples enfoques que se utilizan dentro del estudio de la misma. De acuerdo con Domínguez y López (2016), la teoría general de sistemas es útil y aplicable a gran escala como herramienta, así mismo de manera estructurada utiliza una técnica llamada divide y vencerás, la cual genera una versatilidad quien la utilice, de igual manera, si se utiliza un enfoque sistémico genera seguridad para detectar todo tipo de desviación que se generen, así el sistema puede realizar las correcciones necesarias aplicando una visión integral y global de acuerdo al objeto del estudio. Finalmente, Maldonado (2017) nos menciona que la TGS consiste en

un conjunto de diferentes métodos y metodologías, los cuales tienen en común, de manera negativa no eran de manera determinada no simplificada, sin embargo, de manera positiva presentan una visión prismática de todo lo que nos rodea, trabajando así en grupos, los cuales ayudan a brindar soluciones a los problemas, así obtiene una dinámica fluida donde tanto el mundo como la ciencia trabajan para beneficiarse mutuamente.

Luego tenemos a la Teoría de la Información donde según Machado (2016), de igual manera para López y Lombardi (2015), igualmente para Gómez y López (2019), también para Marcos (2018) y del mismo modo para Scozzina (2020) explican que la teoría de la información se basa en la trasmisión, procesamiento y medición de la información y de igual manera como la tecnología es utilizada para transmitir y procesar esta misma, para ser utilizada alrededor de todo el mundo.

En esta investigación tenemos como variables de estudio a la ciberseguridad y la prevención de ataques cibernéticos; de esta manera, se ha recopilado definiciones de cada una de ellas, permitiendo así un mejor entendimiento, siendo así expondremos la primera variable independiente Ciberseguridad, donde se exponen los siguientes autores. De acuerdo con Poma y Vargas (2019) La ciberseguridad es un mecanismo el cual permite en varios casos prevenir que los usuarios sean víctimas de robo de información, así como su identidad, y esta información sea utilizadas para fines inapropiados. De igual manera, Dalal et al. (2022), como también Patino (2021) nos describe que la ciberseguridad brinda un soporte, de igual manera es una estrategia para la seguridad en donde participa en una igualdad para el ámbito internacional para mejorar las prácticas que se aplican en todo el mundo. Así mismo, para Matheu et al. (2020) como también Cano y Rocha (2019), para aplicar la ciberseguridad, no es suficiente conocer y comprender las amenazas que ya se conocen, sino hay que actualizar las nuevas propuestas las cuales nos permitan además de proteger y asegurar los activos más valiosos de las empresas, tenemos que defender y anticiparnos a los diferentes escenarios que nos son desconocidos, en donde es necesario utilizar una vista más sistémica en las

organizaciones y países para que les facilite la identificación y la gestión de riesgos latentes y emergentes. Además, Machín y Gazapo (2016), nos explica que internacionalmente la ciberseguridad está declarada como prioridades en términos de seguridad, ya que actualmente uno de los retos a nivel global es la necesidad de proteger y tratar adecuadamente la información. También para Ignaczak, Goldschmidt y Costa (2022) nos describe a la ciberseguridad como una manera de monitorear las amenazas tradicionales y emergentes que se desarrollan en el ciberespacio, así de esta manera pueden obtener información sobre los posibles riesgos que pueden tener una infraestructura de una organización. Finalmente. Astorga y Shmidt (2019), nos menciona que a la ciberseguridad se le conoce también como seguridad cibernética, abarca los campos como supervisar y gobernar, investigación, operación y mantenimiento, proteger y defender, entre otros, donde el campo donde se avoca más la ciberseguridad es en el de proteger y defender para la seguridad de la información.

Según lo explicado previamente tenemos a las siguientes dimensiones de la variable independiente, descritas a continuación, en primer lugar, la confidencialidad de la información, donde Patino (2020) también para Mendivil, Sanz y Gutierrez (2022), nos menciona que es el intento de proteger y resguardar la integridad y continuidad de cualquier sistema. De igual manera, Cangea (2018) nos describe a la confidencialidad de la información una propiedad que se encarga de proteger y mantener a cualquier información a las personas autorizadas. Para Anchundia-Betancourt (2017) trata sobre cómo es esencial mantener y almacenar los activos en un espacio seguro para evitar que sean víctimas de hackers. Finalmente, para Chuquilla, Guarda y Ninahualpa (2019) nos menciona que ante el gran aumento de ciberataques es necesario el uso de diferentes gestiones y metodologías para garantizar la seguridad en la confidencialidad de la información.

Así mismo como segunda dimensión integridad de la información Patino (2020), nos describe que tanto los sistemas como los datos no haya habido ningún cambio sin autorización previa. De la misma manera, García (2019) nos menciona que para

mantener la integridad de la información es el trabajo tanto de empresas privadas, públicas, de freelancers que deben de tomar las medidas necesarias para protegerse ante cualquier amenaza. Además, Cangea (2018), del mismo modo Campbell (2016) y finalmente para Anatolii et al. (2021), nos describe la integridad de la información como, una manera en como una empresa demuestra la garantía de los datos que maneja son de plena confianza, consistentes y precisos y las únicas personas capaces de realizar cualquier cambio son las que tienen autentificación.

Finalmente, como tercera dimensión disponibilidad de la información Patino (2020) y del mismo modo Cangea (2018), nos describe que se pueden utilizar los sistemas para recabar la información en cualquier momento que se tenga previsto. Así mismo, para Cando-Segovia y Medina-Chicaiza (2021) la disponibilidad de la información vela también por la integridad del funcionamiento de las redes. De la misma manera, Anchundia-Betancourt (2017) nos menciona que cada vez que la sociedad crece y se vuelve más dependiente de la tecnología, la disponibilidad de la información es más crítico y necesario para poder ser transmitidos alrededor del mundo.

De acuerdo a la definición de la variable dependiente Prevención de ataques cibernéticos, se exponen los siguientes autores. En primer lugar, Lehu (2018) el ciberataque consta de una acción que puede ser tanto como individual como colectiva, donde el objetivo es recabar información de la integridad de un sistema de información de una persona, empresa u organización, utilizando las tecnologías y la red de manera total o parcial para realizar estos actos. De igual manera, para Alhari et al. (2021), se interpreta como un acto desfavorable en donde se utiliza las computadoras, redes o sistemas, los cuales son utilizados para interceptar o romper las defensas de una organización para así obtener los activos de esta misma. Así mismo, Pons (2017), nos menciona que cualquier tipo de ciberataque conlleva a tener diferentes efectos, uno de ellos a ser vulnerables, en donde afecta a la protección tanto individual como global, haciendo que estos ataques tengan una

gran difusión en los diferentes medios afectando así la opinión sobre estas organizaciones en todo el mundo. También, para Kotenko et al. (2021) explica como el ritmo avanzado que se está teniendo en el ámbito de las tecnologías, como por ejemplo en las redes, protocolos, sistemas, comunicación hacen que se expongan a nuevas amenazas y sean vulnerables a nuevos tipos de ataques sin precedentes. Finalmente, Networks Asia (2018) en resumen los ciberataques son lanzados no solo a una computadora sino a varias haciendo que otras computadoras se enfrenten a ellas para robar la información.

Según lo explicado más arriba tenemos a las siguientes dimensiones de la variable dependiente, descritas a continuación. La primera dimensión es la detección de vulnerabilidades donde Padilla (2017) menciona que aparte de los ciberataques, una parte vulnerable de la tecnología son los firmwares de los aparatos tecnológicos, en donde para detectar estas vulnerabilidades se tiene que utilizar escáneres para el malware; donde se encargan de buscar códigos malignos y ciertas amenazas que ya son conocidas. De igual manera, para Das y Gündüz (2019) para detectar las vulnerabilidades en nuestros dispositivos es evitar cualquier puerta trasera, las cuales son una forma en donde los atacantes pueden infiltrarse en nuestros sistemas. Así mismo, para Lecklider (2017) una manera para realizar la detección de vulnerabilidades es utilizar el ethical hacking, en donde pones a prueba tu sistema de seguridad, en los mismos casos como si fuera siendo atacado por un atacante, de esta manera se busca encontrar debilidades en los sistemas para poder corregirlo a tiempo y reducir las vulnerabilidades. También, Kara, Hizal y Zengin (2022) un método para detectar las vulnerabilidades es realizar test de seguridad usando redes físicas reales, sin embargo, es costoso y requiere un tiempo de coste demasiado alto, y como contiene información crítica, se recomienda modelar y simular diferentes métodos, de esta forma nos acerca a resultados parecido a los casos reales. Finalmente, para Cangea (2018) como se mencionó una manera para detectar las vulnerabilidades, es utilizar el ethical hacking donde se debe de cumplir las cinco etapas que esta se compone: la investigación,

escaneo, brindar acceso, mantenimiento de los accesos y finalmente cubrir nuestro rastro.

Así mismo, tenemos como segunda dimensión la prevención de robo de información donde Especial Directivos (2020), nos menciona que para prevenir el robo de información solo tenemos que utilizar solo los ordenadores que nos brindan las organizaciones o empresas, mantener actualizados los sistemas de seguridad, mantener la información solo en los equipos de la empresa, no descargar, ni almacenar información de los equipos corporativos en computadoras personales y de igual manera no compartir tal información, así mismo, las empresas deben de mantener unas reglas y monitorizar de manera estricta los accesos y conexiones que realizan cada trabajador, sin importar el rol que tengan. Así mismo, Padilla (2017) nos menciona que, para prevenir el robo de información, tenemos que utilizar firmas criptográficas; las cuales se basan en la criptografía asimétrica, donde se genera una clave pública para mantener la integridad de los datos, de esta manera, se puede comprobar que esta firma es solo del usuario y no ha sido modificada; otra manera es la autentificación; donde no se debe de conceder permisos a cualquier aplicación que se instale o que un usuario solicite, en primer lugar se debe de autentificar al usuario; por último, utilizar herramientas de análisis para valorar en qué nivel de seguridad están los sistemas. También, Das y Zekeriya (2019) nos menciona que para prevenir el robo de información debemos tener un control de acceso a nuestros dispositivos, no solo a ellos sino a cualquier documento o información que nosotros manejamos y queramos proteger, de igual manera, es importante mantener nuestros documentos confidenciales de manera cifrada, también es esencial utilizar sistemas de detección de intrusos. De igual manera, Carlini (2016) nos menciona que se tiene que mejorar las capacidades de análisis, de operación y las habilidades técnicas de los usuarios, promover la cultura de la seguridad a toda la población. Del mismo modo, para Networks Asia (2015), nos menciona que, para prevenir y luchar contra el robo de información, todas las organizaciones deben de tener la capacidad para combatir los ataques de tipo volumétrico. Finalmente, para Campbell (2016), para prevenir el robo de información

requiere el esfuerzo de todos para que funcione, donde se debe de enseñar a cada empleado lo básicos de la ciberseguridad como, por ejemplo: no utilizar contraseñas simples, no conectar tu teléfono personal a una computadora de la empresa.

Finalmente, como tercera dimensión identificación de tipos de ciberataques tenemos a Das y Zekeriya (2019), del mismo modo Campbell (2016), nos describe la inyección de malware; que se basa en la instalación de softwares maliciosos ubicados en el ciberespacio para causar daño, uno de ellos el más conocido el WannaCry Ransomeware; el Phishing que es el ataque que solicita datos de una fuente que quiere pretender ser confiable, también está el Spear phishing; que se parece al mencionado con anterioridad, pero busca que el usuario de clic a un archivo para instalar un software malicioso; tenemos al hacking; que busca obtener acceso a los sistemas en donde busca la obtención de contraseñas para robar la información. De igual manera, para Cangea (2018), nos menciona que la ingeniera social es el método más eficiente de los ciberataques, porque ataca manipulando psicológicamente a las personas utilizando información falsa atacando a la empatía de las personas para que difundan o compartan información confidencial, nos menciona igual al descifrado de contraseñas, suplantación de identidad, sniffing, que corresponde robar o interceptar una información capturada en el tráfico de red, realizar un ataque mediante un intermediario. También para Avci (2021), nos menciona los ciberataques más comunes los cuales son ataque mediante DDoS, las computadoras esclavas o también llamadas botnet o zombies, los spyware o adware, donde busca infectar los sistemas mediante publicidad engañosa, los ya conocidos mensajes spam o basura. Finalmente, para Pyke et al. (2021), nos menciona como en la identificación de tipos de ataques también interviene el conocimiento de los usuarios sobre los ciberataques y cómo manejarlo es un factor que impacta en la susceptibilidad de estos, así mismo ellos toman la ventaja de la baja habilidad de los humanos para detectar o reconocer las señales de los diferentes tipos de ciberataques.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1 Tipo de investigación

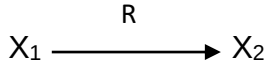
Se consideró en la presente investigación sea de tipo básica. Según Ley-31250 (2021) y de acuerdo a Sánchez, et al. (2018) describen a la investigación básica, también llamada teórica, al estudio cuyo enfoque está en la búsqueda de conocimientos innovadores, sin ningún fin práctico.

3.1.2 Diseño de investigación

Para el desarrollo de este estudio se decidió utilizar una investigación no experimental, debido a que la manera en que se recolectará la información será por medio de las encuestas, con el propósito de obtener una respuesta a la problemática planteada en el desarrollo de este estudio. Para Hernández y Mendoza (2018) se define como el estudio que no manipula de manera intencional a las variables de la investigación, lo que se busca es la observación y la medición de los conceptos de las variables para que sean analizadas luego.

El nivel escogido en el desarrollo de este estudio es el de transversal de nivel correlacional o causal, donde según Hernández y Mendoza (2018) nos describe que este tipo de diseño se especializa en entablar la relación que existe entre dos o más variables, la cual se realiza en un solo momento único. Por esta razón se busca el impacto entre nuestras dos variables, la ciberseguridad y la prevención de ataques cibernéticos.

Esquema:



Donde:

X_1: Ciberseguridad; X_2: Prevención de ataques cibernéticos; R: Relación causal

3.2. Variables y Operacionalización

Variable Independiente: Ciberseguridad

La variable ciberseguridad se define de tipo cualitativa y de tipo ordinal. Según Sánchez, et al. (2018) definen a las variables cualitativas a la forma en que se miden de acuerdo a las características o cualidades.

Definición Conceptual de la variable Ciberseguridad

Según Poma y Vargas (2019) La ciberseguridad es un mecanismo el cual permite en varios casos prevenir que los usuarios sean víctimas de robo de información, así como su identidad, y esta información sea utilizadas para fines inapropiados.

Definición Operacional de la variable Ciberseguridad

Para la variable ciberseguridad se rige bajo tres dimensiones esenciales también llamados pilares las cuales son: confidencialidad, integridad y disponibilidad de la información. En el desarrollo de este estudio fue evaluada utilizado la escala de Likert, los niveles establecidos son de “No óptimo”, “Regular” y “Óptimo”. Ver Anexo 2

Variable Dependiente: Prevención de ataques cibernéticos

La variable prevención de ataques cibernéticos se define de tipo cualitativa y de tipo ordinal. Según Sánchez et al. (2018) definen a las variables cualitativas a la forma en que se miden de acuerdo a las características o cualidades.

Definición Conceptual de la variable Prevención de ataques cibernéticos

Según Lehu (2018) el ciberataque consta de una acción que puede ser tanto como individual como colectiva, donde el objetivo es recabar información de la integridad de un sistema de información de una persona, empresa u organización, utilizando las tecnologías y la red de manera total o parcial para realizar estos actos.

Definición Operacional de la variable Prevención de ataques cibernéticos

Según la variable prevención de ataques cibernéticos en este estudio se rige bajo tres dimensiones: detección de vulnerabilidades, prevención de robo de información e identificación de tipos de ataques. En el desarrollo de este estudio será evaluada utilizado la escala de Likert, los niveles establecidos son de “Baja prevalencia”, “Media prevalencia” y “Alta prevalencia”. Ver Anexo 2

3.3. Población, muestra, muestreo y unidad de análisis

Población

De acuerdo con Sánchez, et al. (2018) describe a la población como al conjunto de elementos, los cuales poseen las mismas características.

De esta manera, para el presente estudio se consideró la población que existe en el distrito de Jesús María, según INEI (2022) menciona que la cantidad actual de adultos mayores de 60 años ubicados en el distrito de Jesús María son de 16 535 habitantes. En la siguiente tabla se detalla:

Tabla 1

Población identificada por edad de adulto mayor

Población	Cantidad
60 a 64 años	4,913
65 a 69 años	4,736
70 a 74 años	3,991
75 a 79 años	2,895
Total de población	16,535

Fuente: INEI (2022)

Muestra

Según Hernández y Mendoza (2018) describe a la muestra como una parte que fue escogida a partir de la población, la cual cumple con las características necesarias para la investigación, de la cual se realizará la recolección de datos.

Para poder realizar el cálculo de la muestra se utilizó el software estadístico, cuyo nombre es Decision Analyst STATS versión 2.0.0.2, en el cual se registró el tamaño de la población mencionada con antelación, se ingresó un 5% como margen de error y un 95% de nivel de confianza. Se obtuvo como resultado unos 375 habitantes como muestra de una población de habitantes.

Tabla 2

Muestra identificada por edad de adulto mayor

Población	Cantidad
60 a 64 años	111
65 a 69 años	107
70 a 74 años	91
75 a 79 años	66
Total de muestra	375

Muestreo

Para el presente estudio de investigación se optó por un muestreo no probabilístico simple. Según Hernández y Mendoza (2018), describe a este tipo de muestreo como la elección de los participantes en base a ciertas características que se asemejen.

Unidad de Análisis

Para el desarrollo de esta investigación se consideró a la unidad de análisis a todos los adultos mayores a partir de los 60 años.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

La técnica que se va a utilizar en este estudio es la encuesta. De acuerdo con Sánchez, et al. (2018) menciona que por medio de este método se busca recolectar información por medio de un conjunto de cuestiones la cual es aplicada a nuestra muestra.

Instrumentos de recolección de datos

De acuerdo a lo anterior, se utilizó como medio de colección de datos, el cuestionario. De acuerdo, Hernández y Mendoza (2018), nos describe al cuestionario como un conjunto de preguntas relacionadas a la operación de las variables las cuales vamos a medir. Ver Anexo 3.

Tabla 3

Ficha Técnica del instrumento de recolección de datos

Nombre del Instrumento:		Cuestionario para los adultos mayores de 60 años en el distrito de Jesús María	
Autor:		Mauricio Nicolas Saldaña Díaz	
Año:		2022	
Tipo de Instrumento:		Cuestionario	
Objetivo:		Determinar el impacto de la ciberseguridad en la prevención de ataques cibernéticos en los adultos mayores del distrito de Jesús María.	
Población:		16 535 adultos mayores del distrito de Jesús María	
Número de Ítems:		36 preguntas	
Aplicación:		En línea	
Tiempo de administración:		10 minutos	
Normas de aplicación:		El encuestador deberá seleccionar una solo opción de cada pregunta, dependiendo de su opinión y lo que considere correcto.	
Escala:		Escala de Likert	
Descripción	Valor		
Nunca	1		
Casi nunca	2		
A veces	3		
Casi siempre	4		
Siempre	5		
Niveles Variable Independiente	Rango	Niveles Variable Dependiente	Rango
No óptimo	18 – 42	Baja prevalencia	18 – 42
Regular	43 – 67	Media prevalencia	43 – 67
Óptimo	68 - 90	Alta prevalencia	68 - 90

Validez

Para realizar la validez del instrumento de investigación, se está realizando un juicio de experto los cuales serán evaluados por personal calificado, los cuales son expertos en el tema y cumplen con los requisitos para evaluar el instrumento (Ver anexo 4). De esta manera, Hernández y Mendoza (2018), menciona que la validez de un instrumento es la manera en cómo se busca medir las variables, lo demuestra cuando el instrumento escogido evidencia los conceptos teóricos de las variables.

Tabla 4

Validación del instrumento de recolección de datos

DNI	Grado académico, apellidos y nombres	Institución donde labora	Calificación
45914991	Mgtr. Roque Quezada, Juan Carlos Ezequiel	Universidad Ricardo Palma	Aplicable
09656793	Dr. Lezama Gonzales, Pedo Martin	Universidad César Vallejo	Aplicable
42097456	Dr. Acuña Benítez, Marlon Frank	Universidad César Vallejo	Aplicable

Confiabilidad

De acuerdo con Hernández y Mendoza (2018), menciona que la confiabilidad es el grado en donde un instrumento de investigación obtiene resultados realistas para demostrar el objetivo de la investigación. Es por esta razón, que se utilizará el programa llamado IBM SPSS Statistics donde se aplicará el cálculo estadístico Alfa de Cronbach, de esta manera se busca precisar la confiabilidad del instrumento. De acuerdo a la prueba piloto, donde se realizó unos 20 cuestionarios y se obtuvo el valor de 0.783 del coeficiente Alfa de Cronbach, de modo parecido para la prueba general donde se aplicó las 375 encuestas de la muestra se obtuvo el 0.801 del Alfa de Cronbach. Donde Hernández y Mendoza (2018) nos menciona que va entre el 0 y el 1, en donde si el resultado obtenido se acerca a uno o tiene un rango mínimo de 0.70, se puede decir que los resultados son confiables.

Tabla 5

Confiablidad del instrumento de recolección de datos

Tipo de Aplicación	N° de encuestas	N° de Items	Alfa de Cronbach
Piloto	20	36	0,783
General	375	36	0,801

3.5. Procedimientos

Para poder conseguir los resultados estadísticos, se preparó en primer lugar se elaboró un instrumento para la recolección de datos. En segundo lugar, se escogió a tres expertos los cuales se encargaron de validar el instrumento, de esta manera se consiguió un grado alto de validez para obtener datos confiables. En tercer lugar, se realizó analizó la confiabilidad del instrumento de recolección de datos de una prueba piloto de la muestra y luego se realizó la prueba real. Finalmente se obtuvo los resultados en una hoja de Microsoft Excel, para luego ser transportados al software IBM SPSS Statistics para obtener los resultados descriptivos e inferenciales.

3.6. Método de análisis de datos

Para reflejar la realidad se decidió utilizar un análisis de datos, de esta manera se cargó los datos que se obtuvieron gracias la encuesta realizada, donde posteriormente se utilizó el software IBM SPSS v.25 para conseguir los resultados para la base de este proyecto.

En nuestro análisis descriptivo, se utilizó tablas e histogramas de manera bidimensional para poder explicar los valores que se obtuvieron de nuestra muestra.

Por último, en el análisis inferencial se decidió utilizar un método paramétrico, donde se usó el coeficiente de regresión ordinal, para poder determinar de esta manera el grado de casualidad entre ambas variables.

3.7. Aspectos éticos

Para garantizar la seguridad e integridad de este estudio, se cumplió de manera honesta los estándares éticos que establece la Universidad César Vallejo, los cuales están expuestos en la Resolución de Consejo Universitario N°0262-2020/UCV, en donde expresa que la información que se está manejando debe de ser transparente, concisa y veraz.

Durante esta investigación se cumplieron el principio de transparencia, en el cual toda información brindada pueda ser replicada para comprobar su validez y confianza. Del mismo modo, el principio de la responsabilidad, en donde se acepta cualquier consecuencia que pueda ser derivada al momento de realizar la investigación del presente estudio. Y finalmente, el principio de probidad, por el cual se busca demostrar de manera honesta, resultados fidedignos sin ninguna modificación sin previa autorización de un comité de ética.

De igual manera, de acuerdo a la Ley N° 29733, llamada Ley de Protección de Datos Personales, explica que tiene el objetivo de asegurar como su mismo nombre lo dice la de proteger toda información personal que ha sido recopilada en esta investigación cumpliendo que ha sido recolectada de manera veraz y su uso solo será en esta investigación. Para esta investigación se respetó el anonimato de cada participante que respondió la encuesta de este estudio.

IV. RESULTADOS

Análisis descriptivos.

Análisis descriptivo de la Variable ciberseguridad y la Variable prevención de ataques cibernéticos.

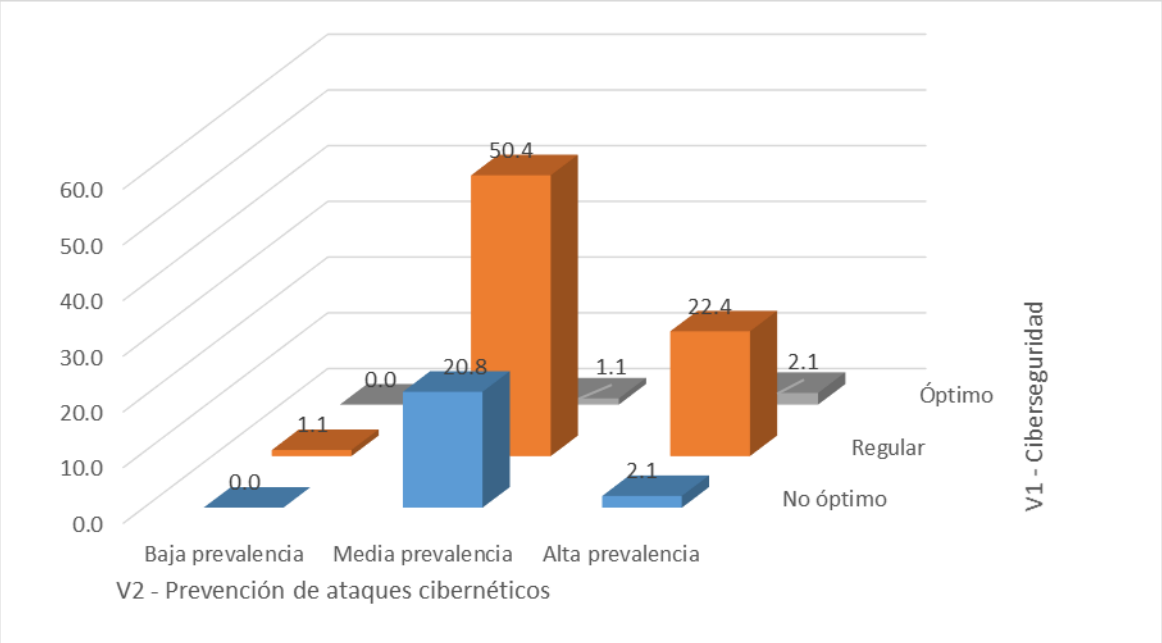
Tabla 6

Cruce de las tablas de las variables ciberseguridad y prevención de ataques cibernéticos

		V2 - Prevención ataques cibernéticos			
		Baja prevalencia	Media prevalencia	Alta prevalencia	Total
V1- Ciberseguridad	No óptimo	0 (0.0%)	78 (20.8%)	8 (2.1%)	86 (22.9%)
	Regular	4 (1.1%)	189 (50.4%)	84 (22.4%)	277 (73.9%)
	Óptimo	0 (0.0%)	4 (1.1%)	8 (2.1%)	12 (3.2%)
	Total	4 (1.1%)	271 (72.3%)	100 (26.7%)	375 (100.0%)

Figura 1.

Barras cruzadas de las variables ciberseguridad y prevención de ataques cibernéticos



De acuerdo a la tabla 6 podemos observar que el índice de frecuencia con la aprobación más alta se encuentra entre el nivel “Media prevalencia” de la variable Prevención de ataques cibernéticos con el nivel “Regular” de la variable Ciberseguridad, con 375 respuestas, el cual representa el 50,4% de todas las respuestas. Así mismo, el índice de frecuencia con la menor aprobación se encuentra entre el nivel “Baja prevalencia” de la variable Prevención de ataques cibernéticos con el nivel “No óptimo” de la variable Ciberseguridad, el cual representa el 0% de todas las respuestas. Podemos observar que en la figura 1, el nivel “Regular” es el que contiene el índice de frecuencia con la aprobación más alta, con 375 respuestas en donde representa el 72.3%.

Análisis descriptivo de la Variable ciberseguridad y la dimensión detección de vulnerabilidades de la Variable prevención de ataques cibernéticos.

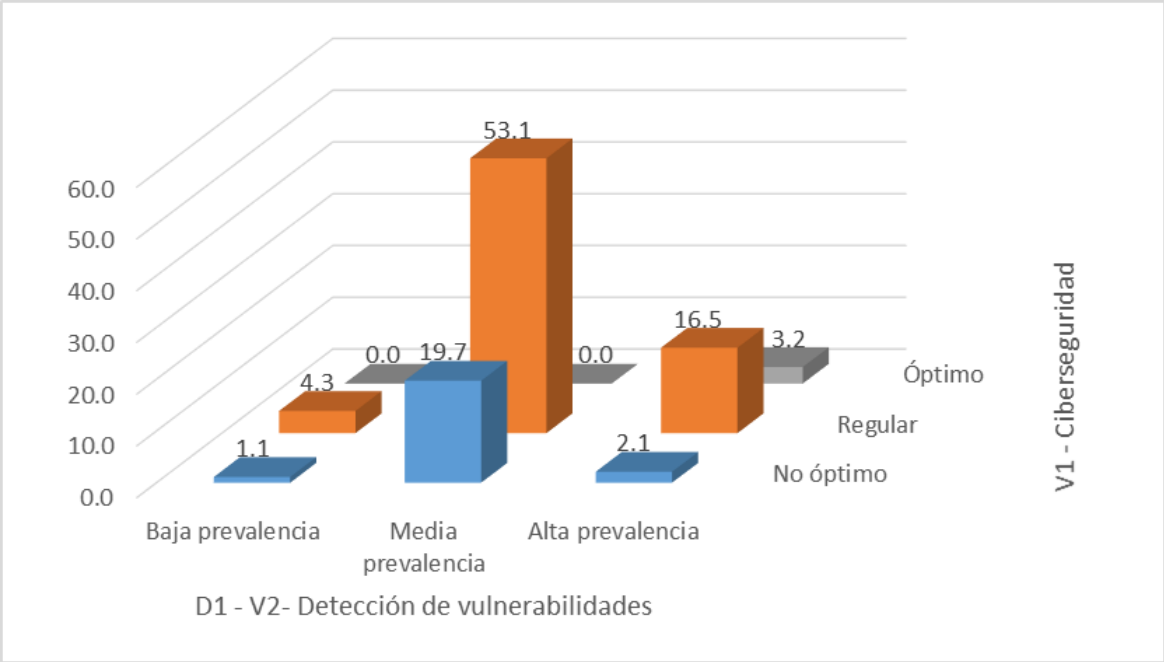
Tabla 7

Cruce de tablas de la variable ciberseguridad y la dimensión detección de vulnerabilidades de la variable prevención de ataques cibernéticos

		D1 - V2 - Detección de vulnerabilidades			
		Baja prevalencia	Media prevalencia	Alta prevalencia	Total
V1- Ciberseguridad	No óptimo	4 (1.1%)	74 (19.7%)	8 (2.1%)	86 (22.9%)
	Regular	16 (4.3%)	199 (53.1%)	62 (16.5%)	277 (73.9%)
	Óptimo	0 (0.0%)	0 (0.0%)	12 (3.2%)	12 (3.2%)
	Total	20 (5.3%)	273 (72.8%)	82 (21.9%)	375 (100.0%)

Figura 2.

Barras cruzadas de la variable ciberseguridad y la dimensión detección de vulnerabilidades de la variable prevención de ataques cibernéticos



De acuerdo a la tabla 7 podemos observar que el índice de frecuencia con la aprobación más alta se encuentra entre el nivel “Media prevalencia” de la dimensión Detección de vulnerabilidades con el nivel “Regular” de la variable Ciberseguridad, con 375 respuestas, el cual representa el 53,1% de todas las respuestas. Así mismo, el índice de frecuencia con la menor aprobación se encuentra entre el nivel “Baja prevalencia” de la dimensión Detección de vulnerabilidades con el nivel “No óptimo” de la variable Ciberseguridad, el cual representa el 1.1% de todas las respuestas. Podemos observar que en la figura 2, el nivel “Regular” es el que contiene el índice de frecuencia con la aprobación más alta, con 375 respuestas en donde representa el 72.8%.

Análisis descriptivo de la Variable ciberseguridad y la dimensión prevención de robo de información de la Variable prevención de ataques cibernéticos.

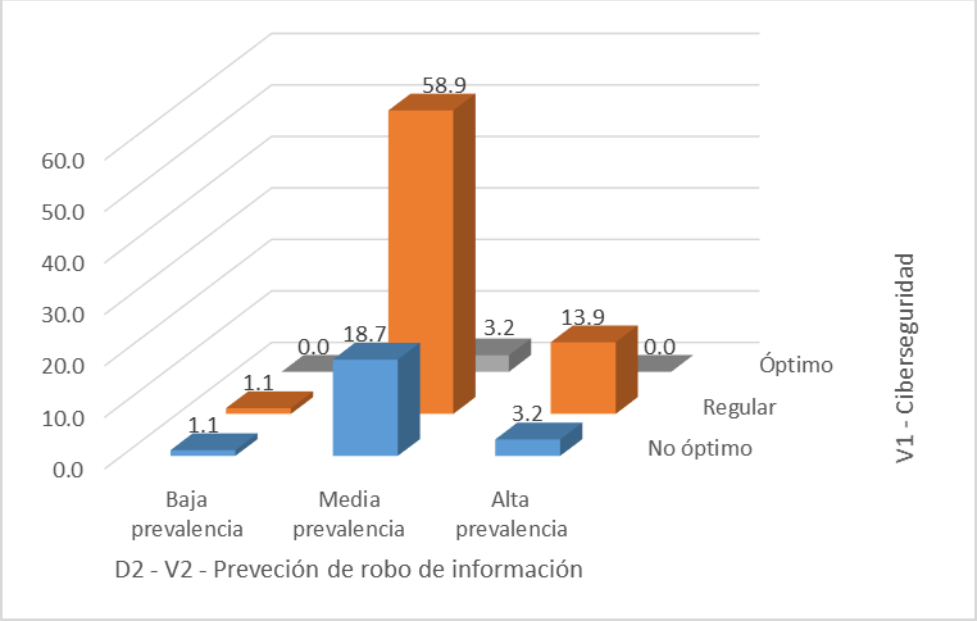
Tabla 8

Cruce de tablas de la variable ciberseguridad y la dimensión prevención de robo de información de la variable prevención de ataques cibernéticos

		D2 - V2-Prevencion de robo de información			
		Baja prevalencia	Media prevalencia	Alta prevalencia	Total
V1-Ciberseguridad	No óptimo	4 (1.1%)	70 (18.7%)	12 (3.2%)	86 (22.9%)
	Regular	4 (1.1%)	221 (58.9%)	52 (13.9%)	277 (73.9%)
	Óptimo	0 (0.0%)	12 (3.2%)	0 (0.0%)	12 (3.2%)
	Total	8 (2.1%)	303 (80.8%)	64 (17.1%)	375 (100.0%)

Figura 3.

Barras cruzadas de la variable ciberseguridad y la dimensión prevención de robo de información de la variable prevención de ataques cibernéticos



De acuerdo a la tabla 8 podemos observar que el índice de frecuencia con la aprobación más alta se encuentra entre el nivel “Media prevalencia” de la dimensión Prevención de robo de información con el nivel “Regular” de la variable Ciberseguridad, con 375 respuestas, el cual representa el 58,9% de todas las

respuestas. Así mismo, el índice de frecuencia con la menor aprobación se encuentra entre el nivel “Baja prevalencia” de la dimensión Prevención de robo de información con el nivel “No óptimo” de la variable Ciberseguridad, el cual representa el 1.1% de todas las respuestas. Podemos observar que en la figura 3, el nivel “Regular” es el que contiene el índice de frecuencia con la aprobación más alta, con 375 respuestas en donde representa el 80.8%.

Análisis descriptivo de la Variable ciberseguridad y la dimensión identificación de tipos de ciberataques de la Variable prevención de ataques cibernéticos

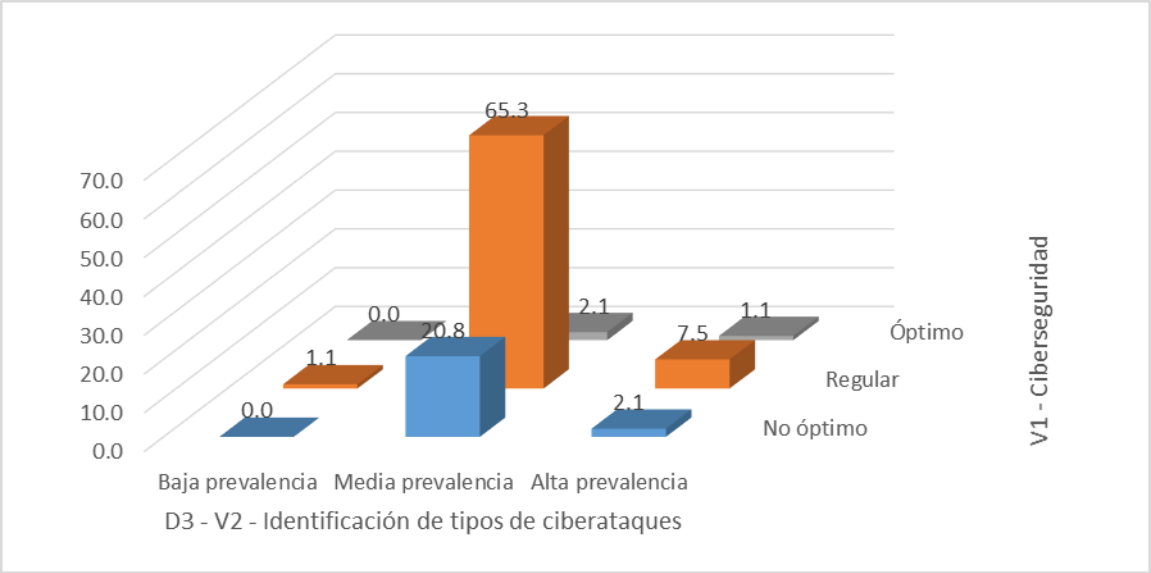
Tabla 9.

Cruce de tablas de la variable ciberseguridad y la dimensión identificación de tipos de ciberataques de la variable prevención de ataques cibernéticos

		D3- V2-Identificación de tipos de ciberataques			
		Baja prevalencia	Media prevalencia	Alta prevalencia	Total
V1- Ciberseguridad	No óptimo	0 (0.0%)	78 (20.8%)	8 (2.1%)	86 (22.9%)
	Regular	4 (1.1%)	245 (65.3%)	28 (7.5%)	277 (73.9%)
	Óptimo	0 (0.0%)	8 (2.1%)	4 (1.1%)	12 (3.2%)
	Total	4 (1.1%)	331 (88.3%)	40 (10.7%)	375 (100.0%)

Figura 4.

Barras cruzadas de la variable ciberseguridad y la dimensión identificación de tipos de ciberataques de la variable prevención de ataques cibernéticos



De acuerdo a la tabla 9 podemos observar que el índice de frecuencia con la aprobación más alta se encuentra entre el nivel “Media prevalencia” de la dimensión Identificación de tipos de ciberataques con el nivel “Regular” de la variable Ciberseguridad, con 375 respuestas, el cual representa el 65,3% de todas las respuestas. Así mismo, el índice de frecuencia con la menor aprobación se encuentra entre el nivel “Baja prevalencia” de la dimensión Identificación de tipos de ciberataques con el nivel “No óptimo” de la variable Ciberseguridad, el cual representa el 0% de todas las respuestas. Podemos observar que en la figura 4, el nivel “Regular” es el que contiene el índice de frecuencia con la aprobación más alta, con 375 respuestas en donde representa el 88.2%.

Análisis Inferencial

Para el desarrollo del análisis inferencial se buscó establecer el impacto entre las dos variables y las dimensiones, por el cual, de acuerdo a Montes, et al. (2021) menciona los rangos y su relación donde 0.01 a 0.10 es débil, 0.11 a 0.50 es media, 0.51 a 0.75 es considerable, 0.76 a 0.90 es fuerte y 0.91 a 1.00 es perfecta.

Para el desarrollo de esta investigación se utilizó una regresión logística ordinal, de acuerdo a Hernández y Mendoza (2018), nos menciona que a partir de un modelo estadístico busca la manera de obtener los resultados o el efecto que tiene la variable independiente con la variable dependiente. Logit y Cloglog son las funciones más utilizadas, para el desarrollo de esta investigación se utilizó la primera opción, debido tienen datos ordinales y están distribuidas normalmente.

Prueba de Hipótesis

Prueba de Hipótesis General:

H_1: La ciberseguridad impacta significativamente en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022.

H_0: La ciberseguridad no impacta significativamente en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022.

Tabla 10

Modelo de ajustes para la variable prevención de ataques cibernéticos

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	45,220			
Final	22,109	23,111	2	0,000

En primer lugar, se comprueba el valor sig, como podemos observar en la tabla 10, se obtuvo un valor de 0,000, el cual es menor a 0,05, es decir que el modelo se ajusta para un análisis ordinal.

Tabla 11

Ajuste de bondad del impacto de la variable ciberseguridad en la variable prevención de ataques cibernéticos

	Chi-cuadrado	gl	Sig.
Pearson	4,716	2	0,095
Desvianza	6,247	2	0,044

En la tabla 11, se puede observar que en el Chi-cuadrado de Pearson se obtuvo un valor de 0.095, el cual es mayor a 0.05, da a entender que los datos obtenidos se ajustan al modelo y son consistentes.

Tabla 12

Coeficiente R cuadrado para la variable prevención de ataques cibernéticos

Coeficiente R^2	Valor
Cox y Snell	0,060
Nagelkerke	0,083
McFadden	0,048

Podemos observar que en la tabla 12, se obtuvieron resultados bajos en los tres valores que nos describe el coeficiente de R cuadrado, dándonos a determinar que existe un impacto entre las variables. Así mismo, escogemos el valor de Nagelkerke debido a que tienen los valores más exactos, donde se obtuvo un valor de 0,083 en donde en porcentaje es un 8,3%, donde podemos determinar que el valor obtenido es el impacto de la variable ciberseguridad con la variable prevención de ataques cibernéticos, dándonos a entender que existe una relación débil, debido a que se encuentra entre 0,01 y 0,10.

Tabla 13

Estimación paramétrica del impacto de la variable ciberseguridad en la variable Prevención de ataques cibernéticos.

		Estimación	Desv. Error	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[V2 = 1]	-6,493	0,807	64,696	1	0,000	-8,075	-4,911
	[V2 = 2]	-,695	0,612	1,290	1	0,256	-1,896	,505
Ubicación	[V1=1]	-2.743	0,693	15,692	1	0,000	-4,105	-1,388
	[V1=2]	-1,552	0,626	6,143	1	0,013	-2,779	-,325

Podemos observar en la tabla 13, el coeficiente de regresión estimado de la variable independiente (ciberseguridad) se ha obtenido un -2,742, así mismo, se ha obtenido una sig. del 0,000 y un coeficiente de acuerdo a la población (Wald) mayor a 15, dicho esto se considera que existe un impacto de la variable ciberseguridad con la variable prevención de ataques cibernéticos.

Por lo que luego de aplicar una regresión logística ordinal, se consiguió un nivel de sig. de 0,000, en donde es menor al 0,05 el cual representa el error significativo, donde podemos evidenciar que se rechaza la hipótesis nula (H_0), dando a entender que la ciberseguridad impacta significativamente en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022.

Prueba de Hipótesis especifica 1:

H_1: La ciberseguridad impacta significativamente en la dimensión detección de vulnerabilidades en los adultos mayores en el distrito de Jesús María, Lima 2022.

H_0: La ciberseguridad no impacta significativamente en la dimensión detección de vulnerabilidades en el distrito de Jesús María, Lima 2022.

Tabla 14

Modelo de ajustes para la dimensión detección de vulnerabilidades

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	63,936			
Final	21,391	42,545	2	0,000

En primer lugar, se comprueba la sig. estadística, como podemos observar en la tabla 14, se obtuvo un valor de 0,000, el cual es menor a 0,05, es decir que el modelo se ajusta para un análisis ordinal.

Tabla 15

Ajuste de bondad del impacto de la variable ciberseguridad en la dimensión detección de vulnerabilidades

	Chi-cuadrado	gl	Sig.
Pearson	3,814	2	0,149
Desvianza	4,079	2	0,130

En la tabla 15, se puede observar que en el Chi-cuadrado de Pearson se obtuvo un valor de 0.149, el cual es mayor a 0.05, da a entender que los datos obtenidos se ajustan al modelo y son consistentes.

Tabla 16

Coeficiente R cuadrado para la dimensión detección de vulnerabilidades

Coeficiente R^2	Valor
Cox y Snell	0,107
Nagelkerke	0,141
McFadden	0,079

Podemos observar que en la tabla 16, se obtuvieron resultados bajos en los tres valores que nos describe el coeficiente de R cuadrado, dándonos a determinar que existe un impacto entre las variables. Así mismo, escogemos el valor de Nagelkerke debido a que tienen los valores más exactos, donde se obtuvo un valor de 0,141 en

donde en porcentaje es un 14,1%, donde podemos determinar que el valor obtenido es el impacto de la variable ciberseguridad con la variable prevención de ataques cibernéticos, dándonos a entender que existe una relación media, debido a que se encuentra entre 0,11 y 0,50.

Tabla 17

Estimación paramétrica del impacto de la variable ciberseguridad en la dimensión detección de vulnerabilidades

		Estimación	Desv. Error	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[V2D1 = 1]	-22,053	0,252	7,645,404	1	0,000	-22,547	-21,558
	[V2D1 = 2]	-17,723	0,143	15,254,094	1	0,000	-18,004	-17,441
Ubicación	[V1=1]	-19,646	0,301	4,252,882	1	0,000	-20,237	-19,056
	[V1=2]	-19,022	0,000	.	1	.	-19,022	-19,022

Podemos observar en la tabla 17, el coeficiente de regresión estimado de la variable independiente (ciberseguridad) se ha obtenido un -19,646, así mismo, se ha obtenido una sig. del 0,000 y un coeficiente de acuerdo a la población (Wald) se obtuvo un valor elevado, dicho esto se considera que existe un impacto de la variable ciberseguridad con la dimensión detección de vulnerabilidades.

Por lo que luego de aplicar una regresión logística ordinal, se consiguió un nivel de sig. de 0,000, en donde es menor al 0,05 el cual representa el error significativo, donde podemos evidenciar que se rechaza la hipótesis nula (H_0), dando a entender que la ciberseguridad impacta significativamente en la dimensión detección de vulnerabilidades en los adultos mayores en el distrito de Jesús María, Lima 2022.

Prueba de Hipótesis especifica 2:

H_1: La ciberseguridad impacta significativamente en la dimensión prevención de robo de información en los adultos mayores en el distrito de Jesús María, Lima 2022.

H_0: La ciberseguridad no impacta significativamente en la dimensión prevención de robo de información en el distrito de Jesús María, Lima 2022.

Tabla 18

Modelo de ajustes para la dimensión prevención de robo de información

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	24,965			
Final	20588	4,377	2	0,112

En primer lugar, se comprueba la sig. estadística, como podemos observar en la tabla 18, se obtuvo un valor de 0,112, el cual es mayor a 0,05, es decir que el modelo no se ajusta para un análisis ordinal.

Tabla 19

Ajuste de bondad del impacto de la variable ciberseguridad en la dimensión prevención de robo de información

	Chi-cuadrado	gl	Sig.
Pearson	3,070	2	0,215
Desvianza	4,359	2	0,113

En la tabla 19, se puede observar que en el Chi-cuadrado de Pearson se obtuvo un valor de 0.215, el cual es mayor a 0.05, da a entender que los datos obtenidos se ajustan al modelo y son consistentes.

Tabla 20

Coeficiente R cuadrado para la dimensión prevención de robo de información

Coeficiente R^2	Valor
Cox y Snell	0,012
Nagelkerke	0,017
McFadden	0,010

Podemos observar que en la tabla 20, se obtuvieron resultados bajos en los tres valores que nos describe el coeficiente de R cuadrado, dándonos a determinar que existe un impacto entre las variables. Así mismo, escogemos el valor de Nagelkerke

debido a que tienen los valores más exactos, donde se obtuvo un valor de 0,017 en donde en porcentaje es un 1,7%, donde podemos determinar que el valor obtenido es el impacto de la variable ciberseguridad con la variable prevención de ataques cibernéticos, dándonos a entender que existe una relación baja, debido a que se encuentra entre 0,01 y 0,10.

Tabla 21

Estimación paramétrica del impacto de la variable ciberseguridad en la dimensión prevención de robo de información

		Estimación	Desv. Error	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[V2D2 = 1]	-2,744	0,904	9,206	1	0,002	-4,516	-,971
	[V2D2 = 2]	2,744	0,904	9,206	1	0,002	0,971	4,516
Ubicación	[V1=1]	0,782	0,941	0,692	1	0,406	-1,061	2,626
	[V1=2]	1,294	0,910	2,022	1	0,155	-,489	3,078

Podemos observar en la tabla 21, el coeficiente de regresión estimado de la variable independiente (ciberseguridad) se ha obtenido un 1,294, así mismo, se ha obtenido una sig. del 0,155 y un coeficiente de acuerdo a la población (Wald) es mayor a 2, dicho esto se considera que no existe un impacto de la variable ciberseguridad con la dimensión prevención de robo de información.

Por lo que luego de aplicar una regresión logística ordinal, se consiguió un nivel de sig. de 0,155, en donde es mayor al 0,05 el cual representa el error significativo, donde podemos evidenciar que se rechaza la hipótesis alterna (H_1), dando a entender que la ciberseguridad no impacta significativamente en la dimensión prevención de robo de información en los adultos mayores en el distrito de Jesús María, Lima 2022.

Prueba de Hipótesis especifica 3:

H_1: La ciberseguridad impacta significativamente en la dimensión identificación de tipos de ciberataques en los adultos mayores en el distrito de Jesús María, Lima 2022.

H_0: La ciberseguridad no impacta significativamente en la identificación de tipos de ciberataques en el distrito de Jesús María, Lima 2022.

Tabla 22

Modelo de ajustes para la dimensión identificación de tipos de ciberataques

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	22,117			
Final	17313	4,804	2	0,091

En primer lugar, se comprueba la sig. estadística, como podemos observar en la tabla 22, se obtuvo un valor de 0,091, el cual es mayor a 0,05, es decir que el modelo no se ajusta para un análisis ordinal.

Tabla 23

Ajuste de bondad del impacto de la variable ciberseguridad en la dimensión identificación de tipos de ciberataques

	Chi-cuadrado	gl	Sig.
Pearson	1,374	2	0,503
Desvianza	2,286	2	0,319

En la tabla 23, se puede observar que en el Chi-cuadrado de Pearson se obtuvo un valor de 0.503, el cual es mayor a 0.05, da a entender que los datos obtenidos se ajustan al modelo y son consistentes.

Tabla 24

Coeficiente R cuadrado para la dimensión identificación de tipos de ciberataques

Coeficiente R^2	Valor
Cox y Snell	0,013
Nagelkerke	0,023
McFadden	0,016

Podemos observar que en la tabla 24, se obtuvieron resultados bajos en los tres valores que nos describe el coeficiente de R cuadrado, dándonos a determinar que existe un impacto entre las variables. Así mismo, escogemos el valor de Nagelkerke debido a que tienen los valores más exactos, donde se obtuvo un valor de 0,023 en donde en porcentaje es un 2,3%, donde podemos determinar que el valor obtenido es el impacto de la variable ciberseguridad con la variable prevención de ataques cibernéticos, dándonos a entender que existe una relación baja, debido a que se encuentra entre 0,01 y 0,10.

Tabla 25

Estimación paramétrica del impacto de la variable ciberseguridad en la dimensión identificación de tipos de ciberataques

		Estimación	Desv. Error	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[V2D3 = 1]	-6,026	0,803	56,261	1	0,000	-7,601	-4,451
	[V2D3 = 2]	0,686	0,610	1,264	1	0,261	-,510	1,882
Ubicación	[V1=1]	-1,483	0,700	4,487	1	0,034	-2,855	-,111
	[V1=2]	-1,534	0,642	5,710	1	0,017	-2,792	-,276

Podemos observar en la tabla 25, el coeficiente de regresión estimado de la variable independiente (ciberseguridad) se ha obtenido un -1,534, así mismo, se ha obtenido una sig. del 0,017 y un coeficiente de acuerdo a la población (Wald) es mayor a 5, dicho esto se considera que existe un impacto de la variable ciberseguridad con la dimensión prevención de robo de información.

Por lo que luego de aplicar una regresión logística ordinal, se consiguió un nivel de sig. de 0,017, en donde es menor al 0,05 el cual representa el error significativo, donde podemos evidenciar que se rechaza la hipótesis nula (H_0), dando a entender que la ciberseguridad impacta significativamente en la dimensión identificación de tipos de ciberataques en los adultos mayores en el distrito de Jesús María, Lima 2022.

V. DISCUSIÓN

Con respecto al objetivo general de la presente investigación, procederemos a discutir los resultados que se ha obtenido en relación a la ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores en el distrito Jesús María, Lima 2022.

De acuerdo en el análisis descriptivo, se pudo determinar que en el nivel “Media prevalencia” de la variable dependiente prevención de ataques cibernéticos el cual está asociado al nivel regular de la variable independiente, ciberseguridad representa el 50.4%. Por otro lado, en el nivel “Baja prevalencia” de la variable dependiente prevención de ataques cibernéticos con el nivel “No óptimo” de la variable independiente ciberseguridad, representa el 0.0%. Y finalmente en el nivel “Alta prevalencia” de la variable dependiente prevención de ataques cibernéticos con el nivel “Regular” de la variable independiente ciberseguridad, representa el 22.4%.

De acuerdo en el análisis inferencial, se pudo determinar que, siguiendo el modelo de regresión logística ordinal, es relevante debido a que en la primera prueba donde se realizó el ajuste de los modelos, se obtuvo una sig., cuyo valor fue de 0.000 el cual es menor al 0.05. Así mismo, de acuerdo al Chi-cuadrado de Pearson, cuyo valor fue de 0.095 que es mayor a 0.05. Luego, de acuerdo al Pseudo R cuadrado de Nagelkerke, el valor que se obtuvo fue de 8.3%, el cual nos indica y explica la varianza existe entre la variable independiente ciberseguridad y la variable dependiente prevención de ataques cibernéticos. Finalmente, luego de aplicar nuestro coeficiente estadístico, regresión logística ordinal, el valor obtenido fue -2 742 y el de sig. fue de 0.000 siendo este último menor a 0.05, por consiguiente, se afirma que la ciberseguridad si impacta en la prevención de ataques cibernéticos.

Con respecto a lo ya mencionado, a los resultados obtenidos de la investigación, Aliaga (2021), en su investigación una implementación de un sistema de seguridad

ayudo en gran medida de manera positiva con la prevención de ataques cibernéticos en la empresa radiadores fortaleza. De igual manera, Bohorquez (2021) en su investigación la ciberseguridad demostró relacionarse con la gestión de tecnologías de información en una empresa eléctrica. Así mismo, Medina (2021) en su investigación demostró que hay una correlación entre el teletrabajo y la gestión de seguridad de la información, en donde si se utiliza más el teletrabajo, habrá un aumento en la gestión de seguridad de la información. De este modo, Camargo (2020) en su investigación determina que la ciberseguridad y el teletrabajo tuvo un gran impacto durante la pandemia COVID-19 y repercutió en cómo se manejó las distintas aplicaciones y normas para resguardar la información de una empresa y de los usuarios.

Según lo mencionado anteriormente, están relacionados con la variable independiente ciberseguridad el cual según Poma y Vargas (2019) La ciberseguridad es un mecanismo el cual permite en varios casos prevenir que los usuarios sean víctimas de robo de información, así como su identidad, y esta información sea utilizadas para fines inapropiados. Y la variable dependiente prevención de ataques cibernéticos el cual según Lehu (2018) el ciberataque consta de una acción que puede ser tanto como individual como colectiva, donde el objetivo es recabar información de la integridad de un sistema de información de una persona, empresa u organización, utilizando las tecnologías y la red de manera total o parcial para realizar estos actos. los mismos que se fundamentan en la Teoría General de Sistemas (T.G.S) el cual según Ossa (2017), donde explica de manera amplia que la T.G.S., es el estudio de los sistemas de manera interdisciplinaria, que busca aplicar los principios en cualquier sistema.

Con respecto al objetivo específico uno de la presente investigación, procederemos a discutir los resultados que se ha obtenido con respecto a la ciberseguridad y su impacto en la dimensión detección de vulnerabilidades en los adultos mayores en el distrito Jesús María, Lima 2022.

De acuerdo al análisis descriptivo, se pudo determinar que en el nivel “Media prevalencia” de la dimensión detección de vulnerabilidades de la variable dependiente prevención de ataques cibernéticos el cual está asociado al nivel regular de la variable independiente, ciberseguridad representa el 53.1%. Por otro lado, en el nivel “Baja prevalencia” de la dimensión detección de vulnerabilidades de la variable dependiente prevención de ataques cibernéticos con el nivel “No óptimo” de la variable independiente ciberseguridad, representa el 1.1%. Y finalmente en el nivel “Alta prevalencia” de la dimensión detección de vulnerabilidades de la variable dependiente prevención de ataques cibernéticos con el nivel “Regular” de la variable independiente ciberseguridad, representa el 16.5%.

De acuerdo al análisis inferencial, se pudo determinar que, siguiendo el modelo de regresión logística ordinal, es relevante debido a que en la primera prueba donde se realizó el ajuste de los modelos, se obtuvo una sig., cuyo valor fue de 0.000 el cual es menor al 0.05. Así mismo, de acuerdo al Chi-cuadrado de Pearson, cuyo valor fue de 0.149 que es mayor a 0.05. Luego, de acuerdo al Pseudo R cuadrado de Nagelkerke, el valor que se obtuvo fue de 14.1%, el cual nos indica y explica la varianza existe entre la variable independiente ciberseguridad y la dimensión detección de vulnerabilidades de la variable dependiente prevención de ataques cibernéticos. Finalmente, luego de aplicar nuestro coeficiente estadístico, regresión logística ordinal, el valor obtenido fue -19 646 y el de sig. fue de 0.000 siendo este último menor a 0.05, por consiguiente, se afirma que la ciberseguridad si impacta en la dimensión detección de vulnerabilidades de la prevención de ataques cibernéticos.

Con respecto a lo ya mencionado a los resultados obtenidos de la investigación, Díaz (2018) en su investigación determina mediante la dimensión confiabilidad de la variable seguridad informática equivale el 40%. De la misma manera, Morales (2020) en su investigación coincide que el uso de la normativa que fue utilizada en la investigación protege la privacidad de las personas, de esta manera evitando que sean objetivos vulnerables. Así mismo, Fritzvold (2017), en su investigación

determina que la detección de vulnerabilidades en sistemas digitales aún se relaciona a factores humanos.

Según lo mencionado anteriormente, están relacionados con la variable independiente ciberseguridad el cual según Poma y Vargas (2019) La ciberseguridad es un mecanismo el cual permite en varios casos prevenir que los usuarios sean víctimas de robo de información, así como su identidad, y esta información sea utilizadas para fines inapropiados. Y la dimensión detección de vulnerabilidades de la variable dependiente prevención de ataques cibernéticos el cual, según Kara, et al. (2022) un método para detectar las vulnerabilidades es realizar test de seguridad usando redes físicas reales, sin embargo, es costoso y requiere un tiempo de coste demasiado alto, y como contiene información crítica, se recomienda modelar y simular diferentes métodos, de esta forma nos acerca a resultados parecido a los casos reales. Los mismos que se fundamentan en la Teoría General de Sistemas (T.G.S) el cual según Ossa (2017), donde explica de manera amplia que la T.G.S., es el estudio de los sistemas de manera interdisciplinaria, que busca aplicar los principios en cualquier sistema.

Con respecto al objetivo específico dos de la presente investigación, procederemos a discutir los resultados que se ha obtenido con respecto a la ciberseguridad y su impacto en la dimensión prevención de robo de información en los adultos mayores en el distrito Jesús María, Lima 2022.

De acuerdo al análisis descriptivo, se pudo determinar que en el nivel “Media prevalencia” de la dimensión prevención de robo de información de la variable dependiente prevención de ataques cibernéticos el cual está asociado al nivel regular de la variable independiente, ciberseguridad representa el 58.9%. Por otro lado, en el nivel “Baja prevalencia” de la dimensión prevención de robo de información de la variable dependiente prevención de ataques cibernéticos con el nivel “No óptimo” de la variable independiente ciberseguridad, representa el 1.1%. Y finalmente en el nivel “Alta prevalencia” de la dimensión prevención de robo de

información de la variable dependiente prevención de ataques cibernéticos con el nivel “Regular” de la variable independiente ciberseguridad, representa el 13.9%.

De acuerdo al análisis inferencial, se pudo determinar que, siguiendo el modelo de regresión logística ordinal, no es relevante debido a que en la primera prueba donde se realizó el ajuste de los modelos, se obtuvo una sig., cuyo valor fue de 0.112 el cual es mayor al 0.05. Así mismo, de acuerdo al Chi-cuadrado de Pearson, cuyo valor fue de 0.215 que es mayor a 0.05. Luego, de acuerdo al Pseudo R cuadrado de Nagelkerke, el valor que se obtuvo fue de 1.7%, el cual nos indica y explica la varianza no existe entre la variable independiente ciberseguridad y la variable dependiente prevención de ataques cibernéticos. Finalmente, luego de aplicar nuestro coeficiente estadístico, regresión logística ordinal, el valor obtenido fue 1 294 y el de sig. fue de 0.406 siendo este último mayor a 0.05, por consiguiente, se afirma que la ciberseguridad no impacta en la prevención de ataques cibernéticos.

Con respecto a lo ya mencionado a los resultados obtenidos de la investigación, Anchundia-Betancourt (2017), en su investigación determina que el factor de la globalización con el incremento del desarrollo de nuevas tecnologías trae beneficios, pero igual llevan consigo retos en la seguridad, protección y privacidad de datos. De igual manera, Bernashvili (2017) en su investigación determina que una forma para desarrollar defensas para los ciberataques y prevenir el robo de información debe de existir un equipo de voluntarios y que de desarrolle un establecimiento que se dedique a estas tareas.

Según lo mencionado anteriormente, están relacionados con la variable independiente ciberseguridad el cual según Poma y Vargas (2019) La ciberseguridad es un mecanismo el cual permite en varios casos prevenir que los usuarios sean víctimas de robo de información, así como su identidad, y esta información sea utilizadas para fines inapropiados. Y la dimensión prevención de robo de información de la variable dependiente prevención de ataques cibernéticos el cual según Campbell (2016), para prevenir el robo de información requiere el

esfuerzo de todos para que funcione, donde se debe de enseñar a cada empleado lo básicos de la ciberseguridad como, por ejemplo: no utilizar contraseñas simples, no conectar tu teléfono personal a una computadora de la empresa. Los mismos que se fundamentan en la Teoría General de Sistemas (T.G.S) el cual según Ossa (2017), donde explica de manera amplia que la T.G.S., es el estudio de los sistemas de manera interdisciplinaria, que busca aplicar los principios en cualquier sistema.

Con respecto al objetivo específico tres de la presente investigación, procederemos a discutir los resultados que se ha obtenido con respecto a la ciberseguridad y su impacto en la dimensión identificación de tipos de ciberataques en los adultos mayores en el distrito Jesús María, Lima 2022.

De acuerdo al análisis descriptivo, se pudo determinar que en el nivel “Media prevalencia” de la dimensión identificación de tipos de ciberataques de la variable dependiente prevención de ataques cibernéticos el cual está asociado al nivel regular de la variable independiente, ciberseguridad representa el 65.3%. Por otro lado, en el nivel “Baja prevalencia” de la dimensión identificación de tipos de ciberataques de la variable dependiente prevención de ataques cibernéticos con el nivel “No óptimo” de la variable independiente ciberseguridad, representa el 0.0%. Y finalmente en el nivel “Alta prevalencia” de la dimensión identificación de tipos de ciberataques de la variable dependiente prevención de ataques cibernéticos con el nivel “Regular” de la variable independiente ciberseguridad, representa el 7.5%.

De acuerdo al análisis inferencial, se pudo determinar que, siguiendo el modelo de regresión logística ordinal, no es relevante debido a que en la primera prueba donde se realizó el ajuste de los modelos, se obtuvo una sig., cuyo valor fue de 0.091 el cual es mayor al 0.05. Así mismo, de acuerdo al Chi-cuadrado de Pearson, cuyo valor fue de 0.503 que es mayor a 0.05. Luego, de acuerdo al Pseudo R cuadrado de Nagelkerke, el valor que se obtuvo fue de 2.3%, el cual nos indica y explica la varianza que no existe entre la variable independiente ciberseguridad y la variable dependiente prevención de ataques cibernéticos. Finalmente, luego de aplicar

nuestro coeficiente estadístico, regresión logística ordinal, el valor obtenido fue -1 534 y el de sig. fue de 0.017 menor siendo este último menor a 0.05, por consiguiente, se afirma que la ciberseguridad si impacta en la prevención de ataques cibernéticos.

Con respecto a lo ya mencionado a los resultados obtenidos de la investigación, Choejey (2018) en su investigación determina que existe varios factores que dificultan para realizar las prácticas básicas de la ciberseguridad siendo uno de estas la capacitación y concientización para que de esta manera se pueda proteger de los ciberataques. De la misma manera, Fritzvold (2017), en su investigación determina que personal especializado van a donde los usuarios y/o empleados y los capacita para poder reconocer e identificar debilidades dentro de los sistemas.

Según lo mencionado anteriormente, están relacionados con la variable independiente ciberseguridad el cual según Poma y Vargas (2019) La ciberseguridad es un mecanismo el cual permite en varios casos prevenir que los usuarios sean víctimas de robo de información, así como su identidad, y esta información sea utilizadas para fines inapropiados. Y la dimensión identificación de tipos de ciberataques de la variable dependiente prevención de ataques cibernéticos el cual según Pyke, et al. (2021), nos menciona como en la identificación de tipos de ataques también interviene el conocimiento de los usuarios sobre los ciberataques y cómo manejarlo es un factor que impacta en la susceptibilidad de estos, así mismo ellos toman la ventaja de la baja habilidad de los humanos para detectar o reconocer las señales de los diferentes tipos de ciberataques. Los mismos que se fundamentan en la Teoría General de Sistemas (T.G.S) el cual según Ossa (2017), donde explica de manera amplia que la T.G.S., es el estudio de los sistemas de manera interdisciplinaria, que busca aplicar los principios en cualquier sistema.

Con respecto a la metodología que se utilizó en la presente investigación, nos permitió fortalecerla, debido a que es de tipo básica, en donde se estudió la

problemática presentada, en base a conocimientos, es decir, se recolectó información de diferentes autores para determinar las variables, dimensiones y teorías escogidas. Para el desarrollo de esta investigación no se requirió una aplicación práctica para poder comprobar los objetivos propuestos. De esta manera, al ser de un diseño no experimental, permitió realizar un análisis y descripción de ambas variables y la relación que existe entre estas sin la necesidad de realizar ningún cambio.

De igual manera, el uso de un cuestionario de manera online, como instrumento de datos, permitió obtener la información requerida, pese al contexto actual de la pandemia, de la cual ha sido desarrollada esta investigación, debido a que fue fueron desarrolladas sin importar la hora y el lugar. Sin embargo, una dificultad fue llegar a la muestra de la investigación, debido a que muchos adultos mayores no manejan muy bien la tecnología.

Finalmente, sobre la relevancia social de esta investigación proporcionó los conocimientos necesarios y brindó la realidad en la que viven los adultos mayores con respecto a la ciberseguridad y el impacto en la prevención de ataques cibernéticos. De la misma manera, esta investigación puede ser aplicada en diferentes distritos o ampliarla a nivel Lima Metropolitana.

VI. CONCLUSIONES

Primero La ciberseguridad alcanzó un valor de estimación de -2 743 y el de sig. de 0.000 en la prueba Wald, de esta manera, se concluye que la ciberseguridad impacta significativamente en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022. Además, con los valores obtenidos de Nagelkerke fue de 8.3% en donde existe una relación débil.

Segundo La ciberseguridad alcanzó un valor de estimación de -19 646 y el de sig. de 0.000 en la prueba Wald, de esta manera, se concluye que la ciberseguridad impacta significativamente en la dimensión detección de vulnerabilidades en los adultos mayores en el distrito de Jesús María, Lima 2022. Además, con los valores obtenidos de Nagelkerke fue de 14.1% en donde existe una relación media.

Tercero La ciberseguridad alcanzó un valor de estimación de 1 294 y el de sig. de 0.155 en la prueba Wald, de esta manera, se concluye que la ciberseguridad no impacta significativamente en la dimensión prevención de robo de información en los adultos mayores en el distrito de Jesús María, Lima 2022. Además, con los valores obtenidos de Nagelkerke fue de 1.37% en donde existe una relación baja.

Cuarto La ciberseguridad alcanzó un valor de estimación de -1 534 y el de sig. 0.017 en la prueba de Wald, de esta manera, se concluye que la ciberseguridad impacta significativamente en la dimensión identificación de tipos de ciberataques en los adultos mayores en el distrito de Jesús María, Lima 2022. Además, con los valores obtenidos de Nagelkerke fue de 2.3% en donde existe una relación baja.

VII. RECOMENDACIONES

Primero Con el propósito de que mejore la ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores del distrito de Jesús María, se recomienda al área llamada “Casa del Adulto Mayor” del distrito de Jesús María proponer unas clases de capacitación a los adultos mayores para darles a conocer las ventajas sobre la ciberseguridad de manera didáctica y sencilla, así de esta manera enseñarles cómo prevenir los ataques cibernéticos.

Segundo Con el propósito de que mejore la ciberseguridad y su impacto en la dimensión detección de vulnerabilidades en los adultos mayores del distrito de Jesús María, se recomienda al área llamada “Casa del Adulto Mayor” del distrito de Jesús María proponer realizar un análisis en profundidad para detectar que edad es la más vulnerable para ser víctima de ataques cibernéticos.

Tercero Con el propósito de que mejore la ciberseguridad y su impacto en la prevención de robo de información en los adultos mayores del distrito de Jesús María, se recomienda al área llamada “Casa del Adulto Mayor” del distrito de Jesús María proponer desarrollar boletines mensuales o semanales en donde informen de manera sencilla que pasos utilizar para proteger la información del usuario.

Cuarto Con el propósito de que mejore la ciberseguridad y su impacto en la identificación de tipos de ciberataques en los adultos mayores del distrito de Jesús María, se recomienda al área llamada “Casa del Adulto Mayor” del distrito de Jesús María proponer desarrollar boletines mensuales o semanales en donde informen de manera sencilla los casos más comunes de ciberataques y como defenderse de ellos y que acciones tomar.

REFERENCIAS

Alharbi, F., Alsulami, M., AL-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia. Sensors, 21(20), 6901. Extraído de: https://doi.org/10.3390/s21206901

Aliaga, C. (2021). Implementación de un Sistema de ciberseguridad para la prevención de los ataques cibernéticos en la Empresa Radiadores Fortaleza, 2021. Universidad César Vallejo. Extraído de: https://repositorio.ucv.edu.pe/handle/20.500.12692/70776

Anatolii, L., Spartak, H., Mykola, Y., Maksym, T., Nataliya, M., & Volodymyr, S. (2021). Development of the Concept of Cybersecurity of the Organization. TEM Journal, 1447-1453. Extraído de: https://doi.org/10.18421/TEM103-57

Anchundia-Betancourt, C. (2017). Ciberseguridad en los sistemas de información de las universidades. Revista Científica Dominio de las ciencias, 3, 200-217. Extraído de: http://dominiodelasciencias.com/ojs/index.php/es/index.

Astorga, C., & Schmidt, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. Revista Electrónica Educare, 23(3), 1-24. Extraído de: https://doi.org/10.15359/ree.23-3.17

Avci, İ. (2021). Investigation of Cyber-Attack Methods and Measures in Smart Grids. Sakarya University Journal of Science, 25(4), 1061–1074. Extraído de: https://doi.org/10.16984/saufenbilder.955914

Bernashvili, I. (2017). The Impact of Cybercrime and Legal Frameworks of volunteers in Cybersecurity: Case of Georgia. Tallinn University of Technology. Extraído de: https://digikogu.taltech.ee/en/Download/ad236629e73d4efdbf1bb19a8e5cd063

Bohorquez, A. (2021). Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020. Universidad César Vallejo. Extraído de: https://repositorio.ucv.edu.pe/handle/20.500.12692/63128

Camargo, L. (2020). Ciberseguridad y Teletrabajo en tiempos de COVID-19. Universidad del Rosario. Extraído de: https://repository.urosario.edu.co/handle/10336/25394

Campbell, C. (2016). Protect your System from Cyberattacks! Opflow, American Water Works Association - Cybersecurity, 42(8), 8-11. Extraído de: https://doi.org/10.5991/OPF.2016.42.0045

Cangea, O. (2018). Ethical Hacking Solution to Defeat Cyber Attacks. Petroleum - Gas University of Ploiesti Bulletin, Technical Series, 70(2), 29–36. Extraído de: https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=136232 619&lang=es&site=eds-live

Cando-Segovia, M., & Medina-Chicaiza, P. (2021). Prevención en ciberseguridad: Enfocada a los procesos de infraestructura tecnológica. 3C TIC: Cuadernos de desarrollo aplicados a las TIC, 10(1), 17-41. Extraído de: https://doi.org/10.17993/3ctic.2021.101.17-41

Cano, J., & Rocha, A. (2019). Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital. RISTI - Revista Ibérica de Sistemas e Tecnologías de Información, 32, VII-IX. Extraído de: https://doi.org/10.17013/risti.32.0

Carlini, A. (2016). Ciberseguridad: Un nuevo desafío para la comunidad internacional. 67, 16. Extraído de: https://dialnet.unirioja.es/servlet/articulo?codigo=5998287

Choejey, P. (2018). Cybersecurity Challanges and Practices: A Case Study of Bhutan. Murdoch University. Extraído de: https://researchrepository.murdoch.edu.au/id/eprint/42353/

Chuquilla, A., Guarda, T., & Ninahualpa, G. (2019). Ransomware—WannaCry Security is everyone's. 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), 1-4. Extraído de: https://doi.org/10.23919/CISTI.2019.8760749

Dalal, R., Howard, D., Bennett, R., Posey, C., Zaccaro, S., & Brummel, B.(2022). Organizational science and cybersecurity: abundant opportunities for research at the interface. Journal of Business & Psychology, 37(1), 1–29. Extraído de: https://doi.org/10.1007/s10869-021-09732-9

Das, R., & Gündüz, M. (2019). Analysis of Cyber-Attacks in IoT-based Critical Infrastructures. 13. Extraído de: http://ijiss.org/ijiss/index.php/ijiss/article/view/490

Díaz, R. (2018). La auditoría informática y la seguridad de la información en el área de sistemas de la caja del Santa, Chimbote-2018. Universidad Privada del Norte. Extraído de: https://repositorio.upn.edu.pe/handle/11537/13870

Domínguez, V., & López, M. (2019). Teoría General de Sistemas, un enfoque práctico. TECNOCIENCIA Chihuahua, 10(3), 125-132. Extraído de: https://vocero.uach.mx/index.php/tecnociencia/article/view/174

Especial Directivos (2020). Diez medidas para protegerse de los ciberataques en tiempos del COVID-19. 1775, 55–57. Extraído de: https://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=142529946&lang=es&site=eds-live

Fritzvold, E. (2017), Cyber Security in Organizations. Universitetet i Stavanger. Extraído de: https://uis.brage.unit.no/uis-xmlui/handle/11250/2460083

García, V. (2019). ¿Cómo Está Avanzando La Ciberseguridad en El Perú? Breve Aproximación Al Marco Normativo. Actualidad Jurídica (1578-956X), 52, 176–179. Extraído de: https://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=142290641&lang=es&site=eds-live

Gómez, G., & López, J. (2019). Adaptación de la teoría de la información para el régimen de propagación lineal de una red óptica DWDM de próxima generación. Lámpsakos, 22, 27-36. Extraído de: https://doi.org/10.21501/21454086.3127

Hernández, S. (2020). Teoría general de sistemas aplicada al diseño arquitectónico sustentable. Legado De Arquitectura Y Diseño, 3(4), 55-66. Extraído de: https://legadodearquitecturaydiseno.uaemex.mx/article/view/13756

Hernández-Sampieri, R., & Mendoza, C. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. ISBN 978-1-4562-6096-5. Extraído de: http://repositorio.uasb.edu.bo:8080/handle/54000/1292

Ignaczak, L., Goldschmidt, G., Costa, C., & Righi, R. (2022). Text Mining in Cybersecurity: A Systematic Literature Review. ACM Computing Surveys, 54(7), 1-36. Extraído de: https://doi.org/10.1145/3462477

Instituto Nacional de Estadística e Informática (INEI) (2019). Compendio Estadístico Provincia de Lima 2019. Extraído de: https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1714/Libro.pdf

Kara, S., Hizal, S., & Zengin, A. (2022). Design and Implementation of a DEVS-Based Cyber-Attack Simulator for Cyber Security. International Journal of Simulation Modelling, 21(1), 53-64. Extraído de: https://doi.org/10.2507/IJSIMM21-1-587

Kotenko, I., Saenko, I., Lauta, O., & Karpov, M. (2021). Methodology for Management of the Protection System of Smart Power Supply Networks in the Context of Cyberattacks. Energies, 14(18), 5963. Extraído de: https://doi.org/10.3390/en14185963

Lehu, J. (2018). Cyberattaque: La gestion du risque est-elle encore possible?: Analyse et enseignements du cas Sony Pictures. La Revue des Sciences de Gestion, 291-292(3), 41. Extraído de: https://doi.org/10.3917/rsg.291.0041

Lecklider, T. (2017). Defending against cyberattacks. EE-Evaluation Engineering, 56(3), 14+. Extraído de: https://link.gale.com/apps/doc/A490622837/AONE?u=anon~1f0252f1&sid=googleScholar&xid=c0b50518

López, C., & Lombardi, O. (2015). Información clásica e información cuántica: ¿dos tipos de información? Scientiae Studia, v. 13, n. 1, pp. 143-174. Extraído de: https://doi.org/10.1590/S1678-31662015000100007. ISSN 1678-3166.

Machado, A. (2016). Teoría de la Información más que una teoría matemática. e-ikon (3), 4, 29-32. Extraído de: https://app.eam.edu.co/ojs/index.php/eikon/article/view/119/225

Machín, N., & Gazapo, M. (2016). La Ciberseguridad como factor crítico en la Seguridad de la Unión Europea. Revista UNISCI, 0(42), 47-67. Extraído de: https://doi.org/10.5209/RUNI.53786

Maldonado, C. (2017). Ciencia hecha realidad. Innovar Revista de Ciencias Administrativas y Sociales, 27(64), 157-159. ISSN: 0121-5051. Extraído de: https://doi.org/10.15446/innovar.v27n64.62377

Marcos A. (2018) ¿Qué entendemos por información?, Investigación y Ciencia (edición española de Scientific American), septiembre, pp. 54-55. ISSN: 0210136X. Extraído de: http://www.fyl.uva.es/~wfilosof/webMarcos/

Matheu, S., Hernández-Ramos, J., Skarmeta, A., & Baldini, G. (2020). A Survey of Cybersecurity Certification for the Internet of Things. ACM Computing Surveys, 53(6), 1–36. Extraído de: https://doi.org/10.1145/3410160

Medina, R. (2021). Teletrabajo y la gestión de seguridad de la información en la empresa Infoservicios, Lima - 2020. Universidad César Vallejo. Extraído de: https://repositorio.ucv.edu.pe/handle/20.500.12692/60728

Mendivil, J., Sanz, B., & Gutierrez, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: Una revisión sistemática de literatura. Pixel-Bit, Revista de Medios y Educación, 63, 197-225. Extraído de: https://doi.org/10.12795/pixelbit.91640

Montes, A., Ochoa, J., Juárez, B., Vázquez, M., & Díaz, L. (2021). Aplicación del coeficiente de correlación de Spearman en un estudio de fisioterpia. 4.

Extraído de: https://www.fcfm.buap.mx/SIEP/2021/Extensos%20Carteles/Extenso%20Juliana.pdf

Morales, E. (2020). Uso de tecnologías de información y comunicaciones en la seguridad ciudadana del distrito de Santiago de Surco. Universidad César Vallejo. Lima, Perú. Extraído de: https://repositorio.ucv.edu.pe/handle/20.500.12692/52559

Networks Asia (2015). The case for security as a service to protect against cyberattacks in a hybrid world. 12(1), 20–21. Best DDOS Protection - F5 Networks. Extraído de: https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=110086520&lang=es&site=eds-live

Networks Asia (2018). What is a cyber-attack? Recent examples show disturbing trends. 1–N.PAG. Extraído de: https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=128438593&lang=es&site=eds-live

Ossa, C. (2016). Teoría General de Sistemas: Conceptos y aplicaciones. Universidad Tecnológica de Pereira. Extraído de: https://doi.org/10.22517/9789587222289

Padilla, E. (2017). Tips to Prevent, Detect & Respond to Cyberattacks: How Safe Is Your Firmware? IESE Insight, 33, 31-37. Extraído de: https://doi.org/10.15581/002.ART-3014

Patino, G. (2021). Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos. OASIS, 34, 107-126. Extraído de: https://doi.org/10.18601/16577558.n34.07

Peralta, E. (2016). Teoría general de los sistemas aplicada a modelos de gestión. Aglala, 7(1), 122–145. ISSN 2215-7360 Extraído de: https://doi.org/10.22519/22157360.901

Pichihua, S. (2021). Cada mes hay más de 300 denuncias por delitos informáticos. *Agencia de Noticias Andina.* Extraído de: https://andina.pe/agencia/noticia-cada-mes-hay-mas-300-denuncias-delitos-informaticos-830617.aspx

Poma, A., & Vargas, R. (2019). Problematic in cybersecurity as protection of computer system and social networks in Peru and the World. SCIÉNDO, 22(4), 275-282. Extraído de: https://doi.org/10.17268/sciendo.2019.034

Pons, V. (2017). Internet, la nueva era del delito: Ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity. URVIO - Revista Latinoamericana de Estudios de Seguridad, 20, 80. Extraído de: https://doi.org/10.17141/urvio.20.2017.2563

Protek (2022). 12 estadísticas de ciberseguridad para 2022. Seguridad Informática. Paraguay. Extraído de: https://www.protek.com.py/novedades/estadisticas-de-ciberseguridad/#:~:text=Se%20estima%20que%20aproximadamente%20el,la%20pandemia%20del%20COVID-19

Pyke, A., Rovira, E., Murray, S., Pritts, J., Carp, C., & Thomson, R. (2021). Predicting individual differences to cyber-attacks: Knowledge, arousal, emotional and trust responses. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 15(4). Extraído de: https://doi.org/10.5817/CP2021-4-9

Sánchez, H., Reyes, C., Mejía, K. (2018) Manual de términos de investigación científica, tecnológica y humanística. Universidad Ricardo Palma. ISBN N° 978-612-47351-4-1. Extraído de: http://repositorio.urp.edu.pe/handle/URP/1480

Scozzina, E. (2020). Teoría de la información y codificación: El significado de la entropía en la transmisión de información. Extensionismo, Innovación y Transferencia Tecnológica, 6(0), 208-218. Extraído de: https://doi.org/10.30972/eitt.604394

ANEXOS

Anexo 1: Matriz de Consistencia

TÍTULO: Ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores del distrito de Jesús María , Lima 2022

AUTOR: Saldaña Diaz, Mauricio Nicolas

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES
Problema principal: ¿De qué manera la ciberseguridad impacta en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022? **Problemas específicos:** PE1: ¿De qué manera la ciberseguridad impacta en la dimensión detección de vulnerabilidades en los adultos mayores en el distrito de Jesús María, Lima 2022? PE2: ¿De qué manera la ciberseguridad impacta en la dimensión prevención de robo de información de los adultos mayores en el distrito de Jesús María, Lima 2022?	**Objetivo principal:** Determinar el impacto de la ciberseguridad en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022. **Objetivos específicos:** OE1: Determinar el impacto de la ciberseguridad en la dimensión detección de vulnerabilidades en los adultos mayores en el distrito de Jesús María, Lima 2022. OE2: Determinar el impacto de la ciberseguridad en la dimensión prevención de robo de información de los adultos mayores en el distrito de Jesús María, Lima 2022.	**Hipótesis principal:** La ciberseguridad impacta significativamente en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022. **Hipótesis específicas:** HE1: La ciberseguridad impacta significativamente en la dimensión detección de vulnerabilidades en los adultos mayores en el distrito de Jesús María, Lima 2022. HE2: La ciberseguridad impacta significativamente en la dimensión prevención de robo de información de los adultos mayores en el distrito de Jesús María, Lima 2022.	**Variable - Independiente:** Ciberseguridad

Dimensiones	Indicadores	Ítems	Niveles
Confidencialidad de la información	Privacidad	1 – 2	No óptimo
	Acceso	3 – 4	
	Proteger	5 – 6	Regular
Integridad de la información	Confiabilidad	7 – 8	
	Conformidad	9 – 10	Óptimo
	Consistencia	11 – 12	
Disponibilidad de la información	Acceso	13 – 14	
	Prevención	15 – 16	
	Seguridad	17 – 18	

Variable - Dependiente: Prevención de ataques cibernéticos

Dimensiones	Indicadores	Ítems	Niveles
Detección de vulnerabilidades	Anticipación	19 – 20	Baja prevalencia
	Confiabilidad	21 – 22	
	Mejora	23 – 24	Media prevalencia
	Anticipación	25 – 26	

TÍTULO: Ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores del distrito de Jesús María , Lima 2022

AUTOR: Saldaña Diaz, Mauricio Nicolas

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
PE3: ¿De qué manera la ciberseguridad impacta en la dimensión identificación de tipos de ciberataques en los adultos mayores en el distrito de Jesús María, Lima 2022?	OE3: Determinar el impacto de la ciberseguridad en la dimensión identificación de tipos de ciberataques en los adultos mayores en el distrito de Jesús María, Lima 2022. .	HE3: La ciberseguridad impacta significativamente en la dimensión identificación de tipos de ciberataques en los adultos mayores en el distrito de Jesús María, Lima 2022. .	Prevención de robo de información	Confiabilidad	27 – 28	Alta prevalencia
				Integridad	29 – 30	
			Identificación de tipos de ciberataques	Amenazas	31 – 32	
				Conocimiento	33 – 34	
				Protección	35 – 36	

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Básica **Diseño:** No Experimental	**Población:** 16,535 habitantes adultos mayores **Tamaño de muestra:** 375 habitantes **Muestreo:** No probabilístico del tipo simple	**Técnicas:** Encuesta **Instrumentos:** Cuestionario	**Descriptiva:** En nuestro análisis descriptivo, se utilizó tablas e histogramas de manera bidimensional para poder explicar los valores que se obtuvieron de nuestra muestra **Inferencial:** En el análisis inferencial se utilizó un método paramétrico, donde se usó el coeficiente de análisis de regresión logística ordinal, para poder determinar de esta manera el grado de casualidad entre ambas variables.

Anexo 2: Matriz de Operacionalización de Variables

TÍTULO: Ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores del distrito de Jesús María, Lima 2022

AUTOR: Saldaña Díaz, Mauricio Nicolas

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Ciberseguridad Según Poma y Vargas (2019) La ciberseguridad es un mecanismo el cual permite en varios casos prevenir que los usuarios sean víctimas de robo de información, así como su identidad, y esta información sea utilizadas para fines inapropiados**.**	**Confidencialidad de la información** Según Cangea (2018) nos describe a la confidencialidad de la información una propiedad que se encarga de proteger y mantener a cualquier información a las personas autorizadas.	Privacidad	1	Frecuentemente se informa acerca de cómo mantener su información de manera privada.	No óptimo Regular Óptimo
			2	Frecuentemente se informa acerca de las reglas básicas para mantener su información de manera privada.	
		Acceso	3	Frecuentemente personas ajenas o en su entorno familiar tiene acceso a sus dispositivos electrónicos.	
			4	Frecuentemente utiliza los medios de seguridad que tiene sus dispositivos electrónicos, por ejemplo: el patrón, clave, etc.	
		Proteger	5	¿Cuenta con los conocimientos para realizar copias de seguridad de su información personal?	
			6	Frecuentemente utiliza elementos externos, como agendas, post-its para almacenar información personal como sus contraseñas, etc.	
	Integridad de la información Según Patino (2020), nos describe que tanto los sistemas como los datos no haya habido ningún cambio sin autorización previa.	Confiabilidad	7	Frecuentemente usted analiza cada información que lee en el internet.	
			8	Es una persona susceptible a creer toda la información que lee dentro del internet, como por ejemplo estos mensajes en cadena.	
		Conformidad	9	Frecuentemente usted filtra la información que recibe por los medios de comunicación.	
			10	Frecuentemente utiliza grupos de interés para asegurar la información.	
		Consistencia	11	Frecuentemente revisa su información personal para asegurar que no haya sido modificada.	
			12	¿Cuenta con los conocimientos para poder recuperar información que ha sido eliminada accidentalmente?	

TÍTULO: Ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores del distrito de Jesús María, Lima 2022

AUTOR: Saldaña Díaz, Mauricio Nicolas

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Disponibilidad de la información Según Cangea (2018), nos describe que se pueden utilizar los sistemas para recabar la información en cualquier momento que se tenga previsto	Acceso	13	¿Cuenta a su disposición mecanismos para reportar cualquier incidente ocurrido con su información personal?	
			14	¿Cuenta con mecanismos para recuperar su información ante cualquier inconveniente con respecto a su red?	
		Prevención	15	¿Cree usted que al momento de pedir tu información personal a cualquier entidad te identifican primero?	
			16	¿Cree usted que toda entidad cumple con los lineamientos, normas y/o estándares de seguridad para proteger su información personal a cualquier costa?	
		Seguridad	17	¿Implementa medios de seguridad para resguardar su información personal?	
			18	Frecuentemente recibe llamadas desconocidas o ataques informáticos que paralizan sus actividades.	
Prevención de ataques cibernéticos Según Lehu (2018) el ciberataque consta de una acción que puede ser tanto como individual como colectiva, donde el objetivo es recabar información de la integridad de un sistema de información de una persona, empresa u organización, utilizando las tecnologías y la red de manera total o parcial para realizar estos actos.	**Detección de vulnerabilidades** Según Kara, Hizal y Zengin (2022) un método para detectar las vulnerabilidades es realizar test de seguridad usando redes físicas reales, sin embargo, es costoso y requiere un tiempo de coste demasiado alto, y como contiene información crítica, se recomienda modelar y simular diferentes métodos, de esta forma nos acerca a resultados parecido a los casos reales.	Anticipación	19	¿Está de acuerdo en utilizar programas para detectar diferentes ataques cibernéticos?	Baja prevalencia Media prevalencia Ala prevalencia
			20	¿Cree usted que utilizar un generador de contraseñas ayuda a evitar el robo de información?	
		Confiabilidad	21	¿Cree que las empresas encargadas a la seguridad supervisan y previenen la pérdida o robo de información?	
			22	¿Cree que es importante aumentar los sistemas de seguridad cuando se realiza cualquier compra donde implique ingresar datos confidenciales?	
		Mejora	23	¿Cree que existe alguna oficina que se encargue netamente para la seguridad de información?	
			24	¿Cree usted que las empresas que brindan seguridad cuenta con personal enfocado para la protección de sus datos?	
	Prevención de robo de información	Anticipación	25	¿Está de acuerdo con el uso de programas para proteger la información en cualquier sistema?	

TÍTULO: Ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores del distrito de Jesús María, Lima 2022

AUTOR: Saldaña Díaz, Mauricio Nicolas

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Según Campbell (2016), para prevenir el robo de información requiere el esfuerzo de todos para que funcione, donde se debe de enseñar a cada empleado lo básicos de la ciberseguridad como, por ejemplo: no utilizar contraseñas simples, no conectar tu teléfono personal a una computadora de la empresa.		26	¿Está de acuerdo en cómo los medios nos informa sobre cómo actuar ante los ciberataques más comunes?	
		Confiabilidad	27	¿Cree que las empresas deben de realizar rigurosos procesos de selección para elegir a su personal en puntos de ventas?	
			28	¿Cree usted que las empresas resguardan su información de manera segura para evitar ser robada?	
		Integridad	29	¿Cree usted que todas las empresas tienen incorporado softwares de seguridad para evitar ataques cibernéticos?	
			30	¿Cree usted que incorpora medidas de seguridad en donde no tenga información confidencial al alcance a terceros?	
	Identificación de tipos de ciberataques Según Pyke, Rovira, Murray, Pritts, Carp y Thomson (2021), nos menciona como en la identificación de tipos de ataques también interviene el conocimiento de los usuarios sobre los ciberataques y cómo manejarlo es un factor que impacta en la susceptibilidad de estos, así mismo ellos toman la ventaja de la baja habilidad de los humanos para detectar o reconocer las señales de los diferentes tipos de ciberataques.	Anticipación	31	¿Está de acuerdo a utilizar y/o comprar un antivirus en su computadora?	
			32	¿Cree usted que es susceptible a ser víctima de distintos robos de información?	
		Conocimiento	33	¿Cree usted que está capacitado para hacerle frente a los ciberataques?	
			34	¿Cree usted que está capacitado para identificar y diferenciar los distintos modos de robo de información más comunes?	
		Protección	35	¿Está de acuerdo a que el gobierno implemente un sistema que ayude a proteger tu información?	

TÍTULO: Ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores del distrito de Jesús María, Lima 2022

AUTOR: Saldaña Díaz, Mauricio Nicolas

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
			36	¿Está de acuerdo que se desarrolle un sistema que le informe y le ayude a identificar los robos de información más comunes y como protegerse de ellos?	

Anexo 3: Instrumento de Recolección de Datos

Cuestionario para usuarios del distrito de Jesús María

Fecha: [/ /] **Edad:** **Sexo:** [ ]

Instrucciones: Marque con un aspa la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo al siguiente **ejemplo**: Nunca (1), Casi Nunca (2), A veces (3), Casi siempre (4), Siempre (5) // Totalmente en desacuerdo (1), En desacuerdo (2), Ni de acuerdo ni en desacuerdo (3), De acuerdo (4) y Totalmente de acuerdo (5).

No	Pregunta	Valoración				
		1	2	3	4	5
	Sobre Ciberseguridad					
1	Frecuentemente se informa acerca de cómo mantener su información de manera privada.	Nunca	Casi nunca	A veces	Casi siempre	Siempre
2	Frecuentemente se informa acerca de las reglas básicas para mantener su información de manera privada.	Nunca	Casi nunca	A veces	Casi siempre	Siempre
3	Frecuentemente personas ajenas o en su entorno familiar tiene acceso a sus dispositivos electrónicos.	Nunca	Casi nunca	A veces	Casi siempre	Siempre
4	Frecuentemente utiliza los medios de seguridad que tiene sus dispositivos electrónicos, por ejemplo: el patrón, clave, etc.	Nunca	Casi nunca	A veces	Casi siempre	Siempre
5	¿Cuenta con los conocimientos para realizar copias de seguridad de su información personal?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
6	Frecuentemente utiliza elementos externos, como agendas, post-its para almacenar información personal como sus contraseñas, etc.	Nunca	Casi nunca	A veces	Casi siempre	Siempre
7	Frecuentemente usted analiza cada información que lee en el internet.	Nunca	Casi nunca	A veces	Casi siempre	Siempre
8	Es una persona susceptible a creer toda la información que lee dentro del internet, como por ejemplo estos mensajes en cadena.	Nunca	Casi nunca	A veces	Casi siempre	Siempre
9	Frecuentemente usted filtra la información que recibe por los medios de comunicación.	Nunca	Casi nunca	A veces	Casi siempre	Siempre
10	Frecuentemente utiliza grupos de interés para asegurar la información.	Nunca	Casi nunca	A veces	Casi siempre	Siempre
11	Frecuentemente revisa su información personal para asegurar que no haya sido modificada.	Nunca	Casi nunca	A veces	Casi siempre	Siempre

No	Pregunta	Valoración				
		1	2	3	4	5
12	¿Cuenta con los conocimientos para poder recuperar información que ha sido eliminada accidentalmente?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
13	¿Cuenta a su disposición mecanismos para reportar cualquier incidente ocurrido con su información personal?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
14	¿Cuenta con mecanismos para recuperar su información ante cualquier inconveniente con respecto a su red?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
15	¿Cree usted que al momento de pedir tu información personal a cualquier entidad te identifican primero?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
16	¿Cree usted que toda entidad cumple con los lineamientos, normas y/o estándares de seguridad para proteger su información personal a cualquier costa?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
17	¿Implementa medios de seguridad para resguardar su información personal?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
18	Frecuentemente recibe llamadas desconocidas o ataques informáticos que paralizan sus actividades.	Nunca	Casi nunca	A veces	Casi siempre	Siempre
	Sobre la prevención de ataques cibernéticos					
19	¿Está de acuerdo en utilizar programas para detectar diferentes ataques cibernéticos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
20	¿Cree usted que utilizar un generador de contraseñas ayuda a evitar el robo de información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
21	¿Cree que las empresas encargadas a la seguridad supervisan y previenen la pérdida o robo de información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
22	¿Cree que es importante aumentar los sistemas de seguridad cuando se realiza cualquier compra donde implique ingresar datos confidenciales?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
23	¿Cree que existe alguna oficina que se encargue netamente para la seguridad de información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
24	¿Cree usted que las empresas que brindan seguridad cuenta con personal enfocado para la protección de sus datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
25	¿Está de acuerdo con el uso de programas para proteger la información en cualquier sistema?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

No	Pregunta	Valoración				
		1	2	3	4	5
26	¿Está de acuerdo en cómo los medios nos informa sobre cómo actuar ante los ciberataques más comunes?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
27	¿Cree que las empresas deben de realizar rigurosos procesos de selección para elegir a su personal en puntos de ventas?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
28	¿Cree usted que las empresas resguardan su información de manera segura para evitar ser robada?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
29	¿Cree usted que todas las empresas tienen incorporado softwares de seguridad para evitar ataques cibernéticos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
30	¿Cree usted que incorpora medidas de seguridad en donde no tenga información confidencial al alcance a terceros?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
31	¿Está de acuerdo a utilizar y/o comprar un antivirus en su computadora?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
32	¿Cree usted que es susceptible a ser víctima de distintos robos de información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
33	¿Cree usted que está capacitado para hacerle frente a los ciberataques?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
34	¿Cree usted que está capacitado para identificar y diferenciar los distintos modos de robo de información más comunes?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
35	¿Está de acuerdo a que el gobierno implemente una normativa que ayude a proteger tu información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
36	¿Está de acuerdo que se desarrolle un sistema que le informe y le ayude a identificar los robos de información más comunes y como protegerse de ellos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

¡Gracias por su tiempo!

Anexo 4: Certificado de Validación del Instrumento de Recolección de Datos

Validación del Experto N°1

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: Ciberseguridad

Nº	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Confidencialidad de la información	Si	No	Si	No	Si	No	
1	Frecuentemente se informa acerca de cómo mantener su información de manera privada.	x		x		x		
2	Frecuentemente se informa acerca de las reglas básicas para mantener su información de manera privada.	x		x		x		
3	Frecuentemente personas ajenas o en su entorno familiar tiene acceso a sus dispositivos electrónicos.	x		x		x		
4	Frecuentemente utiliza los medios de seguridad que tiene sus dispositivos electrónicos, por ejemplo: el patrón, clave, etc.	x		x		x		
5	¿Cuenta con los conocimientos para realizar copias de seguridad de su información personal?	x		x		x		
6	Frecuentemente utiliza elementos externos, como agendas, post-its para almacenar información personal como sus contraseñas, etc.	x		x		x		
	Integridad de la información	Si	No	Si	No	Si	No	
7	Frecuentemente usted analiza cada información que lee en el internet	x		x		x		
8	Es una persona susceptible a creer toda la información que lee dentro del internet, como por ejemplo estos mensajes en cadena.	x		x		x		
9	Frecuentemente usted filtra la información que recibe por los medios de comunicación.	x		x		x		
10	Frecuentemente utiliza grupos de interés para asegurar la información.	x		x		x		
11	Frecuentemente revisa su información personal para asegurar que no haya sido modificada.	x		x		x		
12	¿Cuenta con los conocimientos para poder recuperar información que ha sido eliminada accidentalmente?	x		x		x		
	Disponibilidad de la información	Si	No	Si	No	Si	No	
13	¿Cuenta a su disposición mecanismos para reportar cualquier incidente ocurrido con su información personal?	x		x		x		
14	¿Cuenta con mecanismos para recuperar su información ante cualquier inconveniente con respecto a su red?	x		x		x		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
15	¿Cree usted que al momento de pedir tu información personal a cualquier entidad te identifican primero?	x		x		x		
16	¿Cree usted que toda entidad cumple con los lineamientos, normas y/o estándares de seguridad para proteger su información personal a cualquier costa?	x		x		x		
17	¿Implementa medios de seguridad para resguardar su información personal?	x		x		x		
18	Frecuentemente recibe llamadas desconocidas o ataques informáticos que paralizan sus actividades.	x		x		x		

/ARIABLE: Prevención de ataques cibernéticos

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Detección de vulnerabilidades	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Está de acuerdo en utilizar programas para detectar diferentes ataques cibernéticos?	x		x		x		
20	¿Cree usted que utilizar un generador de contraseñas ayuda a evitar el robo de información?	x		x		x		
21	¿Cree que las empresas encargadas a la seguridad supervisan y previenen la pérdida o robo de información?	x		x		x		
22	¿Cree que es importante aumentar los sistemas de seguridad cuando se realiza cualquier compra donde implique ingresar datos confidenciales?	x		x		x		
23	¿Cree que existe alguna oficina que se encargue netamente para la seguridad de información?	x		x		x		
24	¿Cree usted que las empresas que brindan seguridad cuenta con personal enfocado para la protección de sus datos?	x		x		x		
	Prevención de robo de información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Está de acuerdo con el uso de programas para proteger la información en cualquier sistema?	x		x		x		
26	¿Está de acuerdo en cómo los medios nos informa sobre cómo actuar ante los ciberataques más comunes?	x		x		x		
27	¿Cree que las empresas deben de realizar rigurosos procesos de selección para elegir a su personal en puntos de ventas?	x		x		x		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
28	¿Cree usted que las empresas resguardan su información de manera segura para evitar ser robada?	x		x		x		
29	¿Cree usted que todas las empresas tienen incorporado softwares de seguridad para evitar ataques cibernéticos?	x		x		x		
30	¿Cree usted que incorpora medidas de seguridad en donde no tenga información confidencial al alcance a terceros?	x		x		x		
	Identificación de tipos de ciberataques	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Está de acuerdo a utilizar y/o comprar un antivirus en su computadora?	x		x		x		
32	¿Cree usted que es susceptible a ser víctima de distintos robos de información?	x		x		x		
33	¿Cree usted que está capacitado para hacerle frente a los ciberataques?	x		x		x		
34	¿Cree usted que está capacitado para identificar y diferenciar los distintos modos de robo de información más comunes?	x		x		x		
35	¿Está de acuerdo a que el gobierno implemente una normativa que ayude a proteger tu información?	x		x		x		
36	¿Está de acuerdo que se desarrolle un sistema que le informe y le ayude a identificar los robos de información más comunes y como protegerse de ellos?	x		x		x		

Observaciones (precisar si hay suficiencia): EL PRESENTE INSTRUMENTO ES SUFICIENTE PARA MEDIR CONOCIMIENTO EN CIBERSEGURIDAD Y PREVENCION DE ATAQUES CIBERNETICOS

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ] 18 de MAYO del 2020

Apellidos y nombre s del juez evaluador: JUAN CARLOS ROQUE QUEZADA DNI: 45914991

Especialista: Metodólogo [X] Temático [ ]

Grado: Maestro [X] Doctor [ ]

[1] **Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia**: Si el ítem pertenece a la dimensión.
[3] **Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

Validación del Experto N°2

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: Ciberseguridad

Nº	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Confidencialidad de la información	Si	No	Si	No	Si	No	
1	Frecuentemente se informa acerca de cómo mantener su información de manera privada.	X		X		X		
2	Frecuentemente se informa acerca de las reglas básicas para mantener su información de manera privada.	X		X		X		
3	Frecuentemente personas ajenas o en su entorno familiar tiene acceso a sus dispositivos electrónicos.	X		X		X		
4	Frecuentemente utiliza los medios de seguridad que tiene sus dispositivos electrónicos, por ejemplo: el patrón, clave, etc.	X		X		X		
5	¿Cuenta con los conocimientos para realizar copias de seguridad de su información personal?	X		X		X		
6	Frecuentemente utiliza elementos externos, como agendas, post-its para almacenar información personal como sus contraseñas, etc.	X		X		X		
	Integridad de la información	Si	No	Si	No	Si	No	
7	Frecuentemente usted analiza cada información que lee en el internet	X		X		X		
8	Es una persona susceptible a creer toda la información que lee dentro del internet, como por ejemplo estos mensajes en cadena.	X		X		X		
9	Frecuentemente usted filtra la información que recibe por los medios de comunicación.	X		X		X		
10	Frecuentemente utiliza grupos de interés para asegurar la información.	X		X		X		
11	Frecuentemente revisa su información personal para asegurar que no haya sido modificada.	X		X		X		
12	¿Cuenta con los conocimientos para poder recuperar información que ha sido eliminada accidentalmente?	X		X		X		
	Disponibilidad de la información	Si	No	Si	No	Si	No	
13	¿Cuenta a su disposición mecanismos para reportar cualquier incidente ocurrido con su información personal?	X		X		X		
14	¿Cuenta con mecanismos para recuperar su información ante cualquier inconveniente con respecto a su red?	X		X		X		

Nº	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
15	¿Cree usted que al momento de pedir tu información personal a cualquier entidad te identifican primero?	X		X		X		
16	¿Cree usted que toda entidad cumple con los lineamientos, normas y/o estándares de seguridad para proteger su información personal a cualquier costa?	X		X		X		
17	¿Implementa medios de seguridad para resguardar su información personal?	X		X		X		
18	Frecuentemente recibe llamadas desconocidas o ataques informáticos que paralizan sus actividades.	X		X		X		

VARIABLE: Prevención de ataques cibernéticos

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Detección de vulnerabilidades	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Está de acuerdo en utilizar programas para detectar diferentes ataques cibernéticos?	X		X		X		
20	¿Cree usted que utilizar un generador de contraseñas ayuda a evitar el robo de información?	X		X		X		
21	¿Cree que las empresas encargadas a la seguridad supervisan y previenen la pérdida o robo de información?	X		X		X		
22	¿Cree que es importante aumentar los sistemas de seguridad cuando se realiza cualquier compra donde implique ingresar datos confidenciales?	X		X		X		
23	¿Cree que existe alguna oficina que se encargue netamente para la seguridad de información?	X		X		X		
24	¿Cree usted que las empresas que brindan seguridad cuenta con personal enfocado para la protección de sus datos?	X		X		X		
	Prevención de robo de información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Está de acuerdo con el uso de programas para proteger la información en cualquier sistema?	X		X		X		
26	¿Está de acuerdo en cómo los medios nos informa sobre cómo actuar ante los ciberataques más comunes?	X		X		X		
27	¿Cree que las empresas deben de realizar rigurosos procesos de selección para elegir a su personal en puntos de ventas?	X		X		X		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
28	¿Cree usted que las empresas resguardan su información de manera segura para evitar ser robada?	X		X		X		
29	¿Cree usted que todas las empresas tienen incorporado softwares de seguridad para evitar ataques cibernéticos?	X		X		X		
30	¿Cree usted que incorpora medidas de seguridad en donde no tenga información confidencial al alcance a terceros?	X		X		X		
	Identificación de tipos de ciberataques	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Está de acuerdo a utilizar y/o comprar un antivirus en su computadora?	X		X		X		
32	¿Cree usted que es susceptible a ser víctima de distintos robos de información?	X		X		X		
33	¿Cree usted que está capacitado para hacerle frente a los ciberataques?	X		X		X		
34	¿Cree usted que está capacitado para identificar y diferenciar los distintos modos de robo de información más comunes?	X		X		X		
35	¿Está de acuerdo a que el gobierno implemente una normativa que ayude a proteger tu información?	X		X		X		
36	¿Está de acuerdo que se desarrolle un sistema que le informe y le ayude a identificar los robos de información más comunes y como protegerse de ellos?	X		X		X		

Observaciones (precisar si hay suficiencia): EL PRESENTE INSTRUMENTO ES SUFICIENTE PARA MEDIR CONOCIMIENTO EN CIBERSEGURIDAD Y PREVENCION DE ATAQUES CIBERNETICOS

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

18 de mayo del 2020

Apellidos y nombre s del juez evaluador: **Lezama Gonzales, Pedro Martín** **DNI: 09656793**

Especialista: Metodólogo [x] **Temático [ ]**

Grado: Maestro [ ] **Doctor [x]**

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

Validación del Experto N°3

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: Ciberseguridad

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Confidencialidad de la información	Si	No	Si	No	Si	No	
1	Frecuentemente se informa acerca de cómo mantener su información de manera privada.	X		X		X		
2	Frecuentemente se informa acerca de las reglas básicas para mantener su información de manera privada.	X		X		X		
3	Frecuentemente personas ajenas o en su entorno familiar tiene acceso a sus dispositivos electrónicos.	X		X		X		
4	Frecuentemente utiliza los medios de seguridad que tiene sus dispositivos electrónicos, por ejemplo: el patrón, clave, etc.	X		X		X		
5	¿Cuenta con los conocimientos para realizar copias de seguridad de su información personal?	X		X		X		
6	Frecuentemente utiliza elementos externos, como agendas, post-its para almacenar información personal como sus contraseñas, etc.	X		X		X		
	Integridad de la información	Si	No	Si	No	Si	No	
7	Frecuentemente usted analiza cada información que lee en el internet	X		X		X		
8	Es una persona susceptible a creer toda la información que lee dentro del internet, como por ejemplo estos mensajes en cadena.	X		X		X		
9	Frecuentemente usted filtra la información que recibe por los medios de comunicación.	X		X		X		
10	Frecuentemente utiliza grupos de interés para asegurar la información.	X		X		X		
11	Frecuentemente revisa su información personal para asegurar que no haya sido modificada.	X		X		X		
12	¿Cuenta con los conocimientos para poder recuperar información que ha sido eliminada accidentalmente?	X		X		X		
	Disponibilidad de la información	Si	No	Si	No	Si	No	
13	¿Cuenta a su disposición mecanismos para reportar cualquier incidente ocurrido con su información personal?	X		X		X		
14	¿Cuenta con mecanismos para recuperar su información ante cualquier inconveniente con respecto a su red?	X		X		X		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
15	¿Cree usted que al momento de pedir tu información personal a cualquier entidad te identifican primero?	X		X		X		
16	¿Cree usted que toda entidad cumple con los lineamientos, normas y/o estándares de seguridad para proteger su información personal a cualquier costa?	X		X		X		
17	¿Implementa medios de seguridad para resguardar su información personal?	X		X		X		
18	Frecuentemente recibe llamadas desconocidas o ataques informáticos que paralizan sus actividades.	X		X		X		

VARIABLE: Prevención de ataques cibernéticos

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Detección de vulnerabilidades	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Está de acuerdo en utilizar programas para detectar diferentes ataques cibernéticos?	X		X		X		
20	¿Cree usted que utilizar un generador de contraseñas ayuda a evitar el robo de información?	X		X		X		
21	¿Cree que las empresas encargadas a la seguridad supervisan y previenen la pérdida o robo de información?	X		X		X		
22	¿Cree que es importante aumentar los sistemas de seguridad cuando se realiza cualquier compra donde implique ingresar datos confidenciales?	X		X		X		
23	¿Cree que existe alguna oficina que se encargue netamente para la seguridad de información?	X		X		X		
24	¿Cree usted que las empresas que brindan seguridad cuenta con personal enfocado para la protección de sus datos?	X		X		X		
	Prevención de robo de información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Está de acuerdo con el uso de programas para proteger la información en cualquier sistema?	X		X		X		
26	¿Está de acuerdo en cómo los medios nos informa sobre cómo actuar ante los ciberataques más comunes?	X		X		X		
27	¿Cree que las empresas deben de realizar rigurosos procesos de selección para elegir a su personal en puntos de ventas?	X		X		X		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
28	¿Cree usted que las empresas resguardan su información de manera segura para evitar ser robada?	X		X		X		
29	¿Cree usted que todas las empresas tienen incorporado softwares de seguridad para evitar ataques cibernéticos?	X		X		X		
30	¿Cree usted que incorpora medidas de seguridad en donde no tenga información confidencial al alcance a terceros?	X		X		X		
	Identificación de tipos de ciberataques	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Está de acuerdo a utilizar y/o comprar un antivirus en su computadora?	X		X		X		
32	¿Cree usted que es susceptible a ser víctima de distintos robos de información?	X		X		X		
33	¿Cree usted que está capacitado para hacerle frente a los ciberataques?	X		X		X		
34	¿Cree usted que está capacitado para identificar y diferenciar los distintos modos de robo de información más comunes?	X		X		X		
35	¿Está de acuerdo a que el gobierno implemente una normativa que ayude a proteger tu información?	X		X		X		
36	¿Está de acuerdo que se desarrolle un sistema que le informe y le ayude a identificar los robos de información más comunes y como protegerse de ellos?	X		X		X		

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

19 de mayo del 2022

Apellidos y nombre s del juez evaluador: Dr. Marlon Acuña Benites **DNI: 42097456**

Especialista: Metodólogo [ ] **Temático [x]**

Grado: Maestro [ ] **Doctor [x]**

[1] **Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia**: Si el ítem pertenece a la dimensión.
[3] **Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

Anexo 5: Base de datos

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	2	1	4	4	2	4	3	1	3	1	1	1	3	4	3	1	3	1	3	1	3	4	2	4	4	4	4	2	3	5	5	3	4	3	2	1	2	5
2	2	1	4	4	1	5	3	4	4	1	4	2	4	2	4	2	5	4	4	2	4	4	4	4	3	3	4	4	5	3	3	4	4	4	2	2	5	5
3	2	1	2	2	3	5	4	4	4	1	4	4	2	3	3	2	3	3	3	3	4	3	3	4	4	4	4	3	4	3	4	3	4	5	2	3	4	5
4	1	1	2	2	4	5	1	1	3	2	1	2	1	3	1	1	4	2	1	4	4	4	4	5	2	2	5	2	5	2	2	4	5	5	1	1	5	5
5	1	1	3	3	2	5	5	2	4	1	5	3	4	4	4	4	4	4	3	2	3	3	4	5	5	4	4	4	3	4	3	4	2	3	2	2	4	4
6	1	1	3	3	1	5	4	2	3	1	1	1	3	5	5	3	5	2	4	3	5	3	4	5	5	5	5	1	5	3	2	3	5	5	1	4	4	5
7	1	1	2	3	4	4	4	2	2	2	3	4	2	1	1	3	4	1	1	5	4	3	4	4	3	4	4	4	5	5	2	2	4	4	1	1	3	5
8	1	1	3	3	2	5	2	4	2	2	1	2	2	1	4	3	2	4	2	2	5	3	4	5	2	4	4	2	4	2	3	4	4	4	2	2	4	5
9	2	1	3	3	2	5	5	2	3	1	4	4	3	2	3	2	3	4	3	2	4	3	4	4	5	3	4	3	4	4	1	3	4	4	2	4	2	4
10	2	1	5	5	5	5	5	5	5	1	5	5	5	3	5	4	4	2	5	2	4	5	4	5	4	4	5	2	5	3	3	4	3	4	4	3	5	4
11	2	1	4	4	1	3	3	5	4	2	5	4	4	3	4	4	4	2	4	2	5	4	2	5	4	4	4	4	5	4	4	4	4	4	3	4	4	4
12	1	1	2	2	4	3	1	1	2	2	2	2	2	2	2	2	4	3	2	4	5	4	2	5	2	2	5	2	5	2	2	2	5	4	2	2	4	5
13	1	1	3	3	1	5	2	3	2	4	3	2	4	1	4	3	5	3	3	5	5	4	2	5	2	3	5	2	5	3	3	4	5	5	2	2	5	5
14	2	1	3	3	2	5	2	1	3	1	1	2	2	1	1	1	4	2	2	5	4	4	2	4	3	4	4	4	4	2	1	4	5	3	2	2	4	5
15	2	1	4	4	1	5	4	1	3	2	2	3	3	4	2	4	3	3	5	2	4	4	3	4	2	3	4	4	4	2	4	3	4	4	2	2	4	4
16	2	1	4	4	3	4	1	1	4	1	5	4	1	2	4	3	4	3	4	4	4	3	5	5	5	5	5	3	5	5	2	4	4	4	4	4	3	4
17	2	1	2	2	4	5	2	4	3	3	4	2	2	2	2	1	4	3	2	2	5	2	3	5	2	3	3	3	5	3	3	3	5	4	1	1	4	5
18	2	1	5	5	1	5	1	1	3	2	3	2	5	1	1	1	2	2	2	5	5	5	3	5	3	2	5	4	5	3	2	2	5	5	1	1	5	5
19	2	1	3	3	3	4	3	2	3	2	2	3	2	3	3	3	3	3	2	3	3	3	3	4	3	3	4	3	4	3	3	3	4	3	3	3	4	4
20	2	1	3	3	2	3	2	3	2	1	2	2	2	3	2	3	4	3	3	2	4	4	2	5	2	2	5	4	4	1	1	2	3	4	2	2	5	4
21	2	1	5	5	2	4	4	2	5	1	4	4	4	3	5	3	3	2	4	1	5	4	2	4	4	3	4	2	5	2	2	4	4	3	2	4	5	5
22	2	1	3	3	1	3	1	5	3	2	1	3	2	1	3	1	4	2	1	5	5	5	3	4	5	3	5	3	5	4	5	4	5	4	3	3	5	5
23	1	1	3	3	3	2	3	2	3	3	3	3	3	2	1	2	4	2	2	3	4	2	2	4	2	2	4	2	4	2	2	2	4	4	4	2	2	4

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
24	1	1	3	3	3	5	2	1	4	2	4	4	4	3	3	3	2	2	4	4	4	4	3	5	4	3	4	4	5	3	3	4	5	4	3	3	2	5
25	2	1	1	1	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	4	3	3	4	1	1	4	1	4	1	1	3	4	5	1	1	1	5
26	1	1	4	3	3	5	4	4	4	2	2	4	4	3	2	3	4	2	3	1	2	4	4	4	2	2	4	4	5	2	4	2	2	4	2	2	4	4
27	2	1	2	3	2	5	3	2	4	2	5	5	5	3	2	2	5	4	4	4	4	4	4	5	4	4	5	4	5	4	4	4	4	4	2	2	5	5
28	1	1	3	5	2	5	2	1	5	1	5	3	5	2	2	3	5	4	4	5	5	2	3	5	3	3	5	5	5	4	4	3	5	2	3	5	4	4
29	2	1	5	4	2	3	4	1	3	2	4	3	4	4	2	2	3	3	3	2	4	3	3	4	4	4	4	4	4	4	4	4	4	3	2	3	5	5
30	2	1	4	3	1	3	3	1	4	1	4	4	3	2	1	1	3	2	2	2	4	4	3	4	4	4	4	4	4	3	2	4	4	4	2	2	4	4
31	2	1	2	3	4	2	2	2	3	2	2	2	2	2	2	2	2	3	4	2	4	3	4	4	3	3	4	4	4	4	4	3	4	4	2	2	4	4
32	2	2	1	1	1	3	1	1	1	1	1	1	2	1	1	1	3	3	1	5	5	3	1	5	5	3	4	4	4	3	4	4	4	4	1	1	2	5
33	2	1	3	2	3	2	2	1	3	2	2	3	4	3	3	3	5	3	3	4	5	4	3	5	2	4	4	4	5	3	3	3	5	4	3	3	4	5
34	2	1	4	4	4	4	3	3	3	3	3	3	4	3	3	3	3	3	3	2	4	4	3	4	4	4	4	3	4	4	4	4	4	4	3	3	4	4
35	1	1	3	2	1	5	5	1	5	1	5	3	4	2	3	4	3	2	5	2	5	5	2	5	1	2	5	3	5	3	4	4	4	2	2	4	5	5
36	1	1	4	5	5	5	3	1	5	2	4	5	4	5	5	5	4	3	5	3	5	5	3	5	4	2	5	4	5	2	2	4	4	5	5	5	5	3
37	1	1	5	5	1	5	5	2	4	1	4	4	3	4	3	5	3	3	4	2	3	3	4	4	4	2	3	3	4	3	2	3	3	2	3	4	4	5
38	2	1	5	5	3	3	4	1	3	2	3	3	3	3	2	3	5	3	3	3	3	3	3	1	3	3	3	3	3	3	3	3	5	3	3	3	3	4
39	1	4	1	1	4	1	1	3	5	1	1	1	1	1	1	1	5	1	1	3	3	3	3	3	3	3	3	4	5	5	5	3	5	4	1	1	3	5
40	1	1	3	4	1	5	5	2	3	2	4	4	3	5	4	3	3	2	5	3	4	4	4	5	3	4	5	3	3	3	4	4	5	2	3	4	2	5
41	2	2	3	2	4	3	2	3	3	3	2	2	1	1	2	2	4	3	2	4	4	4	1	5	3	2	4	5	5	1	1	2	2	5	1	2	4	5
42	1	1	2	3	2	2	1	3	4	2	4	4	2	1	1	1	4	1	1	4	3	4	1	4	5	4	3	4	4	1	4	1	4	4	2	2	4	4
43	1	2	4	4	1	5	2	1	3	1	3	3	5	4	2	5	5	4	5	3	5	5	3	5	5	2	5	2	3	5	3	4	3	2	4	4	5	5
44	1	1	2	2	3	5	1	1	1	4	2	3	1	1	1	1	3	2	3	2	4	3	2	5	1	2	4	3	5	3	4	4	3	4	2	2	4	4
45	1	1	2	2	3	5	5	1	3	1	5	5	5	5	4	4	5	4	4	2	5	5	3	5	4	4	5	1	5	3	3	4	5	5	5	5	5	5
46	2	2	3	3	2	1	2	1	3	1	4	3	2	2	2	2	4	3	2	4	4	4	2	4	2	3	4	4	5	2	4	3	4	4	2	2	4	5
47	1	1	3	3	2	4	3	3	2	2	2	2	2	3	2	3	4	4	3	5	4	4	4	5	4	3	4	4	4	4	4	4	4	4	3	3	5	4
48	2	2	1	1	2	4	1	1	1	4	3	1	1	1	1	1	1	1	1	1	4	3	3	4	3	1	4	2	4	4	2	3	3	3	2	2	4	4

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
49	1	1	4	4	2	2	1	2	3	1	3	3	2	2	2	2	5	4	5	4	5	4	3	4	5	4	4	4	4	3	2	4	4	2	2	3	5	5
50	1	1	3	2	2	5	5	1	4	2	3	1	5	1	1	1	5	1	2	5	5	4	2	5	5	3	5	4	5	2	3	5	5	5	1	1	5	5
51	1	1	4	3	1	5	4	4	5	2	4	4	4	5	4	4	4	4	4	4	5	5	3	4	4	3	3	3	3	4	4	3	4	4	4	4	3	4
52	1	2	4	4	5	4	5	3	3	2	3	3	2	3	3	4	5	4	4	3	4	5	4	1	4	4	1	4	1	2	4	4	5	4	2	2	1	1
53	1	2	3	3	4	2	2	3	3	3	2	3	3	2	3	3	3	3	2	3	4	4	3	4	3	3	4	3	4	3	3	3	4	4	2	2	4	4
54	1	2	4	4	3	5	3	2	4	3	4	4	5	3	5	5	3	2	4	4	5	4	3	5	4	4	4	3	4	5	3	5	5	5	3	3	1	3
55	1	3	2	2	1	2	1	1	5	3	3	4	5	2	2	1	3	4	1	4	4	1	1	5	3	3	1	1	4	4	2	4	4	4	2	2	4	4
56	1	1	3	2	2	5	2	1	2	2	3	1	1	2	3	1	5	2	1	5	1	5	2	5	5	4	5	5	5	5	4	2	4	4	1	3	5	4
57	2	1	3	2	4	4	2	1	3	4	1	2	2	3	4	2	4	2	2	5	1	1	2	1	2	2	1	1	1	2	2	1	1	1	2	2	1	1
58	1	1	4	3	3	5	3	3	4	2	5	4	4	3	4	3	5	3	4	4	5	4	3	4	3	3	4	4	4	3	4	4	4	4	3	3	3	4
59	1	1	4	4	1	2	3	2	4	4	4	3	2	3	2	2	1	3	2	4	3	4	2	4	3	4	5	4	4	4	4	1	4	4	4	3	4	4
60	1	1	3	3	2	2	4	3	5	1	5	1	2	3	2	3	3	2	3	4	4	4	2	5	4	2	4	3	5	2	5	4	4	4	3	3	5	5
61	2	1	2	2	2	5	3	5	2	1	2	2	2	1	1	1	2	1	2	4	1	2	2	4	3	2	4	4	4	2	2	2	4	4	4	2	4	4
62	2	1	3	3	3	1	3	5	5	1	3	3	3	3	3	3	3	3	3	3	1	1	1	4	4	2	2	2	4	4	4	4	4	4	4	4	4	4
63	2	2	3	3	1	5	3	2	3	1	3	1	4	1	3	5	3	2	3	3	2	2	3	5	3	3	4	4	5	3	3	4	4	4	2	2	1	4
64	1	2	3	3	1	3	2	2	3	1	5	1	2	1	2	2	2	3	2	3	5	4	3	5	1	3	4	3	5	2	3	3	4	5	2	2	5	5
65	1	1	2	2	1	2	1	2	1	2	3	2	2	1	1	1	2	1	2	2	1	4	4	4	5	4	4	4	4	4	4	4	4	4	5	5	4	5
66	1	1	2	2	4	2	1	4	3	3	3	2	1	3	3	2	3	3	2	4	4	3	4	5	4	3	4	3	3	1	2	2	4	3	1	4	3	5
67	1	1	1	2	1	5	3	5	2	3	4	1	2	1	3	2	1	4	5	4	4	2	3	5	4	5	3	5	4	3	4	4	5	4	1	3	5	5
68	1	1	3	2	3	2	1	1	2	1	2	1	2	2	3	4	3	2	3	2	3	4	4	4	2	4	4	3	5	3	4	3	2	4	1	2	1	5
69	1	1	3	1	1	2	2	1	3	3	5	2	3	5	5	5	5	3	5	2	2	4	2	3	1	2	3	1	3	3	3	3	1	2	3	5	4	4
70	1	1	2	2	3	3	3	4	4	1	1	5	3	3	4	4	3	1	4	1	4	3	3	4	2	4	4	2	5	3	1	1	5	4	1	1	4	5
71	1	1	3	3	2	5	5	2	4	1	1	3	4	4	2	3	4	2	2	2	5	3	2	4	3	3	5	3	5	3	2	2	4	3	2	1	4	5
72	1	1	3	3	1	5	3	1	5	3	1	1	5	1	1	1	3	3	4	2	4	3	4	4	3	2	5	4	4	3	3	3	4	2	2	4	4	4
73	2	1	1	2	4	1	1	4	2	3	1	1	1	2	2	2	3	3	4	5	3	2	2	5	3	2	4	2	5	2	4	5	5	5	1	2	2	3

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
74	1	1	3	3	3	4	3	2	2	1	1	4	4	3	2	3	3	3	3	3	4	4	4	4	4	4	4	2	4	4	4	3	5	2	4	5	2	4
75	1	1	1	2	5	2	1	4	3	3	4	2	1	1	1	1	2	2	1	3	4	3	4	5	4	4	4	3	4	5	3	2	4	2	4	1	4	4
76	1	1	4	4	3	5	4	1	3	1	3	3	2	3	2	2	3	3	3	2	5	3	4	5	1	2	4	4	5	2	1	3	5	3	1	1	5	5
77	1	1	4	4	2	4	5	1	4	1	4	3	3	5	5	5	4	3	4	4	4	3	3	5	4	4	5	5	4	3	4	4	5	3	3	4	4	4
78	1	1	3	1	2	4	1	2	3	1	1	2	3	2	3	1	3	2	3	1	5	3	3	4	4	2	5	1	5	1	2	2	5	4	3	1	5	4
79	2	1	4	4	2	4	3	1	3	1	1	1	3	4	3	1	3	1	3	1	3	4	2	4	4	4	4	2	3	5	5	3	4	3	2	1	2	5
80	2	1	4	4	1	5	3	4	4	1	4	2	4	2	4	2	5	4	4	2	4	4	4	4	3	3	4	4	5	3	3	4	4	4	2	2	5	5
81	2	1	2	2	3	5	4	4	4	1	4	4	2	3	3	2	3	3	3	3	4	3	3	4	4	4	4	3	4	3	4	3	4	5	2	3	4	5
82	1	1	2	2	4	5	1	1	3	2	1	2	1	3	1	1	4	2	1	4	4	4	4	5	2	2	5	2	5	2	2	4	5	5	1	1	5	5
83	1	1	3	3	2	5	5	2	4	1	5	3	4	4	4	4	4	4	3	2	3	3	4	5	5	4	4	4	3	4	3	4	2	3	2	2	4	4
84	1	1	3	3	1	5	4	2	3	1	1	1	3	5	5	3	5	2	4	3	5	3	4	5	5	5	5	1	5	3	2	3	5	5	1	4	4	5
85	1	1	2	3	4	4	4	2	2	2	3	4	2	1	1	3	4	1	1	5	4	3	4	4	3	4	4	4	5	5	2	2	4	4	1	1	3	5
86	1	1	3	3	2	5	2	4	2	2	1	2	2	1	4	3	2	4	2	2	5	3	4	5	2	4	4	2	4	2	3	4	4	4	2	2	4	5
87	2	1	3	3	2	5	5	2	3	1	4	4	3	2	3	2	3	4	3	2	4	3	4	4	5	3	4	3	4	4	1	3	4	4	2	4	2	4
88	2	1	5	5	5	5	5	5	5	1	5	5	5	3	5	4	4	2	5	2	4	5	4	5	4	4	5	2	5	3	3	4	3	4	4	3	5	4
89	2	1	4	4	1	3	3	5	4	2	5	4	4	3	4	4	4	2	4	2	5	4	2	5	4	4	4	4	5	4	4	4	4	4	3	4	4	4
90	1	1	2	2	4	3	1	1	2	2	2	2	2	2	2	2	4	3	2	4	5	4	2	5	2	2	5	2	5	2	2	2	5	4	2	2	4	5
91	1	1	3	3	1	5	2	3	2	4	3	2	4	1	4	3	5	3	3	5	5	4	2	5	2	3	5	2	5	3	3	4	5	5	2	2	5	5
92	2	1	3	3	2	5	2	1	3	1	1	2	2	1	1	1	4	2	2	5	4	4	2	4	3	4	4	4	4	2	1	4	5	3	2	2	4	5
93	2	1	4	4	1	5	4	1	3	2	2	3	3	4	2	4	3	3	5	2	4	4	3	4	2	3	4	4	4	2	4	3	4	4	2	2	4	4
94	2	1	4	4	3	4	1	1	4	1	5	4	1	2	4	3	4	3	4	4	4	3	5	5	5	5	5	3	5	5	2	4	4	4	4	4	3	4
95	2	1	2	2	4	5	2	4	3	3	4	2	2	2	2	1	4	3	2	2	5	2	3	5	2	3	3	3	5	3	3	3	5	4	1	1	4	5
96	2	1	5	5	1	5	1	1	3	2	3	2	5	1	1	1	2	2	2	5	5	5	3	5	3	2	5	4	5	3	2	2	5	5	1	1	5	5
97	2	1	3	3	3	4	3	2	3	2	2	3	2	3	3	3	3	3	2	3	3	3	3	4	3	3	4	3	4	3	3	3	4	3	3	3	4	4
98	2	1	3	3	2	3	2	3	2	1	2	2	2	3	2	3	4	3	3	2	4	4	2	5	2	2	5	4	4	1	1	2	3	4	2	2	5	4

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
99	2	1	5	5	2	4	4	2	5	1	4	4	4	3	5	3	3	2	4	1	5	4	2	4	4	3	4	2	5	2	2	4	4	3	2	4	5	5
100	2	1	3	3	1	3	1	5	3	2	1	3	2	1	3	1	4	2	1	5	5	5	3	4	5	3	5	3	5	4	5	4	5	4	3	3	5	5
101	1	1	3	3	3	2	3	2	3	3	3	3	3	2	1	2	4	2	2	3	4	2	2	4	2	2	4	2	4	2	2	2	4	4	4	2	2	4
102	1	1	3	3	3	5	2	1	4	2	4	4	4	3	3	3	2	2	4	4	4	4	3	5	4	3	4	4	5	3	3	4	5	4	3	3	2	5
103	2	1	1	1	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	4	3	3	4	1	1	4	1	4	1	1	3	4	5	1	1	1	5
104	1	1	4	3	3	5	4	4	4	2	2	4	4	3	2	3	4	2	3	1	2	4	4	4	2	2	4	4	5	2	4	2	2	4	2	2	4	4
105	2	1	2	3	2	5	3	2	4	2	5	5	5	3	2	2	5	4	4	4	4	4	4	5	4	4	5	4	5	4	4	4	4	4	2	2	5	5
106	1	1	3	5	2	5	2	1	5	1	5	3	5	2	2	3	5	4	4	5	5	2	3	5	3	3	5	5	5	4	4	3	5	2	3	5	4	4
107	2	1	5	4	2	3	4	1	3	2	4	3	4	4	2	2	3	3	3	2	4	3	3	4	4	4	4	4	4	4	4	4	4	3	2	3	5	5
108	2	1	4	3	1	3	3	1	4	1	4	4	3	2	1	1	3	2	2	2	4	4	3	4	4	4	4	4	4	3	2	4	4	4	2	2	4	4
109	2	1	2	3	4	2	2	2	3	2	2	2	2	2	2	2	2	3	4	2	4	3	4	4	3	3	4	4	4	4	4	3	4	4	2	2	4	4
110	2	2	1	1	1	3	1	1	1	1	1	1	2	1	1	1	3	3	1	5	5	3	1	5	5	3	4	4	4	3	4	4	4	4	1	1	2	5
111	2	1	3	2	3	2	2	1	3	2	2	3	4	3	3	3	5	3	3	4	5	4	3	5	2	4	4	4	5	3	3	3	5	4	3	3	4	5
112	2	1	4	4	4	4	3	3	3	3	3	3	4	3	3	3	3	3	3	2	4	4	3	4	4	4	4	3	4	4	4	4	4	4	3	3	4	4
113	1	1	3	2	1	5	5	1	5	1	5	3	4	2	3	4	3	2	5	2	5	5	2	5	1	2	5	3	5	3	4	4	4	2	2	4	5	5
114	1	1	4	5	5	5	3	1	5	2	4	5	4	5	5	5	4	3	5	3	5	5	3	5	4	2	5	4	5	2	2	4	4	5	5	5	5	3
115	1	1	5	5	1	5	5	2	4	1	4	4	3	4	3	5	3	3	4	2	3	3	4	4	4	2	3	3	4	3	2	3	3	2	3	4	4	5
116	2	1	5	5	3	3	4	1	3	2	3	3	3	3	2	3	5	3	3	3	3	3	3	1	3	3	3	3	3	3	3	3	5	3	3	3	3	4
117	1	4	1	1	4	1	1	3	5	1	1	1	1	1	1	1	5	1	1	3	3	3	3	3	3	3	3	4	5	5	5	3	5	4	1	1	3	5
118	1	1	3	4	1	5	5	2	3	2	4	4	3	5	4	3	3	2	5	3	4	4	4	5	3	4	5	3	3	3	4	4	5	2	3	4	2	5
119	2	2	3	2	4	3	2	3	3	3	2	2	1	1	2	2	4	3	2	4	4	4	1	5	3	2	4	5	5	1	1	2	2	5	1	2	4	5
120	1	1	2	3	2	2	1	3	4	2	4	4	2	1	1	1	4	1	1	4	3	4	1	4	5	4	3	4	4	1	4	1	4	4	2	2	4	4
121	1	2	4	4	1	5	2	1	3	1	3	3	5	4	2	5	5	4	5	3	5	5	3	5	5	2	5	2	3	5	3	4	3	2	4	4	5	5
122	1	1	2	2	3	5	1	1	1	4	2	3	1	1	1	1	3	2	3	2	4	3	2	5	1	2	4	3	5	3	4	4	3	4	2	2	4	4
123	1	1	2	2	3	5	5	1	3	1	5	5	5	5	4	4	5	4	4	2	5	5	3	5	4	4	5	1	5	3	3	4	5	5	5	5	5	5

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
124	2	2	3	3	2	1	2	1	3	1	4	3	2	2	2	2	4	3	2	4	4	4	2	4	2	3	4	4	5	2	4	3	4	4	2	2	4	5
125	1	1	3	3	2	4	3	3	2	2	2	2	2	3	2	3	4	4	3	5	4	4	4	5	4	3	4	4	4	4	4	4	4	4	3	3	5	4
126	2	2	1	1	2	4	1	1	1	4	3	1	1	1	1	1	1	1	1	1	4	3	3	4	3	1	4	2	4	4	2	3	3	3	2	2	4	4
127	1	1	4	4	2	2	1	2	3	1	3	3	2	2	2	2	5	4	5	4	5	4	3	4	5	4	4	4	4	3	2	4	4	2	2	3	5	5
128	1	1	3	2	2	5	5	1	4	2	3	1	5	1	1	1	5	1	2	5	5	4	2	5	5	3	5	4	5	2	3	5	5	5	1	1	5	5
129	1	1	4	3	1	5	4	4	5	2	4	4	4	5	4	4	4	4	4	4	5	5	3	4	4	3	3	3	3	4	4	3	4	4	4	4	3	4
130	1	2	4	4	5	4	5	3	3	2	3	3	2	3	3	4	5	4	4	3	4	5	4	1	4	4	1	4	1	2	4	4	5	4	2	2	1	1
131	1	2	3	3	4	2	2	3	3	3	2	3	3	2	3	3	3	3	2	3	4	4	3	4	3	3	4	3	4	3	3	3	4	4	2	2	4	4
132	1	2	4	4	3	5	3	2	4	3	4	4	5	3	5	5	3	2	4	4	5	4	3	5	4	4	4	3	4	5	3	5	5	5	3	3	1	3
133	1	3	2	2	1	2	1	1	5	3	3	4	5	2	2	1	3	4	1	4	4	1	1	5	3	3	1	1	4	4	2	4	4	4	2	2	4	4
134	1	1	3	2	2	5	2	1	2	2	3	1	1	2	3	1	5	2	1	5	1	5	2	5	5	4	5	5	5	5	4	2	4	4	1	3	5	4
135	2	1	3	2	4	4	2	1	3	4	1	2	2	3	4	2	4	2	2	5	1	1	2	1	2	2	1	1	1	2	2	1	1	1	2	2	1	1
136	1	1	4	3	3	5	3	3	4	2	5	4	4	3	4	3	5	3	4	4	5	4	3	4	3	3	4	4	4	3	4	4	4	4	3	3	3	4
137	1	1	4	4	1	2	3	2	4	4	4	3	2	3	2	2	1	3	2	4	3	4	2	4	3	4	5	4	4	4	4	1	4	4	4	3	4	4
138	1	1	3	3	2	2	4	3	5	1	5	1	2	3	2	3	3	2	3	4	4	4	2	5	4	2	4	3	5	2	5	4	4	4	3	3	5	5
139	2	1	2	2	2	5	3	5	2	1	2	2	2	1	1	1	2	1	2	4	1	2	2	4	3	2	4	4	4	2	2	2	4	4	4	2	4	4
140	2	1	3	3	3	1	3	5	5	1	3	3	3	3	3	3	3	3	3	3	1	1	1	4	4	2	2	2	4	4	4	4	4	4	4	4	4	4
141	2	2	3	3	1	5	3	2	3	1	3	1	4	1	3	5	3	2	3	3	2	2	3	5	3	3	4	4	5	3	3	4	4	4	2	2	1	4
142	1	2	3	3	1	3	2	2	3	1	5	1	2	1	2	2	2	3	2	3	5	4	3	5	1	3	4	3	5	2	3	3	4	5	2	2	5	5
143	1	1	2	2	1	2	1	2	1	2	3	2	2	1	1	1	2	1	2	2	1	4	4	4	5	4	4	4	4	4	4	4	4	4	5	5	4	5
144	1	1	2	2	4	2	1	4	3	3	3	2	1	3	3	2	3	3	2	4	4	3	4	5	4	3	4	3	3	1	2	2	4	3	1	4	3	5
145	1	1	1	2	1	5	3	5	2	3	4	1	2	1	3	2	1	4	5	4	4	2	3	5	4	5	3	5	4	3	4	4	5	4	1	3	5	5
146	1	1	3	2	3	2	1	1	2	1	2	1	2	2	3	4	3	2	3	2	3	4	4	4	2	4	4	3	5	3	4	3	2	4	1	2	1	5
147	1	1	3	1	1	2	2	1	3	3	5	2	3	5	5	5	5	3	5	2	2	4	2	3	1	2	3	1	3	3	3	3	1	2	3	5	4	4
148	1	1	2	2	3	3	3	4	4	1	1	5	3	3	4	4	3	1	4	1	4	3	3	4	2	4	4	2	5	3	1	1	5	4	1	1	4	5

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
149	1	1	3	3	2	5	5	2	4	1	1	3	4	4	2	3	4	2	2	2	5	3	2	4	3	3	5	3	5	3	2	2	4	3	2	1	4	5
150	1	1	3	3	1	5	3	1	5	3	1	1	5	1	1	1	3	3	4	2	4	3	4	4	3	2	5	4	4	3	3	3	4	2	2	4	4	4
151	2	1	1	2	4	1	1	4	2	3	1	1	1	2	2	2	3	3	4	5	3	2	2	5	3	2	4	2	5	2	4	5	5	5	1	2	2	3
152	1	1	3	3	3	4	3	2	2	1	1	4	4	3	2	3	3	3	3	3	4	4	4	4	4	4	4	2	4	4	4	3	5	2	4	5	2	4
153	1	1	1	2	5	2	1	4	3	3	4	2	1	1	1	1	2	2	1	3	4	3	4	5	4	4	4	3	4	5	3	2	4	2	4	1	4	4
154	1	1	4	4	3	5	4	1	3	1	3	3	2	3	2	2	3	3	3	2	5	3	4	5	1	2	4	4	5	2	1	3	5	3	1	1	5	5
155	1	1	4	4	2	4	5	1	4	1	4	3	3	5	5	5	4	3	4	4	4	3	3	5	4	4	5	5	4	3	4	4	5	3	3	4	4	4
156	1	1	3	1	2	4	1	2	3	1	1	2	3	2	3	1	3	2	3	1	5	3	3	4	4	2	5	1	5	1	2	2	5	4	3	1	5	4
157	2	1	4	4	2	4	3	1	3	1	1	1	3	4	3	1	3	1	3	1	3	4	2	4	4	4	4	2	3	5	5	3	4	3	2	1	2	5
158	2	1	4	4	1	5	3	4	4	1	4	2	4	2	4	2	5	4	4	2	4	4	4	4	3	3	4	4	5	3	3	4	4	4	2	2	5	5
159	2	1	2	2	3	5	4	4	4	1	4	4	2	3	3	2	3	3	3	3	4	3	3	4	4	4	4	3	4	3	4	3	4	5	2	3	4	5
160	1	1	2	2	4	5	1	1	3	2	1	2	1	3	1	1	4	2	1	4	4	4	4	5	2	2	5	2	5	2	2	4	5	5	1	1	5	5
161	1	1	3	3	2	5	5	2	4	1	5	3	4	4	4	4	4	4	3	2	3	3	4	5	5	4	4	4	3	4	3	4	2	3	2	2	4	4
162	1	1	3	3	1	5	4	2	3	1	1	1	3	5	5	3	5	2	4	3	5	3	4	5	5	5	5	1	5	3	2	3	5	5	1	4	4	5
163	1	1	2	3	4	4	4	2	2	2	3	4	2	1	1	3	4	1	1	5	4	3	4	4	3	4	4	4	5	5	2	2	4	4	1	1	3	5
164	1	1	3	3	2	5	2	4	2	2	1	2	2	1	4	3	2	4	2	2	5	3	4	5	2	4	4	2	4	2	3	4	4	4	2	2	4	5
165	2	1	3	3	2	5	5	2	3	1	4	4	3	2	3	2	3	4	3	2	4	3	4	4	5	3	4	3	4	4	1	3	4	4	2	4	2	4
166	2	1	5	5	5	5	5	5	5	1	5	5	5	3	5	4	4	2	5	2	4	5	4	5	4	4	5	2	5	3	3	4	3	4	4	3	5	4
167	2	1	4	4	1	3	3	5	4	2	5	4	4	3	4	4	4	2	4	2	5	4	2	5	4	4	4	4	5	4	4	4	4	4	3	4	4	4
168	1	1	2	2	4	3	1	1	2	2	2	2	2	2	2	2	4	3	2	4	5	4	2	5	2	2	5	2	5	2	2	2	5	4	2	2	4	5
169	1	1	3	3	1	5	2	3	2	4	3	2	4	1	4	3	5	3	3	5	5	4	2	5	2	3	5	2	5	3	3	4	5	5	2	2	5	5
170	2	1	3	3	2	5	2	1	3	1	1	2	2	1	1	1	4	2	2	5	4	4	2	4	3	4	4	4	4	2	1	4	5	3	2	2	4	5
171	2	1	4	4	1	5	4	1	3	2	2	3	3	4	2	4	3	3	5	2	4	4	3	4	2	3	4	4	4	2	4	3	4	4	2	2	4	4
172	2	1	4	4	3	4	1	1	4	1	5	4	1	2	4	3	4	3	4	4	4	3	5	5	5	5	5	3	5	5	2	4	4	4	4	4	3	4
173	2	1	2	2	4	5	2	4	3	3	4	2	2	2	2	1	4	3	2	2	5	2	3	5	2	3	3	3	5	3	3	3	5	4	1	1	4	5

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
174	2	1	5	5	1	5	1	1	3	2	3	2	5	1	1	1	2	2	2	5	5	5	3	5	3	2	5	4	5	3	2	2	5	5	1	1	5	5
175	2	1	3	3	3	4	3	2	3	2	2	3	2	3	3	3	3	3	2	3	3	3	3	4	3	3	4	3	4	3	3	3	4	3	3	3	4	4
176	2	1	3	3	2	3	2	3	2	1	2	2	2	3	2	3	4	3	3	2	4	4	2	5	2	2	5	4	4	1	1	2	3	4	2	2	5	4
177	2	1	5	5	2	4	4	2	5	1	4	4	4	3	5	3	3	2	4	1	5	4	2	4	4	3	4	2	5	2	2	4	4	3	2	4	5	5
178	2	1	3	3	1	3	1	5	3	2	1	3	2	1	3	1	4	2	1	5	5	5	3	4	5	3	5	3	5	4	5	4	5	4	3	3	5	5
179	1	1	3	3	3	2	3	2	3	3	3	3	3	2	1	2	4	2	2	3	4	2	2	4	2	2	4	2	4	2	2	2	4	4	4	2	2	4
180	1	1	3	3	3	5	2	1	4	2	4	4	4	3	3	3	2	2	4	4	4	4	3	5	4	3	4	4	5	3	3	4	5	4	3	3	2	5
181	2	1	1	1	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	4	3	3	4	1	1	4	1	4	1	1	3	4	5	1	1	1	5
182	1	1	4	3	3	5	4	4	4	2	2	4	4	3	2	3	4	2	3	1	2	4	4	4	2	2	4	4	5	2	4	2	2	4	2	2	4	4
183	2	1	2	3	2	5	3	2	4	2	5	5	5	3	2	2	5	4	4	4	4	4	4	5	4	4	5	4	5	4	4	4	4	4	2	2	5	5
184	1	1	3	5	2	5	2	1	5	1	5	3	5	2	2	3	5	4	4	5	5	2	3	5	3	3	5	5	5	4	4	3	5	2	3	5	4	4
185	2	1	5	4	2	3	4	1	3	2	4	3	4	4	2	2	3	3	3	2	4	3	3	4	4	4	4	4	4	4	4	4	4	3	2	3	5	5
186	2	1	4	3	1	3	3	1	4	1	4	4	3	2	1	1	3	2	2	2	4	4	3	4	4	4	4	4	4	3	2	4	4	4	2	2	4	4
187	2	1	2	3	4	2	2	2	3	2	2	2	2	2	2	2	2	3	4	2	4	3	4	4	3	3	4	4	4	4	4	3	4	4	2	2	4	4
188	2	2	1	1	1	3	1	1	1	1	1	1	2	1	1	1	3	3	1	5	5	3	1	5	5	3	4	4	4	3	4	4	4	4	1	1	2	5
189	2	1	3	2	3	2	2	1	3	2	2	3	4	3	3	3	5	3	3	4	5	4	3	5	2	4	4	4	5	3	3	3	5	4	3	3	4	5
190	2	1	4	4	4	4	3	3	3	3	3	3	4	3	3	3	3	3	3	2	4	4	3	4	4	4	4	3	4	4	4	4	4	4	3	3	4	4
191	1	1	3	2	1	5	5	1	5	1	5	3	4	2	3	4	3	2	5	2	5	5	2	5	1	2	5	3	5	3	4	4	4	2	2	4	5	5
192	1	1	4	5	5	5	3	1	5	2	4	5	4	5	5	5	4	3	5	3	5	5	3	5	4	2	5	4	5	2	2	4	4	5	5	5	5	3
193	1	1	5	5	1	5	5	2	4	1	4	4	3	4	3	5	3	3	4	2	3	3	4	4	4	2	3	3	4	3	2	3	3	2	3	4	4	5
194	2	1	5	5	3	3	4	1	3	2	3	3	3	3	2	3	5	3	3	3	3	3	3	1	3	3	3	3	3	3	3	3	5	3	3	3	3	4
195	1	4	1	1	4	1	1	3	5	1	1	1	1	1	1	1	5	1	1	3	3	3	3	3	3	3	3	4	5	5	5	3	5	4	1	1	3	5
196	1	1	3	4	1	5	5	2	3	2	4	4	3	5	4	3	3	2	5	3	4	4	4	5	3	4	5	3	3	3	4	4	5	2	3	4	2	5
197	2	2	3	2	4	3	2	3	3	3	2	2	1	1	2	2	4	3	2	4	4	4	1	5	3	2	4	5	5	1	1	2	2	5	1	2	4	5
198	1	1	2	3	2	2	1	3	4	2	4	4	2	1	1	1	4	1	1	4	3	4	1	4	5	4	3	4	4	1	4	1	4	4	2	2	4	4

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
199	1	2	4	4	1	5	2	1	3	1	3	3	5	4	2	5	5	4	5	3	5	5	3	5	5	2	5	2	3	5	3	4	3	2	4	4	5	5
200	1	1	2	2	3	5	1	1	1	4	2	3	1	1	1	1	3	2	3	2	4	3	2	5	1	2	4	3	5	3	4	4	3	4	2	2	4	4
201	1	1	2	2	3	5	5	1	3	1	5	5	5	5	4	4	5	4	4	2	5	5	3	5	4	4	5	1	5	3	3	4	5	5	5	5	5	5
202	2	2	3	3	2	1	2	1	3	1	4	3	2	2	2	2	4	3	2	4	4	4	2	4	2	3	4	4	5	2	4	3	4	4	2	2	4	5
203	1	1	3	3	2	4	3	3	2	2	2	2	2	3	2	3	4	4	3	5	4	4	4	5	4	3	4	4	4	4	4	4	4	4	3	3	5	4
204	2	2	1	1	2	4	1	1	1	4	3	1	1	1	1	1	1	1	1	1	4	3	3	4	3	1	4	2	4	4	2	3	3	3	2	2	4	4
205	1	1	4	4	2	2	1	2	3	1	3	3	2	2	2	2	5	4	5	4	5	4	3	4	5	4	4	4	4	3	2	4	4	2	2	3	5	5
206	1	1	3	2	2	5	5	1	4	2	3	1	5	1	1	1	5	1	2	5	5	4	2	5	5	3	5	4	5	2	3	5	5	5	1	1	5	5
207	1	1	4	3	1	5	4	4	5	2	4	4	4	5	4	4	4	4	4	4	5	5	3	4	4	3	3	3	3	4	4	3	4	4	4	4	3	4
208	1	2	4	4	5	4	5	3	3	2	3	3	2	3	3	4	5	4	4	3	4	5	4	1	4	4	1	4	1	2	4	4	5	4	2	2	1	1
209	1	2	3	3	4	2	2	3	3	3	2	3	3	2	3	3	3	3	2	3	4	4	3	4	3	3	4	3	4	3	3	3	4	4	2	2	4	4
210	1	2	4	4	3	5	3	2	4	3	4	4	5	3	5	5	3	2	4	4	5	4	3	5	4	4	4	3	4	5	3	5	5	5	3	3	1	3
211	1	3	2	2	1	2	1	1	5	3	3	4	5	2	2	1	3	4	1	4	4	1	1	5	3	3	1	1	4	4	2	4	4	4	2	2	4	4
212	1	1	3	2	2	5	2	1	2	2	3	1	1	2	3	1	5	2	1	5	1	5	2	5	5	4	5	5	5	5	4	2	4	4	1	3	5	4
213	2	1	3	2	4	4	2	1	3	4	1	2	2	3	4	2	4	2	2	5	1	1	2	1	2	2	1	1	1	2	2	1	1	1	2	2	1	1
214	1	1	4	3	3	5	3	3	4	2	5	4	4	3	4	3	5	3	4	4	5	4	3	4	3	3	4	4	4	3	4	4	4	4	3	3	3	4
215	1	1	4	4	1	2	3	2	4	4	4	3	2	3	2	2	1	3	2	4	3	4	2	4	3	4	5	4	4	4	4	1	4	4	4	3	4	4
216	1	1	3	3	2	2	4	3	5	1	5	1	2	3	2	3	3	2	3	4	4	4	2	5	4	2	4	3	5	2	5	4	4	4	3	3	5	5
217	2	1	2	2	2	5	3	5	2	1	2	2	2	1	1	1	2	1	2	4	1	2	2	4	3	2	4	4	4	2	2	2	4	4	4	2	4	4
218	2	1	3	3	3	1	3	5	5	1	3	3	3	3	3	3	3	3	3	3	1	1	1	4	4	2	2	2	4	4	4	4	4	4	4	4	4	4
219	2	2	3	3	1	5	3	2	3	1	3	1	4	1	3	5	3	2	3	3	2	2	3	5	3	3	4	4	5	3	3	4	4	4	2	2	1	4
220	1	2	3	3	1	3	2	2	3	1	5	1	2	1	2	2	2	3	2	3	5	4	3	5	1	3	4	3	5	2	3	3	4	5	2	2	5	5
221	1	1	2	2	1	2	1	2	1	2	3	2	2	1	1	1	2	1	2	2	1	4	4	4	5	4	4	4	4	4	4	4	4	4	5	5	4	5
222	1	1	2	2	4	2	1	4	3	3	3	2	1	3	3	2	3	3	2	4	4	3	4	5	4	3	4	3	3	1	2	2	4	3	1	4	3	5
223	1	1	1	2	1	5	3	5	2	3	4	1	2	1	3	2	1	4	5	4	4	2	3	5	4	5	3	5	4	3	4	4	5	4	1	3	5	5

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
224	1	1	3	2	3	2	1	1	2	1	2	1	2	2	3	4	3	2	3	2	3	4	4	4	2	4	4	3	5	3	4	3	2	4	1	2	1	5
225	1	1	3	1	1	2	2	1	3	3	5	2	3	5	5	5	5	3	5	2	2	4	2	3	1	2	3	1	3	3	3	3	1	2	3	5	4	4
226	1	1	2	2	3	3	3	4	4	1	1	5	3	3	4	4	3	1	4	1	4	3	3	4	2	4	4	2	5	3	1	1	5	4	1	1	4	5
227	1	1	3	3	2	5	5	2	4	1	1	3	4	4	2	3	4	2	2	2	5	3	2	4	3	3	5	3	5	3	2	2	4	3	2	1	4	5
228	1	1	3	3	1	5	3	1	5	3	1	1	5	1	1	1	3	3	4	2	4	3	4	4	3	2	5	4	4	3	3	3	4	2	2	4	4	4
229	2	1	1	2	4	1	1	4	2	3	1	1	1	2	2	2	3	3	4	5	3	2	2	5	3	2	4	2	5	2	4	5	5	5	1	2	2	3
230	1	1	3	3	3	4	3	2	2	1	1	4	4	3	2	3	3	3	3	3	4	4	4	4	4	4	4	2	4	4	4	3	5	2	4	5	2	4
231	1	1	1	2	5	2	1	4	3	3	4	2	1	1	1	1	2	2	1	3	4	3	4	5	4	4	4	3	4	5	3	2	4	2	4	1	4	4
232	1	1	4	4	3	5	4	1	3	1	3	3	2	3	2	2	3	3	3	2	5	3	4	5	1	2	4	4	5	2	1	3	5	3	1	1	5	5
233	1	1	4	4	2	4	5	1	4	1	4	3	3	5	5	5	4	3	4	4	4	3	3	5	4	4	5	5	4	3	4	4	5	3	3	4	4	4
234	1	1	3	1	2	4	1	2	3	1	1	2	3	2	3	1	3	2	3	1	5	3	3	4	4	2	5	1	5	1	2	2	5	4	3	1	5	4
235	2	1	4	4	2	4	3	1	3	1	1	1	3	4	3	1	3	1	3	1	3	4	2	4	4	4	4	2	3	5	5	3	4	3	2	1	2	5
236	2	1	4	4	1	5	3	4	4	1	4	2	4	2	4	2	5	4	4	2	4	4	4	4	3	3	4	4	5	3	3	4	4	4	2	2	5	5
237	2	1	2	2	3	5	4	4	4	1	4	4	2	3	3	2	3	3	3	3	4	3	3	4	4	4	4	3	4	3	4	3	4	5	2	3	4	5
238	1	1	2	2	4	5	1	1	3	2	1	2	1	3	1	1	4	2	1	4	4	4	4	5	2	2	5	2	5	2	2	4	5	5	1	1	5	5
239	1	1	3	3	2	5	5	2	4	1	5	3	4	4	4	4	4	4	3	2	3	3	4	5	5	4	4	4	3	4	3	4	2	3	2	2	4	4
240	1	1	3	3	1	5	4	2	3	1	1	1	3	5	5	3	5	2	4	3	5	3	4	5	5	5	5	1	5	3	2	3	5	5	1	4	4	5
241	1	1	2	3	4	4	4	2	2	2	3	4	2	1	1	3	4	1	1	5	4	3	4	4	3	4	4	4	5	5	2	2	4	4	1	1	3	5
242	1	1	3	3	2	5	2	4	2	2	1	2	2	1	4	3	2	4	2	2	5	3	4	5	2	4	4	2	4	2	3	4	4	4	2	2	4	5
243	2	1	3	3	2	5	5	2	3	1	4	4	3	2	3	2	3	4	3	2	4	3	4	4	5	3	4	3	4	4	1	3	4	4	2	4	2	4
244	2	1	5	5	5	5	5	5	5	1	5	5	5	3	5	4	4	2	5	2	4	5	4	5	4	4	5	2	5	3	3	4	3	4	4	3	5	4
245	2	1	4	4	1	3	3	5	4	2	5	4	4	3	4	4	4	2	4	2	5	4	2	5	4	4	4	4	5	4	4	4	4	4	3	4	4	4
246	1	1	2	2	4	3	1	1	2	2	2	2	2	2	2	2	4	3	2	4	5	4	2	5	2	2	5	2	5	2	2	2	5	4	2	2	4	5
247	1	1	3	3	1	5	2	3	2	4	3	2	4	1	4	3	5	3	3	5	5	4	2	5	2	3	5	2	5	3	3	4	5	5	2	2	5	5
248	2	1	3	3	2	5	2	1	3	1	1	2	2	1	1	1	4	2	2	5	4	4	2	4	3	4	4	4	4	2	1	4	5	3	2	2	4	5

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
249	2	1	4	4	1	5	4	1	3	2	2	3	3	4	2	4	3	3	5	2	4	4	3	4	2	3	4	4	4	2	4	3	4	4	2	2	4	4
250	2	1	4	4	3	4	1	1	4	1	5	4	1	2	4	3	4	3	4	4	4	3	5	5	5	5	5	3	5	5	2	4	4	4	4	4	3	4
251	2	1	2	2	4	5	2	4	3	3	4	2	2	2	2	1	4	3	2	2	5	2	3	5	2	3	3	3	5	3	3	3	5	4	1	1	4	5
252	2	1	5	5	1	5	1	1	3	2	3	2	5	1	1	1	2	2	2	5	5	5	3	5	3	2	5	4	5	3	2	2	5	5	1	1	5	5
253	2	1	3	3	3	4	3	2	3	2	2	3	2	3	3	3	3	3	2	3	3	3	3	4	3	3	4	3	4	3	3	3	4	3	3	3	4	4
254	2	1	3	3	2	3	2	3	2	1	2	2	2	3	2	3	4	3	3	2	4	4	2	5	2	2	5	4	4	1	1	2	3	4	2	2	5	4
255	2	1	5	5	2	4	4	2	5	1	4	4	4	3	5	3	3	2	4	1	5	4	2	4	4	3	4	2	5	2	2	4	4	3	2	4	5	5
256	2	1	3	3	1	3	1	5	3	2	1	3	2	1	3	1	4	2	1	5	5	5	3	4	5	3	5	3	5	4	5	4	5	4	3	3	5	5
257	1	1	3	3	3	2	3	2	3	3	3	3	3	2	1	2	4	2	2	3	4	2	2	4	2	2	4	2	4	2	2	2	4	4	4	2	2	4
258	1	1	3	3	3	5	2	1	4	2	4	4	4	3	3	3	2	2	4	4	4	4	3	5	4	3	4	4	5	3	3	4	5	4	3	3	2	5
259	2	1	1	1	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	4	3	3	4	1	1	4	1	4	1	1	3	4	5	1	1	1	5
260	1	1	4	3	3	5	4	4	4	2	2	4	4	3	2	3	4	2	3	1	2	4	4	4	2	2	4	4	5	2	4	2	2	4	2	2	4	4
261	2	1	2	3	2	5	3	2	4	2	5	5	5	3	2	2	5	4	4	4	4	4	4	5	4	4	5	4	5	4	4	4	4	4	2	2	5	5
262	1	1	3	5	2	5	2	1	5	1	5	3	5	2	2	3	5	4	4	5	5	2	3	5	3	3	5	5	5	4	4	3	5	2	3	5	4	4
263	2	1	5	4	2	3	4	1	3	2	4	3	4	4	2	2	3	3	3	2	4	3	3	4	4	4	4	4	4	4	4	4	4	3	2	3	5	5
264	2	1	4	3	1	3	3	1	4	1	4	4	3	2	1	1	3	2	2	2	4	4	3	4	4	4	4	4	4	3	2	4	4	4	2	2	4	4
265	2	1	2	3	4	2	2	2	3	2	2	2	2	2	2	2	2	3	4	2	4	3	4	4	3	3	4	4	4	4	4	3	4	4	2	2	4	4
266	2	2	1	1	1	3	1	1	1	1	1	1	2	1	1	1	3	3	1	5	5	3	1	5	5	3	4	4	4	3	4	4	4	4	1	1	2	5
267	2	1	3	2	3	2	2	1	3	2	2	3	4	3	3	3	5	3	3	4	5	4	3	5	2	4	4	4	5	3	3	3	5	4	3	3	4	5
268	2	1	4	4	4	4	3	3	3	3	3	3	4	3	3	3	3	3	3	2	4	4	3	4	4	4	4	3	4	4	4	4	4	4	3	3	4	4
269	1	1	3	2	1	5	5	1	5	1	5	3	4	2	3	4	3	2	5	2	5	5	2	5	1	2	5	3	5	3	4	4	4	2	2	4	5	5
270	1	1	4	5	5	5	3	1	5	2	4	5	4	5	5	5	4	3	5	3	5	5	3	5	4	2	5	4	5	2	2	4	4	5	5	5	5	3
271	1	1	5	5	1	5	5	2	4	1	4	4	3	4	3	5	3	3	4	2	3	3	4	4	4	2	3	3	4	3	2	3	3	2	3	4	4	5
272	2	1	5	5	3	3	4	1	3	2	3	3	3	3	2	3	5	3	3	3	3	3	3	1	3	3	3	3	3	3	3	3	5	3	3	3	3	4
273	1	4	1	1	4	1	1	3	5	1	1	1	1	1	1	1	5	1	1	3	3	3	3	3	3	3	3	4	5	5	5	3	5	4	1	1	3	5

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
274	1	1	3	4	1	5	5	2	3	2	4	4	3	5	4	3	3	2	5	3	4	4	4	5	3	4	5	3	3	3	4	4	5	2	3	4	2	5
275	2	2	3	2	4	3	2	3	3	3	2	2	1	1	2	2	4	3	2	4	4	4	1	5	3	2	4	5	5	1	1	2	2	5	1	2	4	5
276	1	1	2	3	2	2	1	3	4	2	4	4	2	1	1	1	4	1	1	4	3	4	1	4	5	4	3	4	4	1	4	1	4	4	2	2	4	4
277	1	2	4	4	1	5	2	1	3	1	3	3	5	4	2	5	5	4	5	3	5	5	3	5	5	2	5	2	3	5	3	4	3	2	4	4	5	5
278	1	1	2	2	3	5	1	1	1	4	2	3	1	1	1	1	3	2	3	2	4	3	2	5	1	2	4	3	5	3	4	4	3	4	2	2	4	4
279	1	1	2	2	3	5	5	1	3	1	5	5	5	5	4	4	5	4	4	2	5	5	3	5	4	4	5	1	5	3	3	4	5	5	5	5	5	5
280	2	2	3	3	2	1	2	1	3	1	4	3	2	2	2	2	4	3	2	4	4	4	2	4	2	3	4	4	5	2	4	3	4	4	2	2	4	5
281	1	1	3	3	2	4	3	3	2	2	2	2	2	3	2	3	4	4	3	5	4	4	4	5	4	3	4	4	4	4	4	4	4	4	3	3	5	4
282	2	2	1	1	2	4	1	1	1	4	3	1	1	1	1	1	1	1	1	1	4	3	3	4	3	1	4	2	4	4	2	3	3	3	2	2	4	4
283	1	1	4	4	2	2	1	2	3	1	3	3	2	2	2	2	5	4	5	4	5	4	3	4	5	4	4	4	4	3	2	4	4	2	2	3	5	5
284	1	1	3	2	2	5	5	1	4	2	3	1	5	1	1	1	5	1	2	5	5	4	2	5	5	3	5	4	5	2	3	5	5	5	1	1	5	5
285	1	1	4	3	1	5	4	4	5	2	4	4	4	5	4	4	4	4	4	4	5	5	3	4	4	3	3	3	3	4	4	3	4	4	4	4	3	4
286	1	2	4	4	5	4	5	3	3	2	3	3	2	3	3	4	5	4	4	3	4	5	4	1	4	4	1	4	1	2	4	4	5	4	2	2	1	1
287	1	2	3	3	4	2	2	3	3	3	2	3	3	2	3	3	3	3	2	3	4	4	3	4	3	3	4	3	4	3	3	3	4	4	2	2	4	4
288	1	2	4	4	3	5	3	2	4	3	4	4	5	3	5	5	3	2	4	4	5	4	3	5	4	4	4	3	4	5	3	5	5	5	3	3	1	3
289	1	3	2	2	1	2	1	1	5	3	3	4	5	2	2	1	3	4	1	4	4	1	1	5	3	3	1	1	4	4	2	4	4	4	2	2	4	4
290	1	1	3	2	2	5	2	1	2	2	3	1	1	2	3	1	5	2	1	5	1	5	2	5	5	4	5	5	5	5	4	2	4	4	1	3	5	4
291	2	1	3	2	4	4	2	1	3	4	1	2	2	3	4	2	4	2	2	5	1	1	2	1	2	2	1	1	1	2	2	1	1	1	2	2	1	1
292	1	1	4	3	3	5	3	3	4	2	5	4	4	3	4	3	5	3	4	4	5	4	3	4	3	3	4	4	4	3	4	4	4	4	3	3	3	4
293	1	1	4	4	1	2	3	2	4	4	4	3	2	3	2	2	1	3	2	4	3	4	2	4	3	4	5	4	4	4	4	1	4	4	4	3	4	4
294	1	1	3	3	2	2	4	3	5	1	5	1	2	3	2	3	3	2	3	4	4	4	2	5	4	2	4	3	5	2	5	4	4	4	3	3	5	5
295	2	1	2	2	2	5	3	5	2	1	2	2	2	1	1	1	2	1	2	4	1	2	2	4	3	2	4	4	4	2	2	2	4	4	4	2	4	4
296	2	1	3	3	3	1	3	5	5	1	3	3	3	3	3	3	3	3	3	3	1	1	1	4	4	2	2	2	4	4	4	4	4	4	4	4	4	4
297	2	2	3	3	1	5	3	2	3	1	3	1	4	1	3	5	3	2	3	3	2	2	3	5	3	3	4	4	5	3	3	4	4	4	2	2	1	4
298	1	2	3	3	1	3	2	2	3	1	5	1	2	1	2	2	2	3	2	3	5	4	3	5	1	3	4	3	5	2	3	3	4	5	2	2	5	5

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
299	1	1	2	2	1	2	1	2	1	2	3	2	2	1	1	1	2	1	2	2	1	4	4	4	5	4	4	4	4	4	4	4	4	4	5	5	4	5
300	1	1	2	2	4	2	1	4	3	3	3	2	1	3	3	2	3	3	2	4	4	3	4	5	4	3	4	3	3	1	2	2	4	3	1	4	3	5
301	1	1	1	2	1	5	3	5	2	3	4	1	2	1	3	2	1	4	5	4	4	2	3	5	4	5	3	5	4	3	4	4	5	4	1	3	5	5
302	1	1	3	2	3	2	1	1	2	1	2	1	2	2	3	4	3	2	3	2	3	4	4	4	2	4	4	3	5	3	4	3	2	4	1	2	1	5
303	1	1	3	1	1	2	2	1	3	3	5	2	3	5	5	5	5	3	5	2	2	4	2	3	1	2	3	1	3	3	3	3	1	2	3	5	4	4
304	1	1	2	2	3	3	3	4	4	1	1	5	3	3	4	4	3	1	4	1	4	3	3	4	2	4	4	2	5	3	1	1	5	4	1	1	4	5
305	1	1	3	3	2	5	5	2	4	1	1	3	4	4	2	3	4	2	2	2	5	3	2	4	3	3	5	3	5	3	2	2	4	3	2	1	4	5
306	1	1	3	3	1	5	3	1	5	3	1	1	5	1	1	1	3	3	4	2	4	3	4	4	3	2	5	4	4	3	3	3	4	2	2	4	4	4
307	2	1	1	2	4	1	1	4	2	3	1	1	1	2	2	2	3	3	4	5	3	2	2	5	3	2	4	2	5	2	4	5	5	5	1	2	2	3
308	1	1	3	3	3	4	3	2	2	1	1	4	4	3	2	3	3	3	3	3	4	4	4	4	4	4	4	2	4	4	4	3	5	2	4	5	2	4
309	1	1	1	2	5	2	1	4	3	3	4	2	1	1	1	1	2	2	1	3	4	3	4	5	4	4	4	3	4	5	3	2	4	2	4	1	4	4
310	1	1	4	4	3	5	4	1	3	1	3	3	2	3	2	2	3	3	3	2	5	3	4	5	1	2	4	4	5	2	1	3	5	3	1	1	5	5
311	1	1	4	4	2	4	5	1	4	1	4	3	3	5	5	5	4	3	4	4	4	3	3	5	4	4	5	5	4	3	4	4	5	3	3	4	4	4
312	1	1	3	1	2	4	1	2	3	1	1	2	3	2	3	1	3	2	3	1	5	3	3	4	4	2	5	1	5	1	2	2	5	4	3	1	5	4
313	1	1	2	2	1	2	1	2	1	2	3	2	2	1	1	1	2	1	2	2	1	4	4	4	5	4	4	4	4	4	4	4	4	4	5	5	4	5
314	1	1	2	2	4	2	1	4	3	3	3	2	1	3	3	2	3	3	2	4	4	3	4	5	4	3	4	3	3	1	2	2	4	3	1	4	3	5
315	1	1	1	2	1	5	3	5	2	3	4	1	2	1	3	2	1	4	5	4	4	2	3	5	4	5	3	5	4	3	4	4	5	4	1	3	5	5
316	1	1	3	2	3	2	1	1	2	1	2	1	2	2	3	4	3	2	3	2	3	4	4	4	2	4	4	3	5	3	4	3	2	4	1	2	1	5
317	1	1	3	1	1	2	2	1	3	3	5	2	3	5	5	5	5	3	5	2	2	4	2	3	1	2	3	1	3	3	3	3	1	2	3	5	4	4
318	1	1	2	2	3	3	3	4	4	1	1	5	3	3	4	4	3	1	4	1	4	3	3	4	2	4	4	2	5	3	1	1	5	4	1	1	4	5
319	1	1	3	3	2	5	5	2	4	1	1	3	4	4	2	3	4	2	2	2	5	3	2	4	3	3	5	3	5	3	2	2	4	3	2	1	4	5
320	1	1	3	3	1	5	3	1	5	3	1	1	5	1	1	1	3	3	4	2	4	3	4	4	3	2	5	4	4	3	3	3	4	2	2	4	4	4
321	2	1	1	2	4	1	1	4	2	3	1	1	1	2	2	2	3	3	4	5	3	2	2	5	3	2	4	2	5	2	4	5	5	5	1	2	2	3
322	1	1	3	3	3	4	3	2	2	1	1	4	4	3	2	3	3	3	3	3	4	4	4	4	4	4	4	2	4	4	4	3	5	2	4	5	2	4
323	1	1	1	2	5	2	1	4	3	3	4	2	1	1	1	1	2	2	1	3	4	3	4	5	4	4	4	3	4	5	3	2	4	2	4	1	4	4

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
324	1	1	4	4	3	5	4	1	3	1	3	3	2	3	2	2	3	3	3	2	5	3	4	5	1	2	4	4	5	2	1	3	5	3	1	1	5	5
325	1	1	4	4	2	4	5	1	4	1	4	3	3	5	5	5	4	3	4	4	4	3	3	5	4	4	5	5	4	3	4	4	5	3	3	4	4	4
326	1	1	3	1	2	4	1	2	3	1	1	2	3	2	3	1	3	2	3	1	5	3	3	4	4	2	5	1	5	1	2	2	5	4	3	1	5	4
327	1	1	2	2	1	2	1	2	1	2	3	2	2	1	1	1	2	1	2	2	1	4	4	4	5	4	4	4	4	4	4	4	4	4	5	5	4	5
328	1	1	2	2	4	2	1	4	3	3	3	2	1	3	3	2	3	3	2	4	4	3	4	5	4	3	4	3	3	1	2	2	4	3	1	4	3	5
329	1	1	1	2	1	5	3	5	2	3	4	1	2	1	3	2	1	4	5	4	4	2	3	5	4	5	3	5	4	3	4	4	5	4	1	3	5	5
330	1	1	3	2	3	2	1	1	2	1	2	1	2	2	3	4	3	2	3	2	3	4	4	4	2	4	4	3	5	3	4	3	2	4	1	2	1	5
331	1	1	3	1	1	2	2	1	3	3	5	2	3	5	5	5	5	3	5	2	2	4	2	3	1	2	3	1	3	3	3	3	1	2	3	5	4	4
332	1	1	2	2	3	3	3	4	4	1	1	5	3	3	4	4	3	1	4	1	4	3	3	4	2	4	4	2	5	3	1	1	5	4	1	1	4	5
333	1	1	3	3	2	5	5	2	4	1	1	3	4	4	2	3	4	2	2	2	5	3	2	4	3	3	5	3	5	3	2	2	4	3	2	1	4	5
334	1	1	3	3	1	5	3	1	5	3	1	1	5	1	1	1	3	3	4	2	4	3	4	4	3	2	5	4	4	3	3	3	4	2	2	4	4	4
335	2	1	1	2	4	1	1	4	2	3	1	1	1	2	2	2	3	3	4	5	3	2	2	5	3	2	4	2	5	2	4	5	5	5	1	2	2	3
336	1	1	3	3	3	4	3	2	2	1	1	4	4	3	2	3	3	3	3	3	4	4	4	4	4	4	4	2	4	4	4	3	5	2	4	5	2	4
337	1	1	1	2	5	2	1	4	3	3	4	2	1	1	1	1	2	2	1	3	4	3	4	5	4	4	4	3	4	5	3	2	4	2	4	1	4	4
338	1	1	4	4	3	5	4	1	3	1	3	3	2	3	2	2	3	3	3	2	5	3	4	5	1	2	4	4	5	2	1	3	5	3	1	1	5	5
339	1	1	4	4	2	4	5	1	4	1	4	3	3	5	5	5	4	3	4	4	4	3	3	5	4	4	5	5	4	3	4	4	5	3	3	4	4	4
340	1	1	3	1	2	4	1	2	3	1	1	2	3	2	3	1	3	2	3	1	5	3	3	4	4	2	5	1	5	1	2	2	5	4	3	1	5	4
341	1	1	2	2	1	2	1	2	1	2	3	2	2	1	1	1	2	1	2	2	1	4	4	4	5	4	4	4	4	4	4	4	4	4	5	5	4	5
342	1	1	2	2	4	2	1	4	3	3	3	2	1	3	3	2	3	3	2	4	4	3	4	5	4	3	4	3	3	1	2	2	4	3	1	4	3	5
343	1	1	1	2	1	5	3	5	2	3	4	1	2	1	3	2	1	4	5	4	4	2	3	5	4	5	3	5	4	3	4	4	5	4	1	3	5	5
344	1	1	3	2	3	2	1	1	2	1	2	1	2	2	3	4	3	2	3	2	3	4	4	4	2	4	4	3	5	3	4	3	2	4	1	2	1	5
345	1	1	3	1	1	2	2	1	3	3	5	2	3	5	5	5	5	3	5	2	2	4	2	3	1	2	3	1	3	3	3	3	1	2	3	5	4	4
346	1	1	2	2	3	3	3	4	4	1	1	5	3	3	4	4	3	1	4	1	4	3	3	4	2	4	4	2	5	3	1	1	5	4	1	1	4	5
347	1	1	3	3	2	5	5	2	4	1	1	3	4	4	2	3	4	2	2	2	5	3	2	4	3	3	5	3	5	3	2	2	4	3	2	1	4	5
348	1	1	3	3	1	5	3	1	5	3	1	1	5	1	1	1	3	3	4	2	4	3	4	4	3	2	5	4	4	3	3	3	4	2	2	4	4	4

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
349	2	1	1	2	4	1	1	4	2	3	1	1	1	2	2	2	3	3	4	5	3	2	2	5	3	2	4	2	5	2	4	5	5	5	1	2	2	3
350	1	1	3	3	3	4	3	2	2	1	1	4	4	3	2	3	3	3	3	3	4	4	4	4	4	4	4	2	4	4	4	3	5	2	4	5	2	4
351	1	1	1	2	5	2	1	4	3	3	4	2	1	1	1	1	2	2	1	3	4	3	4	5	4	4	4	3	4	5	3	2	4	2	4	1	4	4
352	1	1	4	4	3	5	4	1	3	1	3	3	2	3	2	2	3	3	3	2	5	3	4	5	1	2	4	4	5	2	1	3	5	3	1	1	5	5
353	1	1	4	4	2	4	5	1	4	1	4	3	3	5	5	5	4	3	4	4	4	3	3	5	4	4	5	5	4	3	4	4	5	3	3	4	4	4
354	1	1	3	1	2	4	1	2	3	1	1	2	3	2	3	1	3	2	3	1	5	3	3	4	4	2	5	1	5	1	2	2	5	4	3	1	5	4
355	1	1	2	2	1	2	1	2	1	2	3	2	2	1	1	1	2	1	2	2	1	4	4	4	5	4	4	4	4	4	4	4	4	4	5	5	4	5
356	1	1	2	2	4	2	1	4	3	3	3	2	1	3	3	2	3	3	2	4	4	3	4	5	4	3	4	3	3	1	2	2	4	3	1	4	3	5
357	1	1	1	2	1	5	3	5	2	3	4	1	2	1	3	2	1	4	5	4	4	2	3	5	4	5	3	5	4	3	4	4	5	4	1	3	5	5
358	1	1	3	2	3	2	1	1	2	1	2	1	2	2	3	4	3	2	3	2	3	4	4	4	2	4	4	3	5	3	4	3	2	4	1	2	1	5
359	1	1	3	1	1	2	2	1	3	3	5	2	3	5	5	5	5	3	5	2	2	4	2	3	1	2	3	1	3	3	3	3	1	2	3	5	4	4
360	1	1	2	2	3	3	3	4	4	1	1	5	3	3	4	4	3	1	4	1	4	3	3	4	2	4	4	2	5	3	1	1	5	4	1	1	4	5
361	1	1	3	3	2	5	5	2	4	1	1	3	4	4	2	3	4	2	2	2	5	3	2	4	3	3	5	3	5	3	2	2	4	3	2	1	4	5
362	1	1	3	3	1	5	3	1	5	3	1	1	5	1	1	1	3	3	4	2	4	3	4	4	3	2	5	4	4	3	3	3	4	2	2	4	4	4
363	2	1	1	2	4	1	1	4	2	3	1	1	1	2	2	2	3	3	4	5	3	2	2	5	3	2	4	2	5	2	4	5	5	5	1	2	2	3
364	1	1	3	3	3	4	3	2	2	1	1	4	4	3	2	3	3	3	3	3	4	4	4	4	4	4	4	2	4	4	4	3	5	2	4	5	2	4
365	1	1	1	2	5	2	1	4	3	3	4	2	1	1	1	1	2	2	1	3	4	3	4	5	4	4	4	3	4	5	3	2	4	2	4	1	4	4
366	1	1	4	4	3	5	4	1	3	1	3	3	2	3	2	2	3	3	3	2	5	3	4	5	1	2	4	4	5	2	1	3	5	3	1	1	5	5
367	1	1	4	4	2	4	5	1	4	1	4	3	3	5	5	5	4	3	4	4	4	3	3	5	4	4	5	5	4	3	4	4	5	3	3	4	4	4
368	1	1	3	1	2	4	1	2	3	1	1	2	3	2	3	1	3	2	3	1	5	3	3	4	4	2	5	1	5	1	2	2	5	4	3	1	5	4
369	1	1	2	2	3	3	3	4	4	1	1	5	3	3	4	4	3	1	4	1	4	3	3	4	2	4	4	2	5	3	1	1	5	4	1	1	4	5
370	1	1	3	3	2	5	5	2	4	1	1	3	4	4	2	3	4	2	2	2	5	3	2	4	3	3	5	3	5	3	2	2	4	3	2	1	4	5
371	1	1	3	3	1	5	3	1	5	3	1	1	5	1	1	1	3	3	4	2	4	3	4	4	3	2	5	4	4	3	3	3	4	2	2	4	4	4
372	2	1	1	2	4	1	1	4	2	3	1	1	1	2	2	2	3	3	4	5	3	2	2	5	3	2	4	2	5	2	4	5	5	5	1	2	2	3
373	1	1	3	3	3	4	3	2	2	1	1	4	4	3	2	3	3	3	3	3	4	4	4	4	4	4	4	2	4	4	4	3	5	2	4	5	2	4

Encuesta	Edad	Sexo	V1																		V2																	
			D1						D2						D3						D1						D2						D3					
			I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
374	2	1	1	2	4	1	1	4	2	3	1	1	1	2	2	2	3	3	4	5	3	2	2	5	3	2	4	2	5	2	4	5	5	5	1	2	2	3
375	1	1	3	3	3	4	3	2	2	1	1	4	4	3	2	3	3	3	3	3	4	4	4	4	4	4	4	2	4	4	4	3	5	2	4	5	2	4

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, VISURRAGA AGUERO JOEL MARTIN, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Ciberseguridad y su impacto en la prevención de ataques cibernéticos en los adultos mayores en el distrito de Jesús María, Lima 2022", cuyo autor es SALDAÑA DIAZ MAURICIO NICOLAS, constato que la investigación cumple con el índice de similitud establecido, y verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 06 de Agosto del 2022

Apellidos y Nombres del Asesor:	**Firma**
VISURRAGA AGUERO JOEL MARTIN **DNI:** 10192315 **ORCID** 0000-0002-0024-668X	Firmado digitalmente por: JMVISURRAGA el 10-08-2022 13:10:34

Código documento Trilce: TRI - 0395696

INVESTIGA UCV