ESCUELA DE POSGRADO

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

Ciberseguridad y su incidencia en el Tratamiento de Datos Personales en una Municipalidad Distrital de Lima Sur, 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Correa Coronel, Miguel Martín (ORCID: 0000-0002-0088-9749)

ASESOR:

Dr. Visurraga Agüero, Joel Martin (ORCID: 0000-0002-0024-668X)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LIMA — PERÚ

2022

Dedicatoria

A mi padre, don Miguel Ángel Correa Falcón, que partió en adviento al encuentro eterno con Dios. Todos tus esfuerzos, aciertos y lecciones, querido papá, me sirvieron en el largo camino de la vida: “Dar de comer al hambriento, dar de beber al sediento”. Gracias por todo, mi viejo.

Agradecimiento

Gracias Señor por ayudarme a culminar estos estudios. Sin ti, nada de esto se habría logrado. También quiero dejar constancia de agradecimiento público a los asesores, Dr. Joel Visurraga y Dr. Pedro Lezama, por sus acertadas lecciones en la construcción de esta tesis; y a todos los docentes y colegas que intervinieron en este entregable. Finalmente, doy gracias a mi esposa, a mis hijos, a mi mamá y a mi hermana por perdonarme todo el tiempo que les robé mientras escribía esta tesis.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

El objetivo de la presente investigación fue determinar la incidencia de la ciberseguridad en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021. Se desarrolló una investigación del tipo aplicada con diseño no experimental, de tipo transversal y de corte correlacional – causal. La población que se consideró fue de 1046 colaboradores y mediante cálculos de muestreo estadístico se definió una muestra representativa de 282 colaboradores. Así mismo, se aplicó un muestreo probabilístico simple procediendo con la técnica de recolección datos denominada encuesta. A su vez el instrumento que se usó fue el cuestionario. En el análisis estadístico descriptivo se usaron tablas cruzadas e histogramas; el análisis inferencial de los datos fue basado en el Coeficiente de Regresión Ordinal.

Los resultados obtenidos permiten concluir que la ciberseguridad incide significativamente en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Palabras clave: Ciberseguridad, tratamiento de datos personales, ley de protección de datos personales.

Abstract

The objective of this research was to determine the incidence of cybersecurity in the processing of personal data in a district Municipality of Lima Sur, 2021. Applied research was developed with a non-experimental design, cross-sectional and correlational-causal design. The population that was considered was of 1046 collaborators and through statistical sampling calculations a representative sample of 282 collaborators was defined. Likewise, a simple probability sampling was applied proceeding with the data collection technique called survey. At the same time, the instrument used was the questionnaire. In the descriptive statistical analysis, cross tables and histograms were used; the inferential analysis of the data was based on the Ordinal Regression Coefficient.

The results obtained allow us to conclude that cybersecurity has a significant impact on the processing of personal data in a district Municipality of Lima Sur, 2021.

Keywords: Cybersecurity, personal data processing, personal data protection law.

I. INTRODUCCIÓN

Una forma de alterar la privacidad individual sucede cuando terceros acceden a datos sensibles de forma no autorizada, y que al hacerse públicos ponen en evidencia diferentes rasgos de la persona y la hacen identificable y vulnerable en un entorno específico. En ese sentido la preocupación por salvaguardar un adecuado tratamiento de datos personales es un imperativo válido e irrenunciable, que va desde la concepción de la misma ciberseguridad, pasando por el campo de la jurisprudencia y aterrizando en el campo de lo ético, tanto para la seguridad propia del individuo, como para las organizaciones y sus estrategias que están orientadas a preservar la información vertida en sus sistemas de información.

A nivel internacional, debemos tener presente que en enero de 1981 el Concejo de Europa suscribe el denominado Convenio N.º 108 o también llamado Convenio de Estrasburgo que en líneas generales representa un estándar en materia de derechos humanos (DD.HH) que por primera vez pone en relieve, de forma enérgica y sustancial en Europa, el tema de la protección de los datos personales a través de canales automatizados o virtualizados por medio de ordenadores. Posteriormente, debido a los avances en materia de protección de datos a nivel global y buscando reforzar la privacidad del tratamiento automatizado de datos de índole personal en Europa, en 2018 el mismo organismo suscribe el protocolo de enmienda denominado Protocolo 223, también llamado Convenio 108+ o Convenio 108 plus, con una prerrogativa legal vinculante que no poseía íntegramente el Convenio N.º 108 original. De esta forma todos los países adherentes al protocolo adquieren este documento como un estándar internacional para legislar en temas de datos personales depositados en bancos de datos. Hay que mencionar, además que, hasta julio de 2020, 121 países del mundo poseen alguna regulación legal sobre datos personales, 84 cuentan con una Autoridad Nacional de Protección de Datos (ANPD) y 4624 millones de personas con acceso a internet (IZAI, 2021).

A nivel nacional, el Banco Interamericano de Desarrollo (BID) (2020) señala que la legislación peruana en materia de protección de datos personales ha tenido

el siguiente avance: Ley N.º 30618, orientada a la seguridad digital; Ley N.º 30096, definida para castigar delitos informáticos; Ley N.º 27309 que anexa el delito informático al Código Penal Peruano; y finalmente, la Ley N.º 29733, Ley de Protección de Datos Personales (LPDP), que trata ampliamente sobre los lineamientos sobre el tratamiento de datos personales y que es aplicable para entidades públicas y privadas.

Por otro lado, a nivel local, el panorama de la protección de datos personales en las municipalidades de Lima no es muy alentador. La gran mayoría de estas organizaciones cuenta con un plan de seguridad informática muy limitado; y no cuentan con un plan específico en la materia de protección de datos. Por ejemplo, basta con señalar que, en el año 2020, el Ministerio de Justicia evidenció que la Municipalidad distrital de Miraflores (Lima) incumplió la LPDP y sugirió una amonestación administrativa de 250 mil soles contra dicha entidad por revelar datos personales de sus vecinos a terceros no autorizados (Paz, 2020).

Bajo este contexto la Municipalidad distrital de Lima Sur en los últimos años ha venido trabajando, desde su Unidad de Desarrollo Tecnológico (UDT), un conjunto de medidas relacionadas a la ciberseguridad de la organización, que se vinculen principalmente a definir e identificar las amenazas que pongan en peligro los sistemas de información, definir claramente el impacto y los riesgos que conllevan dichas amenazas, definir y aplicar las formas de defensa y de respuesta inmediata ante dichos riesgos y amenazas, desarrollar hábitos de buenas prácticas en materia de protección de activos y de información, teniendo principal incidencia en el tratamiento de los datos personales de sus colaboradores alojados en los diferentes sistemas de información. En esta organización existen diversos sistemas informáticos que alojan datos sensibles personales, los cuales deben estar exentos de pérdida, corrupción o deterioro de los mismos. Un claro ejemplo de estas falencias en ciberseguridad recae sobre el proceso de contratación CAS y sobre el tratamiento de datos específicos que se realiza sobre el sistema de gestión documentaria que deja expuestos datos sensibles de los colaboradores recién contratados. En este sentido una Municipalidad distrital de Lima Sur a considerado

a bien apoyar una investigación que relacione la ciberseguridad y el tratamiento de datos personales, con la intención de poder dar solución a la problemática antes descrita, por ende, como problema general de investigación se formuló la siguiente pregunta:

¿De qué manera la ciberseguridad incide en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021?

Así mismo se considerarán como problemas específicos las siguientes preguntas: a) ¿De qué manera la dimensión conservación de la confidencialidad de la ciberseguridad incide en la dimensión principio de consentimiento del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021?, b) ¿De qué manera la dimensión integridad de la ciberseguridad incide en la dimensión del principio de calidad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021?, c) ¿De qué manera la dimensión disponibilidad de la ciberseguridad incide en la dimensión principio de seguridad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021?

Por otro lado, el presente estudio se justifica desde muchas perspectivas académicas. A continuación, enunciamos las principales justificaciones que nos han llevado a realizar la presente investigación:

La justificación epistemológica, que engloba a la investigación respecto todas y cada una de las teorías y definiciones científicas válidas que se usarán para concretar una correcta formulación del problema de investigación, así como el uso del método científico. Adicionalmente, amparándonos en las evidencias recolectadas en el desarrollo de la presente investigación, se obtendrá la validación a las hipótesis definidas, en función del criterio de razonabilidad y la prevalencia del espíritu de la verdad científica.

La justificación teórica, que está fundamentada en la vocación de incrementar y producir información vinculada a la ciberseguridad y al tratamiento de datos personales, con el desinteresado objetivo de poder mejorar el conocimiento de las futuras generaciones de investigadores.

La justificación práctica, que está fundamentada en la medida en que la ciberseguridad a través de sus dimensiones de confiabilidad, integridad y disponibilidad, puedan lograr una significativa incidencia en el tratamiento de datos personales, vinculados respectivamente, a sus dimensiones de principio de consentimiento, principio de calidad y principio de seguridad.

Finalmente, la justificación metodológica que está fundamentada y encuentra arraigo en el diseño no experimental, toda vez que las variables en estudio no son susceptibles de cambio. Con el sano propósito de obtener resultados fehacientes, se argumenta que la compilación de los datos se realizó a través de instrumentos metodológicos fiables y validado por el criterio de juicios de expertos.

Así mismo, como objetivo general para la presente investigación definió lo siguiente: Determinar la incidencia de la ciberseguridad en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Como objetivos específicos se definen las siguientes premisas: a) Determinar la incidencia de la dimensión conservación de la confidencialidad de la ciberseguridad en la dimensión principio de consentimiento del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021; b) Determinar la incidencia de la dimensión integridad de la ciberseguridad en la dimensión principio de calidad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021; y, c) Determinar la incidencia de la dimensión disponibilidad de la ciberseguridad en la dimensión principio de seguridad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Respecto a la hipótesis general de la presente investigación se define lo siguiente: La ciberseguridad incide significativamente en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Del mismo modo, las hipótesis específicas son: a) La dimensión conservación de la confidencialidad de la ciberseguridad incide significativamente en la dimensión principio de consentimiento del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021; b) La dimensión integridad de la

ciberseguridad incide significativamente en la dimensión principio de calidad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021; y, c) La dimensión disponibilidad de la ciberseguridad incide significativamente en la dimensión principio de seguridad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

II. MARCO TEÓRICO

Ahora bien, en relación con la presente investigación es importante resaltar las siguientes investigaciones predecesoras que están relacionadas con el tema en cuestión, de modo que sirvan de apoyo académico al presente trabajo.

En el rubro de los antecedentes internacionales citamos la investigación de Choejey, Murray y Che (2017) con el título Perceptions of Cybersecurity in Government Organizations: Case Study of Bhutan, investigación auspiciada por la revista internacional Engineering and Technology International Journal of Computer and Information Engineering (EE.UU). El objetivo de la investigación se fundamentó en determinar la efectividad de la implementación de la ciberseguridad en las organizaciones. La metodología usada fue del tipo no experimental, correlacional de corte transversal. Respecto a las conclusiones se indica que la ciberseguridad está implementada de forma ligeramente inadecuada en las instituciones y, por ende, existe una distancia para concretar una postura de ciberseguridad ideal organizativa. En ese sentido se concluye que la implementación de la ciberseguridad en las empresas influye en un 40.0% sobre la política de ciberseguridad (protección de datos) de la organización.

Así mismo, citamos a Stefaniuk (2020) en su investigación titulada Training in shaping employee information security awareness, desarrollada y sustentada en la Siedlce University of Natural Sciences and Humanities (Polonia). El objetivo de esta investigación se fundamentó en analizar el nivel de efectividad existente entre la capacitación en formación de conciencia de los empleados en materia de ciberseguridad y su desempeño en la seguridad de la información. La metodología empleada en esta investigación fue del tipo primaria dual y se buscó aportar información para futuras investigaciones sobre el rubro. Respecto a las conclusiones podemos rescatar que se logró justificar una relación significativa entre los sistemas de gestión de seguridad de la información en la organización (ciberseguridad) y la publicación de la Política de seguridad de la información (protección de datos), en donde el aumento del 12.0% de la primera, repercute en el aumento del 18.0% de la segunda, respectivamente.

Del mismo modo tenemos a Luh y Yen (2020), en su investigación titulada Cybersecurity in Science and Medicine: Threats and Challenges, investigación auspiciada y desarrollada por la revista internacional Trends in Biotechnology en los EE. UU, cuyo objetivo fue describir la incidencia de la ciberseguridad sobre los problemas de privacidad de datos de los pacientes, relacionados con investigación de genomas, aparatos médicos y tecnología corporal. La metodología de esta investigación fue descriptiva y estuvo fundamentada en los ejes de Inversión en Tecnología, Políticas Públicas y Asociaciones Público-Privadas. Las conclusiones expuestas en este trabajo describen la incidencia significativa que existe entre la ciberseguridad en la asistencia sanitaria y la seguridad de los datos de los pacientes. Además, se argumenta que, para lograr un adecuado tratamiento de los datos de los pacientes en los ambientes sanitarios, se necesita una mayor coordinación y participación de científicos, asistentes de salud, referentes en ética, organismos estatales vinculantes, pacientes y toda la sociedad en su conjunto. Finalmente, se aconseja implementar mejores prácticas y soluciones que estén orientadas a las necesidades del paciente participante en investigaciones donde se entrega y formulan datos de la salud individual vinculados implícitamente a la privacidad.

Por su parte, Markopoulou, Papakonstantinou y De Hert (2019), realizaron la investigación titulada The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, auspiciada y desarrollada por la editorial científica sanitaria Elsevier en la Unión Europea. El objetivo de la investigación citada estuvo fundamentado en describir la relación que existe entre la Directiva Network Information Service (NIS) de 2017, Ley de ciberseguridad de la Unión Europea (UE) y el Reglamento General de Protección de Datos de la misma UE. La metodología usada para la citada investigación fue descriptiva y la conclusión más relevante recae sobre una crítica a la Directiva NIS que permite a los Estados miembros cierta holgura en el ámbito de respuesta en materia de ciberseguridad.

Así también, citamos a Pérez y Ramos (2020) en su investigación titulada Propuesta de una política de ciberseguridad para las Fuerzas Armadas, investigación patrocinada por la Universidad de las Fuerzas Armadas de Ecuador, cuyo objetivo fue proponer una política de ciberseguridad para proteger la información digital de Fuerza Armadas de Ecuador, mediante la colaboración y coordinación con las instituciones responsables de la seguridad informática del Ecuador. La metodología de la investigación citada fue descriptiva. Las conclusiones más resaltantes de esta investigación se amparan en que la propuesta sustentada por la investigación, sobre políticas de seguridad informática, fomentan un clima estable en materia de ciberseguridad, vinculando habilidades relacionadas a las nuevas tecnologías emergentes en Ecuador. Finalmente, se deja explícitamente sustentado que esta investigación cumplió con validar la matriz de políticas de ciberseguridad en las instancias militares correspondientes.

Finalmente, citamos a Javid, Faris, Beenish y Fahad (2020), en su investigación titulada Cybersecurity and Data Privacy in the Cloudlet for reliminary Healthcare Big Data Analytics, investigación realizada en República Islámica de Pakistán y sustentada en la Universidad de Tabuk, Arabia Saudita. El objetivo fue describir la relación que existe entre la ciberseguridad y la privacidad de datos en la industria de la salud de cara a la cuarta revolución industrial (era del ciberespacio). La metodología usada fue del tipo descriptiva y respecto a las conclusiones podemos señalar que dichos investigadores afirman que existe una gran expectativa desafiante entre la ciberseguridad y la privacidad de los datos en el contexto de las soluciones emergentes post tercera revolución industrial. Finalmente, se señala que la tecnología basada en máquinas virtuales para dispositivos móviles (cloudlet), permitirá realizar un mejor trabajo con latencia mínima y mayor seguridad virtual en el manejo de datos personales relacionados a pacientes.

Por otro lado, en el rubro de los antecedentes nacionales citamos a Taípe (2020), con investigación titulada La auditoría de seguridad informática y su relación en la ciberseguridad en el sector público año 2018, estudio realizado bajo el auspicio

de la Universidad Nacional de Piura. El objetivo de la investigación citada se centra en analizar cómo se relaciona la auditoria de seguridad informática y la ciberseguridad del sector público durante el año 2018. La metodología usada fue del tipo no experimental de corte transversal analítico descriptivo correlacional. Respecto de las conclusiones de esta investigación, se rescata que existe una correspondencia significativa entre la ciberseguridad con respecto a los riesgos de la información digital del sector público durante el año 2018, dado que en la investigación citada la prueba de correlación de Spearman mostró una significancia de 0.003 (menor a cinco centésimos); a su vez, calculando el coeficiente de correlación Rho de Spearman se obtuvo 314 milésimos con lo cual se define una correlación proporcional directa y de intensidad promedia entre las variables descritas. Finalmente, la ciberseguridad en el sector público y las políticas de ciberseguridad (seguridad de la información y datos) se relacionan en los niveles muy alto y óptimo, respectivamente, en un 35.3%.

Del mismo modo, tenemos a Bohorquez (2021) con la investigación titulada Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020. El objetivo de la citada pesquisa fue determinar la relación de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. La metodología empleada fue del tipo no experimental. Respecto de las conclusiones de esta investigación, se rescata que la ciberseguridad se relaciona significativamente (nivel de correlación de nivel muy fuerte) con la gestión de tecnologías de información a consecuencia del cálculo del coeficiente Rho de Spearman equivalente a 832 milésimos. Finalmente, la relación entre la ciberseguridad y la gestión de tecnologías de información se relacionan en los niveles de alta prevalencia y óptimo, reactivamente, en un 14.1%.

Así también, Villarrubia (2021), en su investigación titulada Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la política de seguridad y defensa nacional en la región Lima, 2018, investigación realizada en el Centro de Altos Estudios Nacionales (CAEN), nos indica que su objetivo de investigación fue describir las infraestructuras para la protección de la

información digital de los centros de Informática del Ejército. El diseño de esta investigación fue del tipo empírico. La conclusión más rescatable se fundamenta respecto a las infraestructuras para el tratamiento de datos y protección de la información digital de los centros de Informática del Ejército y se justifica la importancia de un presupuesto idóneo y conservable en el tiempo, que garantice un adecuado funcionamiento de las estructuras descritas.

Finalmente, citamos a Zúñiga (2017) en su investigación titulada Ciberdefensa y su incidencia en la protección de la Información del Ejército del Perú. caso: COPERE 2013 – 2014, investigación realizada en el Instituto Científico Tecnológico del Ejército. El objetivo fue identificar la razón que genera el no cumplimiento de las medidas vinculadas a la ciberdefensa. La metodología usada fue del tipo no experimental y de corte transversal. Referente a las conclusiones se puede señalar que existe una incidencia significativa entre la ciberdefensa y la protección de datos e información del Ejército del Perú.

Respecto a los fundamentos teóricos en los que se respalda la presente investigación, se tiene a bien considerar las siguientes teorías.

Comenzamos con la explicación referente a la Teoría General de Sistemas (TGS) que, según Rosen (1969), amparado en lo establecido por Ludwig Von Bertalanffy, la define como un conjunto de diversos elementos interrelacionados e interdependientes que al entrar en interacción buscan concretar propósitos comunes. Así mismo, Kish et al (2021) y Sagasti y Mitroff (1973) indican que un sistema no puede ser analizado en partes aisladas, sino, holísticamente como un ente íntegro; esto se debe a que la complejidad de las interrelaciones propias del sistema así lo condicionan. Por su parte, Beven (2006) manifiesta que la razón de ser de la TGS se encuentra fundamentada en la perspectiva sistémica de los cambios, alcances y limitaciones propias de un sistema que están vinculados a los fundamentos propios de esta teoría (objetivos, métodos y herramientas) que permiten aplicar esta perspectiva integradora de la realidad a distintos campos de la ciencia, a diferentes niveles de organización y distintas complejidades. A esto último se le conoce como el nombre de isomorfismo sistémico. Finalmente, Seising

(2010), la define como una multidisciplina epistemológica de totalidades e indica una característica clave de la TGS: los sistemas teleológicos. Sistemas capaces de generar una retroalimentación negativa (o también conocida como neguentropía), que busca equilibrar situaciones caóticas (entropía positiva) en donde un sistema puede destruirse a sí mismo. De esta forma se asegura la perdurabilidad del sistema a razón de la homeostasis realizada.

Por otro lado, la Teoría de la Inclusión y Exclusión (TIE) será tratada en esta parte de la investigación, dado que es un referente actual en materia de perspectiva social. Al respecto Luhmann (2005), tal como lo indican Leydesdorff e Ivanova (2013), define que la teoría de la inclusión y exclusión, desde el punto de vista de la comunicación social, se refiere al estilo y la forma de contextualizar el aspecto comunicativo humano, es decir, toda actuación comunicativa del ser humano está predispuesta por la sociedad dominante de la época, la cual condiciona, de cierta forma, el accionar de las personas, por ende, la comunicación al ser una de las tantas actuaciones humanas posee un rol social que incluye o excluye a ciertos grupos de la sociedad. Así mismo, Schirmer y Michailakis (2013) indican que la teoría de la inclusión y exclusión, desde la perspectiva del trabajo social, busca explicar, teóricamente, el comportamiento de los individuos excluidos socialmente en función de sus condiciones iniciales, supuestos y creencias, variables endógenas y su desempeño en la historia contemporánea de la sociedad. Además, señalan que esta teoría es un aporte social con tendencia a la reinserción del individuo excluido en una sociedad más justa. Por su parte, Blanco (2019), fundamentándose en los paradigmas de Niklas Luhmann, señala que existe una dualidad conceptual en la teoría señalada. Tradicionalmente ambos conceptos han sido considerados mutuamente excluyentes en la sociología, sin embargo, para este autor los términos inclusión y exclusión son parte de una misma categoría como si fueran las dos caras de una misma moneda. Esto último tiene sentido pleno, dado que la TIE nos permite describir y comprender los comportamientos y paradigmas de las sociedades contemporáneas en materia económica, de comunicación social y de derechos. Finalmente, Cova, Ivens y Spencer (2020), amparándose en los postulados de Niklas Luhmann, indican que la TIE estudia y explica el estilo con el que una

sociedad permite a sus individuos realizarse como personas en el ámbito comunicacional, es decir, en la medida que no existan barreras para la autopoiesis propia de cada individuo que interactúa con otro sin distinciones de condición social, etnia, credo, ideología, entre otros.

Ahora bien, el siguiente punto ahonda en la definición de las variables de la presente investigación.

Respecto a la definición de la variable independiente de ciberseguridad citamos a la International Organization for Standardization en la norma ISO / IEC 27032 titulada Information Technology — Security Techniques — Guidelines for cybersecurity que está orientada a la gestión de la ciberseguridad. El numeral 4.20 de la norma indicada que la ciberseguridad (también llamada seguridad en el ciberespacio) está definida bajo las dimensiones (también llamados pilares) de conservación de la confidencialidad, integridad y disponibilidad de la información alojada en ordenadores y redes digitales de gran escala y de transmisión de información a nivel mundial, denominado ciberespacio (ISO, 2012). Así también, Craigen, Diakun-Thibault y Purse (2014), como se citó en Wessels et al (2021), argumentan que la ciberseguridad es la forma de organizar y recopilar insumos, procesos y soportes usados para resguardar el ciberespacio y los sistemas creados en él (convenios, protocolos o asistencia técnica especializada), de modo que la seguridad esté orientada a la protección frente a las amenazas y vulnerabilidades de internet y de terceros inescrupulosos. Por otro lado, la International Telecommunication Union (ITU, s/f), como se citó en Quayyum et al (2021), define por ciberseguridad a la colección de herramientas, decisiones políticas (gubernamentales y no gubernamentales), definiciones de seguridad informática, protocolos de seguridad, ejes y enfoques de gestión de riesgos, frameworks, gestión de la capacitación tecnológica, entre otros, destinados a proteger los activos de una organización y sus allegados que están alojados en el entorno del ciberespacio. Finalmente, Rashid et al (2021) y Turk et al (2021) argumentan coincidentemente que la ciberseguridad es el conjunto de herramientas tecnológicas que está orientado a proteger los sistemas informáticos compuestos por computadoras,

redes de transmisión de datos, hardware, software y recursos que interactúan en el ciberespacio. Además, señalan que las principales amenazas con las que lidia a ciberseguridad son los siguientes: phishing, ransomware, malware, social engineering, entre otros.

Por todo lo anteriormente descrito y considerando lo definido por la Organization for Standardization (ISO, 2012) en la norma ISO / IEC 27032, en esta investigación se define para la variable independiente ciberseguridad, lo siguiente: primera dimensión, conservación de la confidencialidad; segunda dimensión, integridad; tercera dimensión, disponibilidad.

Para la primera dimensión de la variable independiente ciberseguridad, Grassi, García y Fenton (2017), como se citó en Giménez-Aguilar et al (2021), señalan que la conservación de la confidencialidad se entiende en el ámbito de la no divulgación de información hacia terceras instituciones o individuos no autorizados. En este sentido la conservación de la confidencialidad se centra principalmente en el despliegue que realizará la institución que resguarda la información para que ésta no sea divulgada de forma irregular. Así mismo Pawlicka et al (2021), fundamentan que la conservación de la confidencialidad es un concepto relacionado íntimamente, tanto para ciberseguridad como para gestión de la privacidad de datos. En consecuencia, de lo anteriormente explicado se puede inferir que la conservación de la confidencialidad es una de las formas que usa la ciberseguridad para hacerle frente a la ciberdelincuencia. Por otro lado, Corallo, Lazoi y Lezzi (2020) indican que la confidencialidad también está ligada a la protección de datos vinculados a maquinas industriales de producción. En ese sentido, perder cierto grado de conservación de la confidencialidad en el ámbito indicado conllevaría a una del nivel de ciberseguridad de las empresas industriales y que, por ende, se generarían impactos comerciales negativos para las empresas del sector. Hay que mencionar, además a Ferdinand (2015), tal como se citó en Rajan et al (2021), que indica que la conservación de la confidencialidad, en términos de ciberseguridad, se fundamenta en controles jurídicos, administrativos, tácticos y técnicos especializados. Finalmente, Lee (2021) añade que la

ciberseguridad tiene como objetivo minimizar los efectos de los ciberataques recibidos maliciosamente por terceros inescrupulosos que buscan debilitar la conservación de la confidencialidad de los sistemas de información en el ciberespacio con la intención clara de apoderarse de datos sensibles de empresas y personas.

Para la segunda dimensión de la variable independiente ciberseguridad, Mohammadpourfard et al (2020) y Pal et al (2021) concuerdan en señalar que la integridad se define como la protección y mantenimiento de la información sin alteración obtenida a través de la comunicación que fluye en el ciberespacio. Así también señalan que la integridad busca inhabilitar toda forma de corrupción de datos que podrían generar data incorrecta. En este sentido Botta, Cavagnino y Esposito (2021) señalan también que la integridad es la forma de garantizar, proteger y verificar que la información de un sistema crítico de seguridad no haya sido manipulada por terceros no autorizados. A su vez, ISO (2012) en su numeral 6.4.2 señala que la pérdida de integridad se produce al dañar un activo (banco de datos, por ejemplo) por medio de una modificación sin autorización. Finalmente, Hubbard y Seiersen (2016) indican que la carencia de integridad de un sistema en un determinado momento puede generar condiciones para la realización de transacciones no autorizadas que generarían como consecuencia pérdida y modificación de datos auténticos.

Para la tercera dimensión de la variable independiente ciberseguridad, Najmi et al (2021) infieren que disponibilidad en términos de ciberseguridad se logra cuando se da el acceso pleno, necesario y debidamente autorizado a las aplicaciones, recursos y servicios alojados en el ciberespacio. Para McCumber (2004), tal como se citó en Maestre (2018), la disponibilidad es uno de los tres pilares de la ciberseguridad junto a la confiabilidad e integridad. Este trio, asegura el autor son de gran preponderancia en materia de ciberseguridad exitosa. Sin embargo, recalca que la ventaja que ofrece la disponibilidad se fundamenta en que ésta genera factores de oportunidad únicos para los interesados al promover que se acceda a la información cuantas veces sea necesario. El no contar con esta

facultad de acceso generaría pérdida de tiempo, costos de oportunidad y redundancia de procesos. Por otro lado, Kilovaty (2020) afirma que la disponibilidad es una propiedad de accesibilidad acreditada hacia ordenadores, datos y redes informáticas que son atacadas por los ciberdelincuentes cuando se generan condiciones para la denegación de los servicios. En ese sentido, la disponibilidad se entiende como la plena disposición de los sistemas, aplicativos y datos. Finalmente, Vacca (2017) y Fosch-Villaronga y Mahler (2021) concuerdan en afirmar que la disponibilidad es una capacidad de soporte fundamental para la ciberseguridad. Según estos autores la disponibilidad está plenamente relacionada con un adecuado diseño sistemático (software, hardware, redes, políticas y protocolos) de acceso a los datos y existen mecanismos estadísticos para garantizar su normal desempeño.

Por otro lado, respecto a la definición de la variable dependiente de esta investigación, es decir, el tratamiento de datos personales, citamos a la Unión Europea (UE, 2018) en el artículo 2 del Convenio 108+, tal como lo indicó Pauletto (2020), que define el tratamiento de datos personales como cualquier tipo de procesamiento, automatizado o no, que tenga como propósito alterar datos personales. De manera semejante, la Ley Federal Rusa del 30 de diciembre de 2001 No. 197-FZ, tal como se citó en Arkhipov y Naumov (2016), indica que el tratamiento de datos personales, a nivel laboral, implica toda forma de recepcionar, almacenar, combinar o transferir datos sensibles de los trabajadores. En ese sentido debemos precisar que el marco legal peruano sigue una definición similar respecto al tratamiento de datos personales. Así mismo la Presidencia del Concejo de Ministros (2017), define por tratamiento de datos personales a cualquier forma técnica, no necesariamente automatizada, que permite la recopilación, inscripción, disposición, almacenamiento, depósito, producción, alteración, sustracción, búsqueda, uso, suspensión, eliminación, transferencia, propagación o cualquier otra forma distinta de encausamiento que permita la manipulación virtual de los datos personales. Más aún, el Ministerio de Justicia y Derechos Humanos, MINJUSDH (2013), citado por Polo (2020), indica que los artículos 7, 8, 9 y 10, del Reglamento de la Ley de Protección de Datos Personales (RLPDP), Ley N.º 29733, definida en el Decreto

Supremo N.º 003-2013-JUS, establecen los principios o dimensiones del concepto de tratamiento de datos personales, el cual se fundamenta en el principio de consentimiento, principio de finalidad, principio de calidad y el principio de seguridad. Finalmente, Stitilis y Laurinaitis (2017) afirman que la definición de tratamiento de datos personales está relacionada implícitamente al concepto de otorgamiento de consentimiento. Esto último debido a que el consentimiento, por lo general, deja sentado tácitamente la posibilidad de que se realicen operaciones con los datos personales recopilados. La legalidad del consentimiento deberá estar entonces relacionada al propósito del tratamiento que se desea hacer con los datos personales.

Por lo anteriormente sustentado y considerando lo definido por MINJUSDH (2013), en esta investigación se define para la variable dependiente tratamiento de datos personales, lo siguiente: primera dimensión, principio de consentimiento; segunda dimensión, principio de calidad; tercera dimensión, principio de seguridad.

Para la primera dimensión de la variable dependiente citamos a Steinfeld (2019) y Maxey (2020) que indican que el principio de consentimiento implica dar el permiso necesario a una entidad con la finalidad de que pueda usar, tratar o distribuir los datos personales asignados en sus bancos de datos. Los importante para este autor es que el principio de consentimiento tendrá un gran impacto en la forma de definir cómo y cuándo se podrán usar los datos personales entregados y resalta el factor preponderante que tiene la voluntad de otorgamiento expresada en términos legales. Así mismo, Koops (2014), citado en Zheng (2021) y Liu (2014) manifiestan que el consentimiento se sustenta en el hecho de que un individuo libremente, y siguiendo su autodeterminación, decide otorgar facultades a una institución externa para que sus datos personales sean recabados para un fin específico. Sin embargo, este autor señala que esto último no ha logrado condicionar las protecciones necesarias en materia de datos personales. Finalmente, Salinas (2019) afirma que el artículo 7 del Reglamento de la Ley N.º 29733 define que el Principio de Consentimiento tiene su arraigo básico cuando un individuo brinda su aprobación libremente, previamente, expresamente,

informadamente e inequívocamente para que sus datos personales sean tratados y registrados en la base de datos de una organización.

Para la segunda dimensión de la variable dependiente citamos a Chua et al (2017) y Yang et al (2021) que indican que el principio de calidad, o también llamado principio de integridad del tratamiento de datos personales, consiste en el despliegue de acciones por parte de la entidad que resguarda los datos personales para que estos gocen de precisión, completitud, veracidad y actualización en función del propósito para el cual fueron recabados. Adicionalmente, la organización también debe garantizar que los datos gozan de un impedimento de fuga de privacidad. A su vez Leal et al (2021) argumenta que el principio de calidad en materia de tratamiento de datos debe cumplir con las condiciones de ser auténticos, inteligibles, actuales, originales y carentes de ambigüedad. Finalmente, Gómez y Montoya (2018); y Mendoza (2018), citado en López (2021), señalan que el artículo 6° de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México; y el artículo 8º de la Ley N.º 29733 promulgada por el Congreso de la República del Perú, respectivamente, definen como principio de calidad a todo el conjunto de procedimientos y normas que buscan garantizar que los datos personales sean completos, puntuales, adecuados, de reciente actualización y fehacientes.

Para la tercera dimensión de la variable dependiente citamos a Polo (2020) y Vásquez (2019) quienes indican que el artículo 9° de la Ley N.º 29733 y el artículo 10º del Reglamento de la misma ley, definen el principio de seguridad como el conjunto de procedimientos y normas que buscan garantizar que los datos personales sean protegidos contra el hurto, la adulteración y el tratamiento o procesamiento por terceros no autorizados. A su vez, Cerda (2006) indica que el principio de seguridad se fundamenta en el conjunto de acciones de índole técnica, organizacional y jurídica que están orientadas a preservar la seguridad, el tratamiento, el acceso autorizado y la reserva de los datos personales alojados en sus bancos de datos. Finalmente, Olivos (2020) y Benussi (2020), coinciden en definir el principio de seguridad como aquel conjunto de obligaciones que asume el

titular del banco de datos y el responsable del tratamiento de los datos que los condiciona legalmente a resguardar, administrar y tratar los datos recibidos por sus propietarios.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

Esta investigación se consideró del tipo aplicada. Al respecto Ñaupas et al (2018) indica que una investigación aplicada es aquella que, amparándose en teorías provenientes de una ciencia pura, da respuestas prácticas e innovadoras a problemáticas concretas de la realidad tecnológica, social, sanitaria, medioambiental, jurídica, financiera, entre otros.

Diseño de investigación

Para la presente investigación se consideró un diseño no experimental de tipo transversal y de corte correlacional - causal. Según Hernández et al (2018) una investigación no experimental se caracteriza por no alterar previamente las variables, es decir, el investigador omite toda forma de injerencia en la manipulación de las variables en investigación. En consecuencia, las variables deben ser analizadas en su medio natural de acción. Así también, Hernández y Mendoza (2018) indican que un estudio es transversal y de corte correlacional, cuando recopila información de forma instantánea para un único momento específico; y busca probar una o varias hipótesis para arribar a conclusiones a partir de la justificación de la relación entre variables, respectivamente.

Esquema del diseño de investigación:

Dónde:

Variable independiente: Ciberseguridad

R: Relación causal

Variable dependiente: Tratamiento de datos personales

3.2. Variables y Operacionalización

Variable independiente: Ciberseguridad

Para esta investigación se define que la variable ciberseguridad es, según su naturaleza, del tipo cualitativa; y, según la definición de sus características intrínsecas, es del tipo categórica. Al respecto Ñaupas et al (2018) indica que una variable cualitativa y categórica expresa cualidades, características, clases, condiciones, entre otras, que se pueden medir usando algún tipo de escala.

Definición conceptual de la variable ciberseguridad

Según ISO (2012) la ciberseguridad está orientada a la protección de la información en el ciberespacio y está definida bajo las dimensiones de conservación de la confidencialidad, integridad y disponibilidad de la información alojada en ordenadores y redes digitales de gran escala y de transmisión a nivel mundial.

Definición operacional de la variable ciberseguridad

La variable ciberseguridad se operacionaliza por tres dimensiones: Conservación de la confidencialidad, integridad y disponibilidad; de modo tal que la información conseguida será evaluada mediante escala de Likert en los niveles: No óptimo (1), Medio (2) y Óptimo (3).

Tabla 1

Matriz de operacionalización de la variable independiente: Ciberseguridad.

Dimensiones	Indicadores	Ítems	Escala de Valores	Niveles	Rangos
Conservación de la confidencialidad	Autorización	1-2	1) Totalmente en desacuerdo	No óptimo	18 – 42
	Almacenamiento	3-4			
	Tránsito	5-6	2) En desacuerdo		
	Precisión	7-8			
Integridad	Completitud	9-10	3) Ni de acuerdo ni en desacuerdo	Medio	43 – 67
	Conformidad	11-12			
Disponibilidad	Acceso	13-14	4) De acuerdo	Óptimo	68 – 90
	Creación	15-16			
	Actualización	17-18	5) Totalmente de acuerdo		

Nota: Esta tabla muestra las dimensiones de la variable independiente ciberseguridad y sus respectivos indicadores.

Variable dependiente: Tratamiento de datos personales

Para esta investigación se definió que la variable tratamiento de datos personales es, según su naturaleza, del tipo cualitativa; y, según la definición de sus características intrínsecas, es del tipo categórica. Al respecto Ñaupas et al (2018) indica que una variable cualitativa y categórica expresa cualidades, características, clases, condiciones, entre otras, que se pueden medir usando algún tipo de escala.

Definición conceptual de la variable tratamiento de datos personales

Para MINJUSDH (2013), citado por Polo (2020), el tratamiento de datos personales es todo aquel procesamiento que se realiza con datos proveídos por personas cuyas dimensiones se fundamentan en el principio de consentimiento, principio de finalidad, principio de calidad y el principio de seguridad.

Definición operacional de la variable tratamiento de datos personales

La variable tratamiento de datos personales se operacionaliza por tres dimensiones: Principio de consentimiento, principio de calidad y principio de seguridad; de modo tal que la información conseguida será evaluada mediante escala de Likert en los niveles: Malo (1), Regular (2) y Bueno (3).

Tabla 2

Matriz de operacionalización de la variable independiente: Tratamiento de datos personales.

Dimensiones	Indicadores	Ítems	Escala de Valores	Niveles	Rangos
Principio de consentimiento	Autorización	19-20	1) Totalmente en desacuerdo	Malo	18 – 42
	Recopilación	21-22			
	Tratamiento	23-24	2) En desacuerdo		
	Precisión	25-26			
Principio de calidad	Veracidad	27-28	3) Ni de acuerdo ni en desacuerdo	Regular	43 – 67
	Finalidad	29-30			
	Fidelidad	31-32			
Principio de seguridad	Conservación	33-34	4) De acuerdo	Bueno	68 – 90
	Rectitud	35-36	5) Totalmente de acuerdo		

Nota: Esta tabla muestra las dimensiones de la variable dependiente tratamiento de datos personales y sus respectivos indicadores.

3.3. Población, muestra y muestreo

Población

Ñaupas et al (2018) indica que una población, en el marco de una investigación científica, se puede definir como una totalidad de individuos o unidades en estudio, que gozan de ciertas características uniformes y requeridas para los fines de la investigación en curso. En ese sentido, en esta investigación se consideró una población de 1046 colaboradores de la Municipalidad distrital de Lima Sur para el año 2021. En consecuencia, se detalla la siguiente tabla:

Tabla 3

Caracterización de la población.

Población	Cantidad
Colaboradores de la Municipalidad distrital de Lima Sur	1046
Total	1046

Nota: En esta tabla se detalla el escalar numérico de total de colaboradores la Municipalidad distrital de Lima Sur actualizada al año 2021.

Muestra

Ñaupas et al (2018) indica que una muestra, en el marco de una investigación científica, se puede definir como una parte o porción representativa de la totalidad de individuos o unidades en estudio. Por otro lado, para calcular el tamaño de la muestra en esta investigación se usará del software estadístico denominado Decision Analyst STATS Versión 2.0.0.2, considerando los siguientes niveles de precisión: tamaño de población, 1046 colaboradores; margen de error, 5.0%; nivel de porcentaje estimado, 50.0%; y, nivel de confianza, 95.0%. Luego, realizando el ingreso de los parámetros indicados anteriormente en el software estadístico se calculó que para 1046 colaboradores se necesita una muestra de 282 colaboradores de la Municipalidad distrital de Lima Sur. En consecuencia, se detalla la siguiente tabla:

Tabla 4

Caracterización de la muestra.

Muestra	Cantidad
Colaboradores de la Municipalidad distrital de Lima Sur	282
Total	282

Nota: En esta tabla se detalla el escalar numérico de la muestra de colaboradores que se está tomando de la población de la Municipalidad distrital de Lima Sur actualizada al año 2021.

Muestreo

Para el presente trabajo de investigación se consideró un muestreo probabilístico simple. Hernández y Mendoza (2018), indican que un muestreo probabilístico simple es aquel que se caracteriza por tener elementos de la muestra del universo con un mismo nivel de probabilidad de elección inicial.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

Se define que la técnica de recolección de datos que se usó en esta investigación es la encuesta. En ese sentido Hernández y Mendoza (2018) argumentan que la encuesta es un tipo de método de recopilación de datos amparada en la formulación de preguntas.

Instrumentos de recolección de datos

Se define que el instrumento de recolección de datos que se usó en este estudio es el cuestionario. En ese sentido Ñaupas et al (2018) indica que el cuestionario es un tipo de encuesta que se fundamenta en la formulación de preguntas escritas sistemáticamente para la obtención de respuestas vinculadas a las variables, objetivos e hipótesis de la investigación. Por otro lado, Hernández y Mendoza (2018) argumentan que la escala de Likert es un conjunto de cinco categorías que se usa para recoger las apreciaciones de los individuos sobre un tema en particular. A continuación, se muestran las especificaciones del instrumento indicado:

Tabla 5

Ficha técnica del instrumento de medición.

Nombre del Instrumento:			Cuestionario para los colaboradores de la Municipalidad de Lima Sur		
Autor:			Miguel Martín Correa Coronel		
Año:			2021		
Tipo de Instrumento:			Cuestionario		
Objetivo:			Determinar la incidencia de la ciberseguridad en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.		
Población:			Colaboradores de la Municipalidad distrital de Lima Sur		
Número de Ítems:			36		
Aplicación:			En línea		
Tiempo de administración:			12 minutos		
Normas de aplicación:			El encuestado debe elegir una entre las cinco categorías de Likert, por ítem (pregunta).		
Escala:			Escala de Likert		
Descripción:			Valor		
Totalmente en desacuerdo			1		
En desacuerdo			2		
Ni de acuerdo ni en desacuerdo			3		
De acuerdo			4		
Totalmente de acuerdo			5		
Niveles:					
Variable: Ciberseguridad			Variable: Tratamiento de datos personales		
Nivel	Valor	Rango	Nivel	Valor	Rango
No óptimo	1	18 – 42	Malo	1	18 – 42
Medio	2	43 – 67	Regular	2	43 – 67
Óptimo	3	68 – 90	Bueno	3	68 – 90

Nota: En esta tabla se detalla la composición de la ficha técnica del instrumento de medición.

Validez

El sustento de validez, que recae en la justificación apropiada de la idoneidad (pertinencia, relevancia y claridad) del cuestionario y sus preguntas de la presente investigación, se fundamentó en el método denominado juicio de experto. En ese sentido Hernández et al (2018) indica que la validez garantiza que el instrumento usado posee la capacidad suficiente para medir aquella característica relevante en la investigación. En ese sentido se muestra la siguiente tabla:

Tabla 6

Validación del instrumento de recolección de datos.

DNI	Grado académico, apellidos y nombres	Institución donde labora	Calificación
10583345	Mtro. Melgar Aliaga, Freud Enrique	Universidad Peruana de Ciencias Aplicadas	Aplicable
09449377	Mtro. Quispe Laguna, Waldir Enrique	Universidad Privada del Norte	Aplicable
44592864	Mtro. Darío Waldyr, Franco Castro	Universidad Tecnológica del Perú	Aplicable

Nota: En esta tabla se detalla la validación del instrumento de recolección de datos.

Confiabilidad

Para Ñaupas et al (2018) la confiabilidad se arraiga fuertemente en la invariación relevante de resultados provenientes del instrumento bajo condiciones semejantes de aplicación. Así también, se empleó el software IBM SPSS Statistics 25 para calcular la ponderación estadística definida como el coeficiente Alfa de Cronbach, que según Ñaupas et al (2018) y Hernández y Mendoza (2018), es un cociente que oscila entre 0 y 1, y que cuando más cercano esté de la unidad, justificará la correlación estadística y la consistencia de la colección de datos para ítems descritos en alguna escala de categorías. Finalmente, en la prueba piloto de esta investigación constituida por 15 encuestados, se logró un resultado de 0,921 y para la prueba general de 282 encuestados, se logró un coeficiente Alfa de Cronbach de 0,994, lo cual sustenta que el instrumento goza de correcta consistencia interna.

Tabla 7

Resultado del coeficiente de Alfa de Cronbach para la prueba piloto y general.

Tipo de aplicación	N.º de encuestados	N.º de elementos	Alfa de Cronbach
Piloto	15	36	0,921
General	282	36	0,994

Nota: En esta tabla se detalla el resultado del coeficiente de Alfa de Cronbach para la prueba de piloto y para prueba general.

3.5. Procedimientos

El procedimiento de la presente investigación inició con la formulación del instrumento de recolección de datos, el mismo que ha sido validado por tres profesionales competentes en materia de investigación mediante el método de juicio

de expertos. Posteriormente, se procedió con la aplicación del cuestionario para la prueba piloto de 15 encuestados, se registró la información obtenida en una hoja de Microsoft Excel y se sometió al software IBM SPSS Statistics 25 para el cálculo del coeficiente de Alfa de Cronbach.

3.6. Método de análisis de datos

El análisis de datos de la presente pesquisa se sustentó en el estudio estadístico descriptivo e inferencial mediante el uso del software IBM SPSS Statistics 25. La base de datos de la investigación se fundamenta en la encuesta realizada, a través del instrumento indicado, a los colaboradores de la Municipalidad distrital de Lima Sur. El análisis descriptivo presentó histogramas y tablas de contingencia dirigidas al análisis bidimensional. El análisis inferencial presentó el método paramétrico haciendo uso del coeficiente de análisis de regresión logística ordinal para justificar, adecuadamente, el grado correlacional existente entre las variables de estudio de esta investigación.

3.7. Aspectos éticos

En la presente pesquisa se cumplió con lo dispuesto en la Resolución de Consejo Universitario N.º 0262-2020/UCV, Código de Ética en Investigación de la Universidad César Vallejo. Así también, se cumplió con lo establecido por el Decreto Legislativo N.º 822 del 24 de abril de 1996, el cual define el marco legal de la Ley sobre el Derecho de Autor. Finalmente, se cumplió cabalmente con los lineamientos de protección establecidos por la Ley de Protección de Datos Personales, Ley N.º 29733, que exige respetar el anonimato y reserva de datos sensibles estipulados en el cuestionario de categorías de la presente investigación.

IV. RESULTADOS

Análisis descriptivos

Análisis descriptivo de la variable ciberseguridad y la variable tratamiento de datos personales

Tabla 8

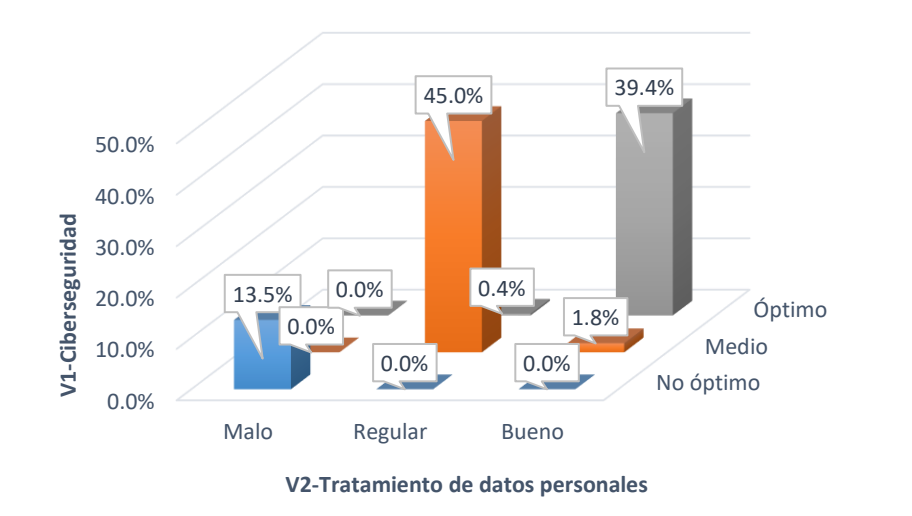
*Tabla cruzada V1: Ciberseguridad * V2: Tratamiento de datos personales.*

		V2-Tratamiento de datos personales			
		Malo	Regular	Bueno	Total
V1-Ciberseguridad	No óptimo	38 (13.5%)	0 (0.0%)	0 (0.0%)	38 (13.5%)
	Medio	0 (0.0%)	127 (45.0%)	5 (1.8%)	132 (46.8%)
	Óptimo	0 (0.0%)	1 (0.4%)	111 (39.4%)	112 (39.7%)
	Total	38 (13.5%)	128 (45.4%)	116 (41.1%)	282 (100.0%)

Nota: Esta información detalla el resultado de la tabla cruzada proveniente de la variable ciberseguridad y tratamiento de datos personales, usando como soporte el software IBM SPSS Statistics 25.

Figura 1

*Histograma, V1:Ciberseguridad * V2:Tratamiento de datos personales.*



En la tabla 8 como y en la figura 1 se evidenció que la mayor frecuencia de aceptación se originó en el cruce del nivel regular de la variable tratamiento de datos personales con el nivel medio de la variable ciberseguridad, haciendo un total de 127 encuestados equivalentes al 45.0% del total.

Análisis descriptivo de la dimensión conservación de la confidencialidad de la variable ciberseguridad y la dimensión principio de consentimiento de la variable tratamiento de datos personales

Tabla 9

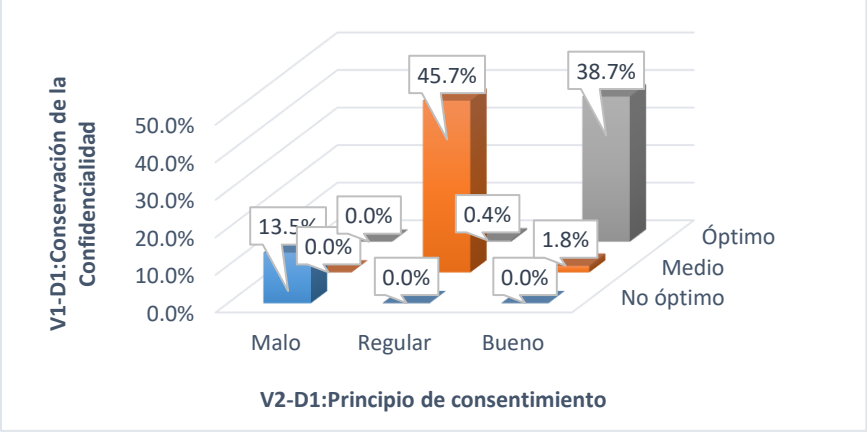
*Tabla cruzada V1-D1:Conservación de la confidencialidad * V2-D1:Principio de consentimiento.*

		V2-D1:Principio de consentimiento			
		Malo	Regular	Bueno	Total
V1-D1:Conservación de la Confidencialidad	No óptimo	38 (13.5%)	0 (0.0%)	0 (0.0%)	38 (13.5%)
	Medio	0 (0.0%)	129 (45.7%)	5 (1.8%)	134 (47.5%)
	Óptimo	0 (0.0%)	1 (0.4%)	109 (38.7%)	110 (39.0%)
	Total	38 (13.5%)	130 (46.1%)	114 (40.4%)	282 (100.0%)

Nota: Esta información detalla el resultado de la tabla cruzada proveniente de la dimensión conservación de la confidencialidad de la variable ciberseguridad y la dimensión principio de consentimiento de la variable tratamiento de datos personales, usando como soporte el software IBM SPSS Statistics 25.

Figura 2

*Histograma, V1-D1:Conservación de la confidencialidad * V2-D1:Principio de consentimiento.*



En la tabla 9 y en la figura 2 se evidenció que la mayor frecuencia de aceptación se originó en el cruce del nivel regular de la dimensión principio de consentimiento de la variable tratamiento de datos personales con el nivel medio de la dimensión conservación de la confidencialidad de la variable ciberseguridad, haciendo un total de 129 encuestados equivalentes al 45.7% del total de encuestados.

Análisis descriptivo de la dimensión Integridad de la variable ciberseguridad y la dimensión principio de calidad de la variable tratamiento de datos personales

Tabla 10

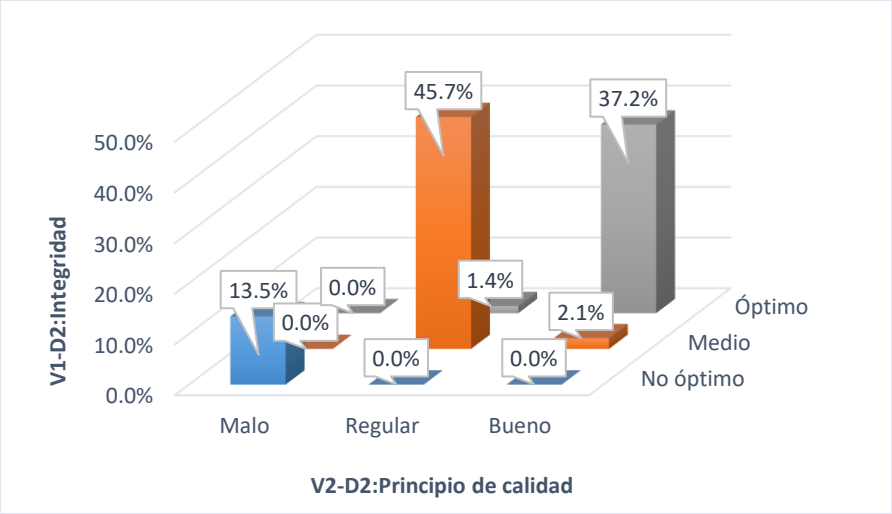
*Tabla cruzada V1-D2:Integridad * V2-D2:Principio de calidad.*

		V2-D2:Principio de calidad			
		Malo	Regular	Bueno	Total
V1-D2: Integridad	No óptimo	38 (13.5%)	0 (0.0%)	0 (0.0%)	38 (13.5%)
	Medio	0 (0.0%)	129 (45.7%)	6 (2.1%)	135 (47.9%)
	Óptimo	0 (0.0%)	4 (1.4%)	105 (37.2%)	109 (38.7%)
	Total	38 (13.5%)	133 (47.2%)	111 (39.4%)	282 (100.0%)

Nota: Esta información detalla el resultado de la tabla cruzada proveniente de la dimensión integridad de la variable ciberseguridad y la dimensión principio de calidad de la variable tratamiento de datos personales, usando como soporte el software IBM SPSS Statistics 25.

Figura 3

*Histograma, V1-D2: Integridad * V2-D2: Principio de calidad.*



En la tabla 10 y en la figura 3 se evidenció que la mayor frecuencia de aceptación se originó en el cruce del nivel regular de la dimensión principio de calidad de la variable tratamiento de datos personales con el nivel medio de la dimensión integridad de la variable ciberseguridad, haciendo un total de 129 encuestados equivalentes al 45.7% del total de encuestados.

Análisis descriptivo de la dimensión disponibilidad de la variable ciberseguridad y la dimensión principio de seguridad de la variable tratamiento de datos personales

Tabla 11

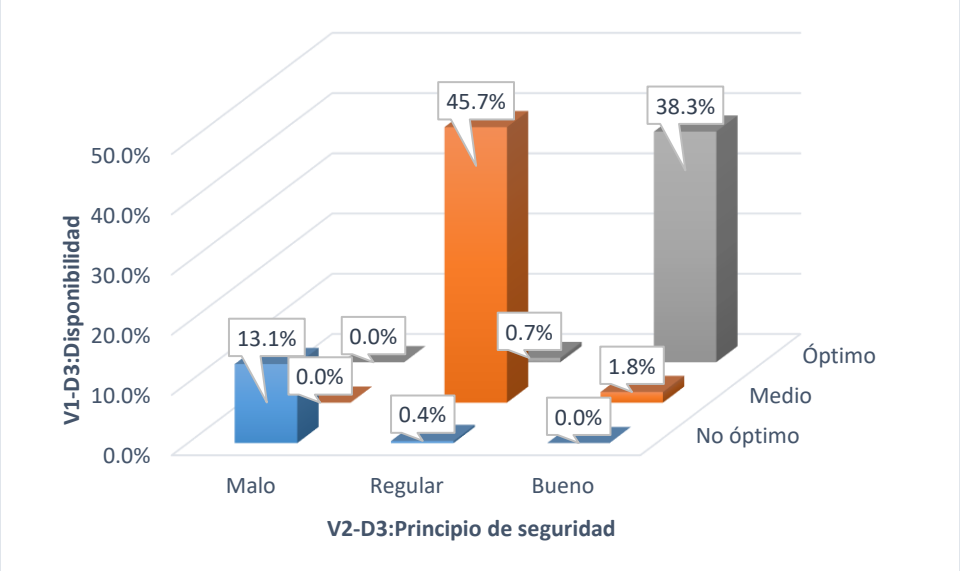
*Tabla cruzada V1-D3:Disponibilidad * V2-D3:Principio de seguridad.*

		V2-D3:Principio de seguridad			
		Malo	Regular	Bueno	Total
V1-D3: Disponibilidad	No óptimo	37 (13.1%)	1 (0.4%)	0 (0.0%)	38 (13.5%)
	Medio	0 (0.0%)	129 (45.7%)	5 (1.8%)	134 (47.5%)
	Óptimo	0 (0.0%)	2 (0.7%)	108 (38.3%)	110 (39.0%)
	Total	37 (13.1%)	132 (46.8%)	113 (40.1%)	282 (100.0%)

Nota: Esta información detalla el resultado de la tabla cruzada proveniente de la dimensión disponibilidad de la variable ciberseguridad y la dimensión principio de seguridad de la variable tratamiento de datos personales, usando como soporte el software IBM SPSS Statistics 25.

Figura 4

*Histograma, V1-D3:Disponibilidad * V2-D3:Principio de seguridad.*



En la tabla 11 y en la figura 4 se evidenció que la mayor frecuencia de aceptación se originó en el cruce del nivel regular de la dimensión principio de seguridad de la variable tratamiento de datos personales con el nivel medio de la dimensión disponibilidad de la variable ciberseguridad, haciendo un total de 129 encuestados equivalentes al 45.7% del total de encuestados.

Análisis inferencial

Prueba de hipótesis

En el análisis inferencial de la presente investigación se optó por el método paramétrico de coeficiente de análisis de Regresión Logística Ordinal (RLO), el cual busca precisar el grado de relación causal de las dos variables en estudio. Según Koletsi y Pandis (2018), la RLO es recomendable cuando se busca predecir el comportamiento de la variable dependiente en términos de categorías ordinales en escala que varían según un determinado número de respuestas predefinidas. En ese sentido se definió el modelo de RLO para esta investigación y se estableció el cumplimiento de los prerrequisitos estadísticos correspondientes. Finalmente, se recurrió al uso de la prueba de Wald para asegurar lo descrito respecto al modelo de RLO.

Prueba de hipótesis general

A continuación, se formuló la hipótesis estadística indicada:

H_1: Existe incidencia significativa entre la variable ciberseguridad y la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

H_0: No existe incidencia significativa entre la variable ciberseguridad y la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Contrastación de hipótesis estadística:

Tabla 12

Información sobre el ajuste del modelo que explica la incidencia de la variable ciberseguridad en la variable tratamiento de datos personales.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	512.090			
Final	9.227	502.862	1	0.000

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

De la tabla 12 se desprendió un valor de significancia final de 0.000, y siendo este valor menor a 0.05 (cinco centésimos), damos por aceptada la hipótesis alterna H1 de la prueba de hipótesis general, haciendo presente que el modelo logístico ordinal aplicado goza de relevancia plena en el contexto de la presente investigación y coligiendo que existe incidencia significativa entre la variable ciberseguridad y la variable tratamiento de datos personales.

Tabla 13

Bondad de ajuste de la incidencia de la variable ciberseguridad en la variable tratamiento de datos personales.

	Chi-cuadrado	gl	Sig.
Pearson	2.970	3	0.396
Desvianza	3.794	3	0.285

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 12, se indica el valor final de ajuste del modelo Chi-cuadrado, el cual es 502.862. Además, en la tabla 13 se indica el valor de la prueba de independencia Chi-cuadrado-Pearson, el cual es 2.970. Luego, sabiendo que 521.707 < 2.970 es incorrecta, se debe rechazar que las variables ciberseguridad y tratamiento de datos personales son estadísticamente independientes y, por ende, asumir que la variable ciberseguridad incide significativamente en la variable tratamiento de datos personales. Finalmente, el nivel de significancia expresado en la tabla 13 corresponde a 0.396, valor que es mayor que 0.05 lo cual justifica que los datos observados son consistentes con el modelo indicado.

Tabla 14

Pseudo R Cuadrado de la incidencia de la variable ciberseguridad en la variable tratamiento de datos personales.

Coeficiente R^2	Valor
Cox y Snell	0.832
Nagelkerke	0.964
McFadden	0.897

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 14 se evidenció un valor de 0.964 para el coeficiente Pseudo R Cuadrado de Nagelkerke, cuya interpretación porcentual del 96.4% recae en la suposición de que cuando este valor tiende más su cercanía a la unidad, entonces se goza de un modelo mucho más ajustado que describe una adecuada predicción de la variable ciberseguridad en relación a la variable tratamiento de datos personales. Así también, se puede aducir que el 96.4% de la varianza es explicada por la variable independiente ciberseguridad sobre la variable dependiente tratamiento de datos personales.

Tabla 15

Estimaciones de los parámetros de incidencia de la variable ciberseguridad en la variable tratamiento de datos personales.

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[V2 = 1]	13.257	2.077	40.722	1	0.000	9.185	17.329
	[V2 = 2]	21.903	2.640	68.815	1	0.000	16.728	27.079
Ubicación	V1	9.256	1.256	54.305	1	0.000	6.794	11.717

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 15 se observó que la estimación de la variable independiente ciberseguridad registró un valor de 9.256, del mismo modo se logró un valor de significancia de 0.000 para la prueba de Wald, el cual es mayor a 1. Luego, se puede inferir que después de aplicar el coeficiente estadístico de RLO se logró un P valor de 0.000 , menor al error significativo de 0.05, por lo tanto, se rechaza la hipótesis nula (H_0). Finalmente, se sustenta contundentemente, con suficiente evidencia estadística, que existe incidencia significativa entre la variable ciberseguridad y la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Prueba de hipótesis especifica 1:

A continuación, se formuló la hipótesis estadística indicada:

H_1: Existe incidencia significativa entre la dimensión conservación de la confidencialidad de la ciberseguridad y la dimensión principio de consentimiento

del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

H_0: No existe incidencia significativa entre la dimensión conservación de la confidencialidad de la ciberseguridad y la dimensión principio de consentimiento del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Contrastación de hipótesis estadística:

Tabla 16

Información sobre el ajuste del modelo que explica la incidencia de la dimensión conservación de la confidencialidad de la variable ciberseguridad en la dimensión principio de consentimiento de la variable tratamiento de datos personales.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	511.513			
Final	9.252	502.261	1	0.000

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

De la tabla 16 se desprendió un valor de significancia final de 0.000, y siendo este valor menor a 0.05 (cinco centésimos), damos por aceptada la hipótesis alterna H1 de la prueba de hipótesis especifica 1, haciendo presente que el modelo logístico ordinal aplicado goza de relevancia plena en el contexto de la presente investigación y coligiendo que existe incidencia significativa entre la dimensión conservación de la confidencialidad de la variable ciberseguridad y la dimensión principio de consentimiento de la variable tratamiento de datos personales.

Tabla 17

Bondad de ajuste de la incidencia de la dimensión conservación de la confidencialidad de la variable ciberseguridad en la dimensión principio de consentimiento de la variable tratamiento de datos personales.

	Chi-cuadrado	gl	Sig.
Pearson	3.002	3	0.391
Desvianza	3.819	3	0.282

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 16 se indica el valor final de ajuste del modelo Chi-cuadrado, el cual es 502.261. Además, en la tabla 17 se indica el valor de la prueba de independencia Chi-cuadrado-Pearson, el cual es 3.002. Luego, sabiendo que 502.261 < 3.002 es incorrecta, se aceptar que la dimensión conservación de la confidencialidad de la variable ciberseguridad incide significativamente en la dimensión principio de consentimiento de la variable tratamiento de datos personales. Finalmente, el nivel de significancia expresado en la tabla 17 corresponde a 0.391 (391 milésimos), valor que es mayor que 0.05 lo cual justifica que los datos observados son consistentes con el modelo indicado.

Tabla 18

Pseudo R Cuadrado de la incidencia de la dimensión conservación de la confidencialidad de la variable ciberseguridad en la dimensión principio de consentimiento de la variable tratamiento de datos personales.

Coeficiente R^2	Valor
Cox y Snell	0.832
Nagelkerke	0.964
McFadden	0.897

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 18 se evidenció un valor de 0.964 para el coeficiente Pseudo R Cuadrado de Nagelkerke, cuya interpretación porcentual del 96.4% recae en la suposición de que cuando este valor tiende más su cercanía a la unidad, entonces se goza de un modelo mucho más ajustado que describe una adecuada predicción de la dimensión conservación de la confidencialidad de la variable ciberseguridad en relación a la dimensión principio de consentimiento de la variable tratamiento de datos personales. Así también, se puede aducir que el 96.4% de la varianza es explicada por la dimensión conservación de la confidencialidad de la variable ciberseguridad sobre la dimensión principio de consentimiento de la variable tratamiento de datos personales.

Tabla 19

Estimaciones de los parámetros de incidencia de la dimensión conservación de la confidencialidad de la variable ciberseguridad en la dimensión principio de consentimiento de la variable tratamiento de datos personales.

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[V1-D1 = 1]	13.260	2.078	40.710	1	0.000	9.187	17.333
	[VA2-D1 = 2]	21.933	2.642	68.924	1	0.000	16.755	27.112
Ubicación	V1-D1	9.263	1.257	54.294	1	0.000	6.799	11.726

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 19 se observó que la estimación de la dimensión conservación de la confidencialidad de la variable ciberseguridad registró un valor de 9.263, del mismo modo se logró un valor de significancia de 0.000 para la prueba de Wald, el cual es mayor a 1. Luego, se puede inferir que después de aplicar el coeficiente estadístico de RLO se logró un P valor de 0.000 , menor al error significativo de 0.05, por lo tanto, se rechaza la hipótesis nula (H_0). Finalmente, se sustenta contundentemente, con suficiente evidencia estadística, que existe incidencia significativa entre la dimensión conservación de la confidencialidad de la variable ciberseguridad y la dimensión principio de consentimiento de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Prueba de hipótesis específica 2:

A continuación, se formuló la hipótesis estadística indicada:

H_1: Existe incidencia significativa entre la dimensión integridad de la variable ciberseguridad y la dimensión principio de calidad de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

H_0: No existe incidencia significativa entre la dimensión Integridad de la variable ciberseguridad y la dimensión principio de calidad de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Contrastación de hipótesis estadística:

Tabla 20

Información sobre el ajuste del modelo que explica la incidencia de la dimensión integridad de la variable ciberseguridad en la dimensión principio de calidad de la variable tratamiento de datos personales.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	482.688			
Final	15.968	466.719	1	0.000

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

De la tabla 20 se desprendió un valor de significancia final de 0.000, y siendo este valor menor a 0.05 (cinco centésimos), damos por aceptada la hipótesis alterna H1 de la prueba de hipótesis especifica 2, haciendo presente que el modelo logístico ordinal aplicado goza de relevancia plena en el contexto de la presente investigación y coligiendo que existe incidencia significativa entre la dimensión integridad de la variable ciberseguridad y la dimensión principio de calidad de la variable tratamiento de datos personales.

Tabla 21

Bondad de ajuste de la incidencia de la dimensión integridad de la variable ciberseguridad en la dimensión principio de calidad de la variable tratamiento de datos personales.

	Chi-cuadrado	gl	Sig.
Pearson	5.925	3	0.115
Desvianza	9.128	3	0.028

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 20 se indica el valor final de ajuste del modelo Chi-cuadrado, el cual es 466.719. Además, en la tabla 21 se indica el valor de la prueba de independencia Chi-cuadrado-Pearson, el cual es 5.925. Luego, sabiendo que 466.719 < 5.925 es incorrecta, se debe aceptar que la dimensión conservación de la confidencialidad de la variable ciberseguridad incide significativamente en la dimensión principio de consentimiento de la variable tratamiento de datos personales. Finalmente, el nivel

de significancia expresado en la tabla 21 corresponde a 0.115 (115 milésimos), valor que es mayor que 0.05 lo cual justifica que los datos observados son consistentes con el modelo indicado.

Tabla 22

Pseudo R Cuadrado de la incidencia de la dimensión integridad de la variable ciberseguridad en la dimensión principio de calidad de la variable tratamiento de datos personales.

Coeficiente R^2	Valor
Cox y Snell	0.809
Nagelkerke	0.938
McFadden	0.835

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 22 se evidenció un valor de 0.938 para el coeficiente Pseudo R Cuadrado de Nagelkerke, cuya interpretación porcentual del 93.8% recae en la suposición de que cuando este valor tiende más su cercanía a la unidad, entonces se goza de un modelo mucho más ajustado que describe una adecuada predicción de la dimensión integridad de la variable ciberseguridad en relación a la dimensión principio de calidad de la variable tratamiento de datos personales. Así también, se puede aducir que el 93.8% de la varianza es explicada por la dimensión integridad de la variable ciberseguridad sobre la dimensión principio de calidad de la variable tratamiento de datos personales.

Tabla 23

Estimaciones de los parámetros de incidencia de la dimensión integridad de la variable ciberseguridad en la dimensión principio de calidad de la variable tratamiento de datos personales.

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[V1-D2 = 1]	10.334	1.135	82.851	1	0.000	8.109	12.559
	[VA2-D2 = 2]	18.085	1.597	128.20	1	0.000	14.954	21.216
Ubicación	V1-D2	7.319	0.659	123.31	1	0.000	6.027	8.611

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 23 se observó que la estimación de la dimensión Integridad de la variable ciberseguridad registró un valor de 7.319, del mismo modo se logró un valor de significancia de 0.000 para la prueba de Wald, el cual es mayor a 1. Luego, se puede inferir que después de aplicar el coeficiente estadístico de RLO se logró un P valor de 0.000 , menor al error significativo de 0.05, por lo tanto, se rechaza la hipótesis nula (H_0). Finalmente, se sustenta contundentemente, con suficiente evidencia estadística, que existe incidencia significativa entre la dimensión integridad de la variable ciberseguridad y la dimensión principio de calidad de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Prueba de hipótesis específica 3:

A continuación, se formuló la hipótesis estadística indicada:

H_1: Existe incidencia significativa entre la dimensión disponibilidad de la variable ciberseguridad y la dimensión principio de seguridad de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

H_0: No existe incidencia significativa entre la dimensión disponibilidad de la variable ciberseguridad y la dimensión principio de seguridad de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

Contrastación de hipótesis estadística:

Tabla 24

Información sobre el ajuste del modelo que explica la incidencia de la dimensión disponibilidad de la variable ciberseguridad en la dimensión principio de seguridad de la variable tratamiento de datos personales.

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	493.453			
Final	10.942	482.512	1	0.000

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

De la tabla 24 se desprendió un valor de significancia final de 0.000, y siendo este valor menor a 0.05 (cinco centésimos), damos por aceptada la hipótesis alterna H1 de la prueba de hipótesis especifica 3, haciendo presente que el modelo logístico

ordinal aplicado goza de relevancia plena en el contexto de la presente investigación y coligiendo que existe incidencia significativa entre la dimensión disponibilidad de la variable ciberseguridad y la dimensión principio de seguridad de la variable tratamiento de datos personales.

Tabla 25

Bondad de ajuste de la incidencia de la dimensión disponibilidad de la variable ciberseguridad en la dimensión principio de seguridad de la variable tratamiento de datos personales.

	Chi-cuadrado	gl	Sig.
Pearson	2.118	3	0.548
Desvianza	2.930	3	0.403

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 24 se indica el valor final de ajuste del modelo Chi-cuadrado, el cual es 482.512. Además, en la tabla 25 se indica el valor de la prueba de independencia Chi-cuadrado-Pearson, el cual es 2.118. Luego, sabiendo que 482.512 < 2.118 es incorrecta, se debe aceptar que la dimensión disponibilidad de la variable ciberseguridad incide significativamente en la dimensión principio de seguridad de la variable tratamiento de datos personales. Finalmente, el nivel de significancia expresado en la tabla 25 corresponde a 0.548 (548 milésimos), valor que es mayor que 0.05 lo cual justifica que los datos observados son consistentes con el modelo indicado.

Tabla 26

Pseudo R Cuadrado de la incidencia de la dimensión disponibilidad de la variable ciberseguridad en la dimensión principio de seguridad de la variable tratamiento de datos personales.

Coeficiente R^2	Valor
Cox y Snell	0.819
Nagelkerke	0.951
McFadden	0.866

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 26 se evidenció un valor de 0.951 para el coeficiente Pseudo R Cuadrado de Nagelkerke, cuya interpretación porcentual del 95.1% recae en la suposición de que cuando este valor tiende más su cercanía a la unidad, entonces se goza de un modelo mucho más ajustado que describe una adecuada predicción de la dimensión disponibilidad de la variable ciberseguridad en relación a la dimensión principio de seguridad de la variable tratamiento de datos personales. Así también, se puede aducir que el 95.1% de la varianza es explicada por la dimensión disponibilidad de la variable ciberseguridad sobre la dimensión principio de seguridad de la variable tratamiento de datos personales.

Tabla 27

Estimaciones de los parámetros de incidencia de la dimensión disponibilidad de la variable ciberseguridad en la dimensión principio de seguridad de la variable tratamiento de datos personales.

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[V1-D3 = 1]	10.977	1.259	75.98	1	0,00	8.509	13.445
	[VA2-D3 = 2]	19.468	1.884	106.83	1	0,00	15.777	23.160
Ubicación	V1-D3	8.008	0.826	94.04	1	0,00	6.390	9.627

Nota: Información procesada mediante el software IBM SPSS Statistics 25.

En la tabla 27 se observó que la estimación de la dimensión integridad de la variable ciberseguridad registró un valor de 8.008, del mismo modo se alcanzó un valor de significancia de 0.000 para la prueba de Wald, el cual es mayor a 1. Luego, se puede

inferir que después de aplicar el coeficiente estadístico de RLO se alcanzó un P valor de 0.000 , menor al error significativo de 0.05, por lo tanto, se rechaza la hipótesis nula (H_0). Finalmente, se sustenta contundentemente, con suficiente evidencia estadística, que existe incidencia significativa entre la dimensión disponibilidad de la variable ciberseguridad y la dimensión principio de seguridad de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

V. DISCUSIÓN

Respecto al objetivo general

A continuación, se expone la discusión de los resultados conseguidos para la presente investigación, respecto a la incidencia de la variable ciberseguridad en la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

En el análisis descriptivo, se evidenció que el nivel regular de la variable tratamiento de datos personales se relacionó en un 45.0% con el nivel medio de la variable ciberseguridad. Así también, se constató que el nivel bueno de la variable tratamiento de datos personales se relacionó en un 39.4% con el nivel óptimo de la variable ciberseguridad. Por otro lado, se verificó que el nivel malo de la variable tratamiento de datos personales se relacionó en un 13.5% con el nivel no óptimo de la variable ciberseguridad. Finalmente, los niveles bueno y medio; y, regular y óptimo, de las variables tratamiento de datos personales y ciberseguridad, se vincularon en un 1.8% y 0.4%, respectivamente.

En el análisis inferencial, en primer lugar, se concluyó que el modelo de RLO es relevante para la presente investigación, dado que en la prueba de ajuste del modelo se registró un valor de significancia de 0,000, cifra que es inferior a 0.05. En esa misma línea, se determinó que los datos analizados inferencialmente, sí gozan de consistencia con el modelo de RLO, dado que se alcanzó un valor de significancia para la prueba Chi-cuadrado de Pearson expresado en la tabla 13 correspondiente a 0.396, valor que es mayor que 0.05. Además, el valor registrado para el Pseudo R Cuadrado de Nagelkerke implica que el 96.4 % de la varianza es explicada por la variable independiente ciberseguridad sobre la variable dependiente tratamiento de datos personales. Finalmente, se pudo justificar que el coeficiente estadístico del modelo RLO para la estimación de parámetros de incidencia es de 9.256, involucrando un valor de significancia con tendencia al 0. 000, siendo esta última cifra menor que 0.05, se pudo afirmar que sí existe

incidencia significativa de la variable ciberseguridad sobre la variable tratamiento de datos personales.

Los resultados señalados líneas arriba concuerdan con los hallados por Choejey, Murray y Che (2017) que indican concluyentemente que la implementación de la ciberseguridad en las empresas influye en un 40.0% sobre la política de ciberseguridad (protección de datos) de la organización.

En esa misma línea, Stefaniuk (2020) concluye en su investigación que existe una correspondencia significativa entre los sistemas de gestión de seguridad de la información en la organización (ciberseguridad) y la publicación de la Política de seguridad de la información (protección de datos), en donde el aumento del 12.0% de la primera, repercute en el aumento del 18.0% de la segunda, respectivamente.

Por otra parte, Luh y Yen (2020) en su investigación consideran que la ciberseguridad incide sobre los problemas de privacidad de datos de pacientes clínicos, permitiendo establecer una relación entre ambas variables. Por otro lado, Markopoulou, Papakonstantinou y De Hert (2019), sostienen en su pesquisa que la Ley de ciberseguridad de la Unión Europea (UE) incide ciertamente sobre Reglamento General de Protección de Datos de la misma UE, reafirmando nuevamente la existencia de la relación entre la ciberseguridad y la protección de datos. Así también, Pérez y Ramos (2020) sustentan en su investigación que una Política de ciberseguridad se relaciona directamente con la protección de la información digital en una institución gubernamental. De esta forma se sustenta que la ciberseguridad y la protección de la información (o tratamiento de datos personales) inciden una sobre la otra, correlacionalmente hablando. De igual manera, citamos a Javid, Faris, Beenish y Fahad (2020) que en su investigación sostienen que existe una correlación directa entre ciberseguridad y la privacidad de datos en la industria de la salud.

Del mismo modo, Taípe (2020) argumenta en su pesquisa que existe una correspondencia significativa entre la ciberseguridad con respecto a los riesgos de la información digital del sector público durante el año 2018, dado que en la investigación citada la prueba de correlación de Spearman mostró una significancia

de 0.003 (menor a cinco centésimos); a su vez, calculando el coeficiente de correlación Rho de Spearman se obtuvo 314 milésimos con lo cual se define una correlación proporcional directa y de intensidad promedia entre las variables descritas. Finalmente, la ciberseguridad en el sector público y las políticas de ciberseguridad (seguridad de la información y datos) se relacionan en los niveles muy alto y óptimo, respectivamente, en un 35.3%.

Así también, Bohorquez (2021) señala en su investigación que la ciberseguridad se relaciona significativamente (nivel de correlación de nivel muy fuerte) con la gestión de tecnologías de información a consecuencia del cálculo del coeficiente Rho de Spearman equivalente a 832 milésimos. Finalmente, la relación entre la ciberseguridad y la gestión de tecnologías de información se relacionan en los niveles de alta prevalencia y óptimo, reactivamente, en un 14.1%.

Por su parte, Villarrubia (2021) en la argumentación de su investigación concluye que el tratamiento de datos y la protección de la información digital se relacionan directamente con la Política de seguridad y la defensa nacional. Finalmente, se concuerda también con Zúñiga (2017), quien sostiene que existe una incidencia significativa entre la ciberdefensa y la protección de datos e información del Ejército del Perú.

Respecto al objetivo específico 1

A continuación, se expone la discusión de los resultados conseguidos para la presente investigación, respecto a la incidencia de la dimensión conservación de la confidencialidad de la variable ciberseguridad en la dimensión principio de consentimiento de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

En el análisis descriptivo, se evidenció que el nivel regular de la dimensión principio de consentimiento de la variable tratamiento de datos personales se relacionó en un 45.7% con el nivel medio de la dimensión conservación de la confidencialidad de la variable ciberseguridad. Así también, se constató que el nivel

bueno de la dimensión principio de consentimiento de la variable tratamiento de datos personales se relacionó en un 38.7% con el nivel óptimo de la dimensión conservación de la confidencialidad de la variable ciberseguridad. Por otro lado, se verificó que el nivel malo de la dimensión principio de consentimiento de la variable tratamiento de datos personales se relacionó en un 13.5% con el nivel no óptimo de la dimensión conservación de la confidencialidad de la variable ciberseguridad. Finalmente, los niveles bueno y medio; y, regular y óptimo, de la dimensión principio de consentimiento de la variable tratamiento de datos personales y la dimensión conservación de la confidencialidad de la variable ciberseguridad se vincularon en un 1.8% y 0.4%, respectivamente.

En el análisis inferencial, en primer lugar, se concluyó que el modelo de RLO es relevante para la presente investigación, dado que en la prueba de ajuste del modelo se registró un valor de significancia de 0.000, cifra que es inferior a 0.05. En esa misma línea, se determinó que los datos analizados inferencialmente, sí gozan de consistencia con el modelo de RLO, dado que se alcanzó un valor de significancia para la prueba Chi-cuadrado de Pearson expresado en la tabla 17 correspondiente a 0.391, valor que es mayor que 0.05. Además, el valor registrado para el Pseudo R Cuadrado de Nagelkerke implica que el 96.4 % de la varianza es explicada por la dimensión conservación de la confidencialidad de la variable ciberseguridad sobre la dimensión principio de consentimiento de la variable tratamiento de datos personales. Finalmente, se pudo justificar que el coeficiente estadístico del modelo RLO para la estimación de parámetros de incidencia es de 9.263, involucrando un valor de significancia con tendencia al 0.000, siendo esta última cifra menor que 0.05, se pudo afirmar que sí existe incidencia significativa de la dimensión conservación de la confidencialidad de la variable ciberseguridad sobre la dimensión principio de consentimiento de la variable tratamiento de datos personales.

Los resultados señalados líneas arriba concuerdan con lo indicado en la investigación de Luh y Yen (2020), donde se alega que garantizar el acceso exclusivo de la información de pacientes por parte de personal autorizado

(conservación de la confidencialidad) incide ciertamente en la predisposición de los pacientes para conceder su consentimiento (principio de consentimiento) en el tratamiento de sus datos personales de índole de salud. De forma similar, Javid, Faris, Beenish y Fahad (2020) sostienen en su investigación que la protección de datos e información (conservación de la confidencialidad) a través de algoritmos computacionales de criptografía incide ciertamente en la preservación de la privacidad de los datos y esto, a su vez, incentiva de forma correcta el otorgamiento de los permisos necesarios para el tratamiento de datos (principio de consentimiento) de usuarios en el sector de la industria de la salud.

Respecto al objetivo específico 2

A continuación, se expone la discusión de los resultados conseguidos para la presente investigación, respecto a la incidencia de la dimensión integridad de la variable ciberseguridad en la dimensión principio de calidad de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

En el análisis descriptivo, se evidenció que el nivel regular de la dimensión principio de calidad de la variable tratamiento de datos personales se relacionó en un 45.7% con el nivel medio de la dimensión integridad de la variable ciberseguridad. Así también, se constató que el nivel bueno de la dimensión principio de calidad de la variable tratamiento de datos personales se relacionó en un 37.2% con el nivel óptimo de la dimensión integridad de la variable ciberseguridad. Por otro lado, se verificó que el nivel malo de la dimensión principio de calidad de la variable tratamiento de datos personales se relacionó en un 13.5% con el nivel no óptimo de la dimensión integridad de la variable ciberseguridad. Finalmente, los niveles bueno y medio; y, regular y óptimo, de la dimensión principio de calidad de la variable tratamiento de datos personales y la dimensión integridad de la variable ciberseguridad, se vincularon en un 2.1% y 1.4%, respectivamente.

En el análisis inferencial, en primer lugar, se concluyó que el modelo de RLO es relevante para la presente investigación, dado que en la prueba de ajuste del

modelo se registró un valor de significancia de 0.000, cifra que es inferior a 0.05. En esa misma línea, se determinó que los datos analizados inferencialmente, sí gozan de consistencia con el modelo de RLO, dado que se alcanzó un valor de significancia para la prueba Chi-cuadrado de Pearson expresado en la tabla 21 correspondiente a 0.115, valor que es mayor que 0.05. Además, el valor registrado para el Pseudo R Cuadrado de Nagelkerke implica que el 93.8 % de la varianza es explicada por la dimensión integridad de la variable ciberseguridad sobre la dimensión principio de calidad de la variable tratamiento de datos personales. Finalmente, se pudo justificar que el coeficiente estadístico del modelo RLO para la estimación de parámetros de incidencia es de 7.319, involucrando un valor de significancia con tendencia al 0, 000, siendo esta última cifra menor que 0.05, se pudo afirmar que sí existe incidencia significativa de la dimensión integridad de la variable ciberseguridad sobre la dimensión principio de calidad de la variable tratamiento de datos personales.

Los resultados señalados líneas arriba concuerdan con lo indicado en la investigación de Markopoulou, Papakonstantinou y De Hert (2019), donde se alega que la preservación de datos tal como fueron recepcionados (Integridad), según la directiva Security of Network and Information Systems (NIS) de la Unión Europea, se relaciona con la presunción de que los datos personales gozan de exactitud y de veracidad (principio de calidad), según la General Data Protection Regulation (GDPR) de la misma entidad internacional. Por su parte, Javid, Faris, Beenish y Fahad (2020) sostienen en su investigación que la disponibilidad de datos e información (Integridad) a través de algoritmos computacionales de criptografía incide en la precisión y exactitud de los datos personales (principio de calidad) de usuarios cuando estos son sometidos en estudios de Big Data.

Respecto al objetivo específico 3

A continuación, se expone la discusión de los resultados conseguidos para la presente investigación, respecto a la incidencia de la dimensión disponibilidad de la

variable ciberseguridad en la dimensión principio de seguridad de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.

En el análisis descriptivo, se evidenció que el nivel regular de la dimensión principio de seguridad de la variable tratamiento de datos personales se relacionó en un 45.7% con el nivel medio de la dimensión disponibilidad de la variable ciberseguridad. Así también, se constató que el nivel bueno de la dimensión principio de seguridad de la variable tratamiento de datos personales se relacionó en un 38.3% con el nivel óptimo de la dimensión disponibilidad de la variable ciberseguridad. Por otro lado, se verificó que el nivel malo de la dimensión principio de seguridad de la variable tratamiento de datos personales se relacionó en un 13.1% con el nivel no óptimo de la dimensión disponibilidad de la variable ciberseguridad. Finalmente, los niveles bueno y medio; y, regular y óptimo, de la dimensión principio de seguridad de la variable tratamiento de datos personales y la dimensión disponibilidad de la variable ciberseguridad, se vincularon en un 1.8% y 0.7%, respectivamente.

En el análisis inferencial, en primer lugar, se concluyó que el modelo de RLO es relevante para la presente investigación, dado que en la prueba de ajuste del modelo se registró un valor de significancia de 0,000, cifra que es inferior a 0.05. En esa misma línea, se determinó que los datos analizados inferencialmente, sí gozan de consistencia con el modelo de RLO, dado que se alcanzó un valor de significancia para la prueba Chi-cuadrado de Pearson expresado en la tabla 25 correspondiente a 0.548, valor que es mayor que 0.05. Además, el valor registrado para el Pseudo R Cuadrado de Nagelkerke implica que el 95.1 % de la varianza es explicada por la dimensión disponibilidad de la variable ciberseguridad sobre la dimensión principio de seguridad de la variable tratamiento de datos personales. Finalmente, se pudo justificar que el coeficiente estadístico del modelo RLO para la estimación de parámetros de incidencia es de 8.008, involucrando un valor de significancia con tendencia al 0.000, siendo esta última cifra menor que 0.05, se pudo afirmar que sí existe incidencia significativa de la dimensión disponibilidad de

la variable ciberseguridad sobre la dimensión principio de seguridad de la variable tratamiento de datos personales.

Los resultados señalados líneas arriba concuerdan con lo indicado en la investigación de Javid, Faris, Beenish y Fahad (2020), quienes postulan que existe una correspondencia entre la ciberseguridad que garantiza que la información debe ser accedida a través de los medios regulares, siempre que sea necesario acceder a ella (disponibilidad), y la privacidad para las comunicaciones de datos biométricos e inalámbricos, que deben ser protegidos de toda adulteración y pérdida (principio de seguridad). Del mismo modo, Taípe (2020) indicó en su investigación la existencia de una relación significativa entre la ciberseguridad (expresada en la disponibilidad de acceder por medios específicos a la información) y los riesgos de la información digital del sector público expresado en la posibilidad de adoptar medidas que tengan como fin mitigar toda pérdida o corrupción de la información (principio de seguridad).

Respecto a la metodología de investigación

La metodología utilizada en esta investigación permitió determinar la incidencia de la variable independiente ciberseguridad en la variable dependiente tratamiento de datos personales, dado que se estableció una relación causal entre ambas variables mencionadas. Así también, al tratarse de una investigación aplicada y al sustentarse las relaciones entre las dimensiones de cada una de las variables definidas, se pudo aportar, dentro de las limitaciones propias de la investigación, ciertos conocimientos en el ámbito tecnológico que sirvieron de asidero, dentro de las perspectivas de la ciberseguridad y que repercutieron en el tratamiento de datos personales en la Municipalidad distrital de Lima Sur. Así también, se recolectó y analizó diferentes teorías para comprender el comportamiento de las variables de esta investigación. Así también, hay que tener presente que el diseño de la investigación fue del tipo de no experimental. Esto permitió contextualizar y analizar las variables tal como ellas se comportan en la realidad circundante, sin necesidad de que el investigador interfiera en ellas. Por otro lado, es preciso señalar el uso y aporte del cuestionario

en línea como instrumento de recolección de datos, dado que permitió obtener información de manera remota, sencilla y muy útil para la investigación, sobre todo en el contexto actual de la pandemia de la Covid-19, que sin duda alguna es factor limitante para toda investigación en estos tiempos. Así también, debemos tener presente que todo estudio sustentado en encuestas siempre presenta cierto sesgo subjetivo propio de la percepción del encuestado. También es importante mencionar que los objetivos expuestos y sustentados en esta investigación permitieron a la Municipalidad distrital de Lima Sur conocer mejor la realidad vinculante entre la ciberseguridad y el tratamiento de datos personales. En ese sentido, la investigación colabora científicamente en el entendimiento de esta variables tecnológicas y sociales.

Finalmente, la relevancia científica de esta investigación recae en todo lo fundamentado desde la perspectiva estadística inferencial, amparándose en los estadísticos descritos y en las pruebas estadísticas matemáticas detalladas en los capítulos anteriores, en consecuencia, esta investigación puede ser replicada de forma similar en otras municipalidades distritales de Lima Sur esperando tener resultados isomorfos a los descritos en esta investigación.

VI. CONCLUSIONES

Primero Para la variable ciberseguridad se registró un valor de estimación de 9.256 y un P valor de significancia de 0.000 en la prueba de Wald (ver tabla 15), por ende, se concluye que sí existe incidencia sobre la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021. De esta forma se da por alcanzado el objetivo general de la investigación. Asimismo, descriptivamente, solo se pudo establecer que el 39.4% (ver tabla 10) de los encuestados considera que la variable tratamiento de datos personales posee un nivel bueno ante la incidencia óptima de la variable ciberseguridad.

Segundo Para la dimensión conservación de la confidencialidad de la variable ciberseguridad se registró un valor de estimación de 9.263 y un P valor de significancia de 0.000 en la prueba de Wald (ver tabla 19), por ende, se concluye que sí existe incidencia sobre la dimensión principio de consentimiento de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021. De esta forma se da por alcanzado el objetivo específico 1 de la investigación. Asimismo, descriptivamente, solo se pudo establecer que el 38.7% (ver tabla 9) de los encuestados considera que la dimensión principio de consentimiento de la variable tratamiento de datos personales posee un nivel bueno ante la incidencia óptima de la dimensión conservación de la confidencialidad de la variable ciberseguridad.

Tercero Para la dimensión Integridad de la variable ciberseguridad se registró un valor de estimación de 7.319 y un P valor de significancia de 0.000 en la prueba de Wald (ver tabla 23), por ende, se concluye que sí existe incidencia sobre la dimensión principio de calidad de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021. De esta forma se da por alcanzado el objetivo específico 2 de la investigación. Asimismo, descriptivamente, solo se pudo establecer que el 37.2% (ver tabla 10) de los encuestados considera

que la dimensión principio de calidad de la variable tratamiento de datos personales posee un nivel bueno ante la incidencia óptima de la dimensión integridad de la variable ciberseguridad.

Cuarto Para la dimensión disponibilidad de la variable ciberseguridad se registró un valor de estimación de 8.008 y un P valor de significancia de 0.000 en la prueba de Wald (ver tabla 27), por ende, se concluye que sí existe incidencia sobre la dimensión principio de seguridad de la variable tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021. De esta forma se da por alcanzado el objetivo específico 3 de la investigación. Asimismo, descriptivamente, solo se pudo establecer que el 38.3% (ver tabla 11) de los encuestados considera que la dimensión principio de seguridad de la variable tratamiento de datos personales posee un nivel bueno ante la incidencia óptima de la dimensión disponibilidad de la variable ciberseguridad.

VII. RECOMENDACIONES

Primero Dado que la variable ciberseguridad tiene incidencia sobre la variable tratamiento de datos personales, se recomienda a la Gerencia municipal de la Municipalidad distrital de Lima Sur realizar un proyecto integral de tecnología de información cuyo propósito sea sensibilizar y capacitar a los colaboradores en la materia de ciberseguridad y tratamiento de datos personales.

Segundo Dado que la dimensión conservación de la confidencialidad de la variable ciberseguridad tiene incidencia sobre la dimensión principio de consentimiento de la variable tratamiento de datos personales, se recomienda a la Gerencia municipal de la Municipalidad distrital de Lima Sur realizar un proyecto de transformación digital que busque integrar los procesos claves del negocio de verificación de identidades autorizadas que acceden a los sistemas de información con el propósito de asegurar la confidencialidad de la ciberseguridad relacionada con el principio de consentimiento en el tratamiento de datos personales.

Tercero Dado que la dimensión integridad de la variable ciberseguridad tiene incidencia sobre la dimensión principio de calidad de la variable tratamiento de datos personales, se recomienda a la Gerencia municipal de la Municipalidad distrital de Lima Sur realizar un proyecto de implementación en tecnología blockchain orientado a garantizar la conservación de la exactitud de la información vertida en los sistemas de información con el propósito de asegurar la integridad de la ciberseguridad relacionada con el principio de calidad en el tratamiento de datos personales.

Cuarto Dado que la dimensión disponibilidad de la variable ciberseguridad tiene incidencia sobre la dimensión principio de seguridad de la variable tratamiento de datos personales, se recomienda a la Gerencia municipal de la Municipalidad distrital de Lima Sur realizar consultorías

en materia de ethical hacking orientadas a detectar vulnerabilidades y amenazas en el acceso idóneo y seguro a los sistemas de información con el propósito de asegurar la disponibilidad de la ciberseguridad relacionada con el principio de seguridad en el tratamiento de datos personales.

REFERENCIAS

Arkhipov, V., y Naumov, V. (2016). *The legal definition of personal data in the regulatory environment of the Russian Federation: Between formal certainty and technological development*. Computer Law & Security Review, 32(6), 868–887. https://doi.org/10.1016/j.clsr.2016.07.009

Banco Interamericano de Desarrollo. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe* [Archivo PDF, Banco Interamericano de Desarrollo]. https://bit.ly/2YbGicX

Benussi, C. (2020). *Obligaciones de seguridad en el tratamiento de datos personales en Chile: escenario actual y desafíos regulatorios pendientes*. Revista Chilena de Derecho y Tecnología, 9(1), 227-279. https://doi.org/10.5354/0719-2584.2020.56660

Beven, K. (2006). *A manifesto for the equifinality thesis*. Journal of Hydrology. https://doi.org/10.1016/j.jhydrol.2005.07.007

Blanco, J. (2019). *The fractal geometry of Luhmann's sociological theory or debugging systems theory*. Technological Forecasting and Social Change, 146, 31–40. https://doi.org/10.1016/j.techfore.2019.05.020

Bohorquez, A. (2021). *Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020* [Tesis de Maestría, Universidad César Vallejo]. https://hdl.handle.net/20.500.12692/63128

Botta, M., Cavagnino, D., y Esposito, R. (2021). *NeuNAC: A novel fragile watermarking algorithm for integrity protection of neural networks*. Information Sciences, 576, 228–241. https://doi.org/10.1016/j.ins.2021.06.073

Cerda, A. (2006). *Mecanismos de Control en la Protección de Datos en Europa*. Ius et Praxis, 12(2), 221-251. https://dx.doi.org/10.4067/S0718-00122006000200009

Choejey, P., Murray, D. & Che, Ch. (2017). *Perceptions of Cybersecurity in Government Organizations: Case Study of Bhutan*. International Journal of Computer and Information Engineering Vol:11, No:1, 2017 https://doi.org/10.5281/zenodo.1131810

Chua, H. N., Herbland, A., Wong, S. F., y Chang, Y. (2017). *Compliance to personal data protection principles: A study of how organizations frame privacy policy notices*. Telematics and Informatics, 34(4), 157–170. https://doi.org/10.1016/j.tele.2017.01.008

Corallo, A., Lazoi, M., y Lezzi, M. (2020). *Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts*. Computers in Industry, 114, 103165. https://doi.org/10.1016/j.compind.2019.103165

Cova, B., Ivens, B. S., y Spencer, R. (2020). *The ins and outs of market shaping: Exclusion as a darkside?* Journal of Business Research. https://doi.org/10.1016/j.jbusres.2020.10.014

Craigen, D., Diakun-Thibault, N., y Purse, R. (2014). *Defining cybersecurity*. Technology Innovation Management Review, 4(10), 13–21. https://doi.org/10.22215/timreview835

Drack, M., & Pouvreau, D. (2015). *On the history of Ludwig von Bertalanffy's "General Systemology", and on its relationship to cybernetics – part III: convergences and divergences*. International Journal of General Systems, 44(5), 523–571. https://sci-hub.se/10.1080/03081079.2014.1000642

Ferdinand, J. (2015). *Building organisational cyber resilience: a strategic knowledge-based view of cyber security management*. J. Bus. Cont. Emerg. Plan. 9 (2), 185–195. PMID: 26642176

Fosch-Villaronga, E., y Mahler, T. (2021). *Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots*. Computer Law & Security Review, 41, 105528. https://sci-hub.se/https://doi.org/10.1016/j.clsr.2021.105528

Giménez-Aguilar, M., de Fuentes, J. M., Gonzalez-Manzano, L., y Arroyo, D. (2021). *Achieving cybersecurity in blockchain-based systems: A survey*. Future Generation Computer Systems, 124, 91–118. https://doi.org/10.1016/j.future.2021.05.007

Gómez, I. y Montoya, N. (2018). *Propuesta de implementación y cumplimiento de la LGPDPPSO a través de la plataforma de Protección de Datos Personales en Posesión de INFOTEC* [Tesis de Maestría, INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación]. http://infotec.repositorioinstitucional.mx/jspui/handle/1027/273

Grassi, P., García, M. y Fenton, J. (2017*). Digital Identity Guidelines*. NIST Special Publication 800-63-3. https://doi.org/10.6028/NIST.SP.800-63-3

Hernández, A., Indacochea, B., Moreno, L., Placencia, B., Quimis, A., y Ramos, M. (2018). *Metodología de la Investigación Científica*. Ed. Área de Innovación y Desarrollo, S.L. ISBN 978-8-494-82570-5

Hernández, R. y Mendoza, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta*. Ed. Mc Graw Hill Education. ISBN: 978-1-4562-6096-5

Hubbard, D. W., y Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk*. https://sci-hub.se/10.1002/9781119162315

ISO. (2012). *ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

IZAI Zacatecas. (29 de enero de 2021). *Ciberseguridad y Protección de Datos Personales* [Archivo de Vídeo]. YouTube. https://www.youtube.com/watch?v=4zYK9-kP2sY

Javid, T., Faris, M., Beenish, H. y Fahad, M. (2020). *Cybersecurity and Data Privacy in the Cloudlet for Preliminary Healthcare Big Data Analytics*. 2020 International Conference on Computing and Information Technology,

Universidad de Tabuk. https://doi.org/10.1109/ICCIT-144147971.2020.9213712

Kilovaty, I. (2020). Availability's Law. Tennessee Law Review, Vol. 88, 2020. SSRN: https://ssrn.com/abstract=3568790

Kish, K., Mallery, D., Yahya Haage, G., Melgar-Melgar, R., Burke, M., Orr, C., … Larson, J. (2021). *Fostering critical pluralism with systems theory, methods, and heuristics*. Ecological Economics, 189, 107171. https://sci-hub.se/https://doi.org/10.1016/j.ecolecon.2021.107171

Koletsi, D., & Pandis, N. (2018). *Ordinal logistic regression.* American Journal of Orthodontics and Dentofacial Orthopedics, 153(1), 157–158. https://sci-hub.se/https://doi.org/10.1016/j.ajodo.2017.11.011

Koops, B. (2014). *The Trouble with European Data Protection Law*. International Data Privacy Law 250-61. https://bit.ly/3v25iiP

Leal, F., Chis, A. E., Caton, S., González–Vélez, H., García–Gómez, J. M., Durá, M., … Mier, M. (2021). *Smart Pharmaceutical Manufacturing: Ensuring End-to-End Traceability and Data Integrity in Medicine Production*. Big Data Research, 24, 100172. https://doi.org/10.1016/j.bdr.2020.100172

Lee, I. (2021). C*ybersecurity: Risk management framework and investment cost analysis*. Business Horizons, 64(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Leydesdorff, L., & Ivanova, I. A. (2013). *Mutual redundancies in interhuman communication systems: Steps toward a calculus of processing meaning*. Journal of the Association for Information Science and Technology, 65(2), 386–399. https://sci-hub.se/https://doi.org/10.1002/asi.22973

Liu, Y. (2014). *User control of personal information concerning mobile-app: Notice and consent?* Computer Law & Security Review, 30(5), 521–529. https://doi.org/10.1016/j.clsr.2014.07.008

López, O. (2021). *Análisis de la ley de protección de los datos personales para establecer los criterios de penalidad de sanción del trabajo social comunitario* [Tesis de Grado, Universidad Señor de Sipán]. https://hdl.handle.net/20.500.12802/8267

Luh, F. y Yen, Y. (2020). *Cybersecurity in Science and Medicine: Threats and Challenges.* Trends in Biotechnology. https://doi.org/10.1016/j.tibtech.2020.02.010

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*. Computer Law & Security Review, 105336. https://doi:10.1016/j.clsr.2019.06.007

Maestre, J. (2018). *Anomaly Recognition for Intrusion Detection on Emergent Monitoring Environments*. ResearchGate. DOI:10.13140/RG.2.2.16984.75529

Maxey, D. (2020). *The challenge of privacy and consent enforcement in large-scale enterprise application programmes*. Computer Fraud & Security, 2020(9), 6–9. https://doi.org/10.1016/S1361-3723(20)30095-6

Mohammadpourfard, M., Weng, Y., Pechenizkiy, M., Tajdinian, M., y Mohammadi-Ivatloo, B. (2020). *Ensuring cybersecurity of smart grid against data integrity attacks under concept drift*. International Journal of Electrical Power & Energy Systems, 119, 105947. https://doi.org/10.1016/j.ijepes.2020.105947

Najmi, Y., AlZain, A., Masud, M., Jhanjhi, Z., Al-Amri, J., y Baz, M. (2021). *A survey on security threats and countermeasures in IoT to achieve users' confidentiality and reliability*. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.03.417

Ñaupas, H., Valdivia, M., Palacios, J. y Romero, H. (2018). *Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis*. Ed. Ediciones de la U. ISBN 978-958-762-876-0.

Olivos, M. (2020). *El Derecho a la Protección de Datos Personales en el Perú: 27 años desde su incorporación en la Constitución Política de 1993*. Revista de Investigación de la Facultad de Derecho. Universidad del Pacífico. https://doi.org/10.35383/ius-usat.v9i1.338

Pal, A., Jolfaei, A., y Kant, K. (2021). *A Fast Prekeying-Based Integrity Protection for Smart Grid Communications*. IEEE Transactions on Industrial Informatics, 17(8), 5751–5758. https://sci-hub.se/10.1109/TII.2020.3030799

Pauletto, C. (2020). *Options towards a global standard for the protection of individuals with regard to the processing of personal data*. Computer Law & Security Review, 105433. https://doi.org/10.1016/j.clsr.2020.105433

Pawlicka, A., Choraś, M., Pawlicki, M., y Kozik, R. (2021). *A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic*. Business Horizons. https://doi.org/10.1016/j.bushor.2021.07.010

Paz, O. (5 de octubre de 2020). *Miraflores podría ser multada hasta con S/250 mil por revelar datos de denunciante*. *El Comercio.* https://bit.ly/2Y6YDr2

Pérez, W. y Ramos, M. (2020). *Propuesta de una Política de Ciberseguridad para las Fuerzas Armadas* [Tesis de Maestría, Universidad de las Fuerzas Armadas de Ecuador]. http://repositorio.espe.edu.ec/handle/21000/23372

Polo, A. (2020). *El impacto de la Ley de Protección de Datos Personales en el contrato de hosting* [Tesis de Maestría, Universidad de Lima]. https://hdl.handle.net/20.500.12724/11714

Presidencia del Concejo de Ministros. (2017). *Decreto Legislativo N.º 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la Regulación de la Gestión de Intereses* [Archivo PDF, Diario Oficial El Peruano]. https://cdn.www.gob.pe/uploads/document/file/251478/Decreto_Legislativo_N__1353.pdf

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). *Cybersecurity awareness for children: A systematic literature review*. International Journal of Child-Computer Interaction, 30, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., Sushil, y Dwivedi, Y. K. (2021). *Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management*. Technological Forecasting and Social Change, 170, 120872. https://doi.org/10.1016/j.techfore.2021.120872

Rashid, Z., Noor, U., y Altmann, J. (2021). *Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem*. Future Generation Computer Systems, 124, 436–466. https://doi.org/10.1016/j.future.2021.05.033

Rosen, R. (1969). *General System Theory. Foundations, Development, Applications. Ludwig von Bertalanffy. Braziller, New York, 1969. xvi + 290 pp., illus. Cloth, $8.95; paper, $3.95*. Science, 164(3880), 681–682. https://www.science.org/doi/10.1126/science.164.3880.681

Sagasti, F. y Mitroff, I. (1973). *Operations research from the viewpoint of general systems theory*. Ed. Omega. https://doi.org/10.1016/0305-0483(73)90087-X

Salinas, K. (2019). *La incompatibilidad existente en las obligaciones del derecho de información del titular de los datos personales* [Tesis de Grado, Pontificia Universidad Católica del Perú]. http://hdl.handle.net/20.500.12404/16333

Schirmer, W., & Michailakis, D. (2013). *The Luhmannian approach to exclusion/inclusion and its relevance to Social Work. Journal of Social Work*, 15(1), 45–64. https://doi.org/10.1177/1468017313504607

Seising, R. (2010). *Cybernetics, system(s) theory, information theory and Fuzzy Sets and Systems in the 1950s and 1960s*. Information Sciences, 180(23), 4459–4476. https://doi.org/10.1016/j.ins.2010.08.001

Stefaniuk, T. (2020). *Training in shaping employee information security awareness*. Entrepreneurship and Sustainability Issues 7(3): 1832-1846. https://doi.org/10.9770/jesi.2020.7.3(26)

Steinfeld, N. (2019). *Situational User Consent for Access to Personal Information: Does purpose make any difference?* Telematics and Informatics, 101341. https://doi.org/10.1016/j.tele.2019.101341

Stitilis, D., y Laurinaitis, M. (2017). *Treatment of biometrically processed personal data: Problem of uniform practice under EU personal data protection law*. Computer Law & Security Review, 33(5), 618–628. https://doi.org/10.1016/j.istr.2009.10.001

Taípe, D. (2020). *La auditoría de seguridad informática y su relación en la ciberseguridad en el sector público año 2018* [Tesis de Maestría, Universidad Nacional de Piura]. https://repositorio.unp.edu.pe/handle/20.500.12676/2361

Turk, Ž., García de Soto, B., Mantha, B., Maciel, A. y Georgescu, A. (2021). *A systemic framework for addressing cybersecurity in construction*. Automation in Construction. https://doi.org/10.1016/j.autcon.2021.103988

Vacca, J. (2017). *Computer and Information Security Handbook*. Network Security, 2017(11), 4. https://doi.org/10.1016/S1353-4858(17)30090-9

Vásquez, R. (2019). (7 de diciembre de 2019). *El principio de seguridad de la Ley de protección de datos personales, por Raúl Vásquez Rodríguez*. Recuperado de https://lpderecho.pe/principio-seguridad-ley-de-proteccion-datos-personales-raul-vasquez-rodriguez/

Villarrubia, G. (2021). *Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la política de seguridad y defensa nacional en la región Lima, 2018* [Tesis de Maestría, Centro de Altos Estudios Nacionales]. https://renati.sunedu.gob.pe/handle/sunedu/2262092

Wessels, M., van den Brink, P., Verburgh, T., Cadet, B., y van Ruijven, T. (2021). *Understanding incentives for cybersecurity investments: Development and*

application of a typology. Digital Business, 1(2), 100014. https://doi.org/10.1016/j.digbus.2021.100014

Yang, C., Zhao, F., Tao, X., y Wang, Y. (2021). *Publicly verifiable outsourced data migration scheme supporting efficient integrity checking*. Journal of Network and Computer Applications, 192, 103184. https://doi.org/10.1016/j.jnca.2021.103184

Zheng, G. (2021). *Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China*, Computer Law & Security Review, Volume 43. https://doi.org/10.1016/j.clsr.2021.105610.

Zúñiga, J. (2017). *Ciberdefensa y su incidencia en la protección de la Información del Ejército del Perú. caso: COPERE 2013 - 2014* [Tesis de Maestría, Instituto Científico Tecnológico del Ejército]. http://repositorio.icte.ejercito.mil.pe/handle/123456789/183

ANEXOS

Anexo 1: Matriz de Consistencia

TÍTULO: Ciberseguridad y su incidencia en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021

AUTOR: Miguel Martín Correa Coronel

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
Problema general: ¿De qué manera la ciberseguridad incide en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021?	**Objetivo general:** Determinar la incidencia de la ciberseguridad en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.	**Hipótesis general:** La ciberseguridad incide significativamente en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.	**Variable - 1: Ciberseguridad**			
			Dimensiones	**Indicadores**	**Ítems**	**Niveles**
Problemas específicos: PE1: ¿De qué manera la dimensión conservación de la confidencialidad de la ciberseguridad incide en la dimensión principio de consentimiento del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021? PE2: ¿De qué manera la dimensión integridad de	**Objetivos específicos:** OE1: Determinar la incidencia de la dimensión conservación de la confidencialidad de la ciberseguridad en la dimensión principio de consentimiento del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.	**Hipótesis específicas:** HE1: La dimensión conservación de la confidencialidad de la ciberseguridad incide significativamente en la dimensión principio de consentimiento del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.	**Conservación de la confidencialidad**	Autorización	1-2	Optimo Medio No optimo
				Almacenamiento	3-4	
				Tránsito	5-6	
			Integridad	Precisión	7-8	
				Completitud	9-10	
				Conformidad	11-12	
			Disponibilidad	Acceso	13-14	
				Creación	15-16	
				Actualización	17-18	

TÍTULO: Ciberseguridad y su incidencia en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021

AUTOR: Miguel Martín Correa Coronel

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES
la ciberseguridad incide en la dimensión principio de calidad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021? PE3: ¿De qué manera la dimensión disponibilidad de la ciberseguridad incide en la dimensión principio de seguridad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021?	OE2: Determinar la incidencia de la dimensión integridad de la ciberseguridad en la dimensión principio de calidad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021. OE3: Determinar la incidencia de la dimensión disponibilidad de la ciberseguridad en la dimensión del principio de seguridad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.	HE2: La dimensión integridad de la ciberseguridad incide significativamente en la dimensión principio de calidad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021. HE3: La dimensión disponibilidad de la ciberseguridad incide significativamente en la dimensión principio de seguridad del tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021.	**Variable - 2: Tratamiento de Datos Personales**

Dimensiones	Indicadores	Ítems	Niveles
Principio de consentimiento	Autorización	19-20	Optimo Medio No optimo
	Recopilación	21-22	
	Tratamiento	23-24	
Principio de calidad	Precisión	25-26	
	Veracidad	27-28	
	Finalidad	29-30	
Principio de seguridad	Fidelidad	25-26	
	Conservación	27-28	
	Rectitud	29-30	

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Aplicada **Diseño:** No experimental Transversal Correlacional-causal	**Población:** 1046 colaboradores de la Municipalidad distrital de Lima Sur. **Tamaño de muestra:** 282 colaboradores de la Municipalidad distrital de Lima Sur. **Muestreo:** Muestreo probabilístico simple.	**Técnicas:** Encuesta **Instrumentos:** Cuestionario	**Descriptiva:** Se utilizará para describir e interpretar los datos recolectados en forma ordenada mediante histogramas y tablas de información numérica. **Inferencial:** Se utilizará en métodos paramétricos con coeficientes de regresión logística para determinar el grado de causalidad o correlación entre la variable independiente y la variable dependiente.

Anexo 2: Matriz de Operacionalización de Variables

TÍTULO: Ciberseguridad y su incidencia en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021

AUTOR: Miguel Martín Correa Coronel

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Variable – 1: Ciberseguridad ISO (2012), indica que se fundamenta en la conservación de la confidencialidad, integridad y disponibilidad de la información alojada en ordenadores y redes digitales de gran escala y de transmisión a nivel mundial, denominado ciberespacio.	**Conservación de la confidencialidad** Grassi, García y Fenton (2017), como se citó en Giménez-Aguilar et al (2021), señalan que consiste en la no divulgación de información hacia terceros no autorizados.	Autorización	1	¿El personal de la institución debe contar con la autorización necesaria para acceder a los datos personales de los colaboradores?	Óptimo Medio No óptimo
			2	¿Está de acuerdo con que sólo personal autorizado acceda a sus datos personales?	
		Almacenamiento	3	¿Cuál es la unidad de la institución responsable del almacenamiento de sus datos personales?	
			4	¿Sabe dónde se almacenan sus datos personales en la institución?	
		Tránsito	5	¿Qué tan seguro es el tránsito virtual de sus datos personales en la institución?	
			6	¿Qué tan frecuente es el tránsito virtual de sus datos personales en la institución?	
	Integridad Mohammadpourfard et al (2020) y Pal et al (2021) la definen como la protección y mantenimiento de la información sin alteración obtenida a través de la comunicación que fluye en el ciberespacio.	Precisión	7	¿Qué tan precisos son los datos personales que brindó a la institución?	
			8	¿Cree que los datos personales que brindó a la institución permanecerán precisos en el tiempo?	
		Completitud	9	¿Qué tan completos son los datos personales que brindó a la institución?	
			10	¿Qué tan completos están los datos personales en la base de datos de la institución?	
		Conformidad	11	¿Los colaboradores dan su conformidad sobre sus datos personales en la institución?	

TÍTULO: Ciberseguridad y su incidencia en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021

AUTOR: Miguel Martín Correa Coronel

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
			12	¿Es importante que la institución cuente con la conformidad de sus colaboradores respecto de sus datos personales?	
	Disponibilidad Najmi et al (2021) indica que se fundamenta en el acceso pleno, necesario y debidamente autorizado a las aplicaciones, recursos y servicios alojados en el ciberespacio.	Acceso	13	¿Los colaboradores pueden acceder a sus datos personales otorgados a la institución?	
			14	¿Es importante que los colaboradores puedan acceder a sus datos personales alojados en la institución?	
		Creación	15	¿Los colaboradores pueden agregar nuevos datos personales a la institución?	
			16	¿Es importante que los colaboradores puedan agregar nuevos datos personales en la institución?	
		Actualización	17	¿Qué tan factible es que los colaboradores puedan actualizar sus datos personales en la institución?	
			18	¿Qué tan rápido es el proceso de actualización de datos personales en la institución?	
Variable - 2: Tratamiento de datos personales Para la Unión Europea (UE, 2018), tal como lo indicó	**Principio de consentimiento** Steinfeld (2019) y Maxey (2020) que indican que consiste en dar el permiso necesario a una entidad con la finalidad de que pueda usar, tratar	Autorización	19	¿Con qué frecuencia la institución solicita la autorización de los colaboradores para tratar sus datos personales?	
			20	¿Es importante que la institución solicite la autorización de sus colaboradores para tratar sus datos personales?	

TÍTULO: Ciberseguridad y su incidencia en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021

AUTOR: Miguel Martín Correa Coronel

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Pauletto (2020), es cualquier tipo de procesamiento, automatizado o no, que tenga como finalidad alterar datos personales.	o distribuir los datos personales asignados en sus bancos de datos.	Recopilación	21	¿Considera eficiente el proceso de recopilación de datos personales que realiza la institución?	Bueno Regular Malo
			22	¿Son seguros los medios de recopilación de datos personales de la institución?	
		Tratamiento	23	¿El tratamiento de datos personales que hace la institución cumple con lo que exige la ley?	
			24	¿Considera eficiente el proceso de tratamiento de datos personales que realiza la institución?	
	Principio de calidad Para Chua et al (2017) y Yang et al (2021) consiste en el despliegue de acciones por parte de la entidad que resguarda los datos personales para que estos gocen de precisión, completitud, veracidad y actualización en función del propósito para el cual fueron recabados.	Precisión	25	¿El proceso de tratamiento de datos personales en la institución se realiza con datos precisos?	
			26	¿Es importante que la institución cuente con datos personales precisos de sus colaboradores?	
		Veracidad	27	¿El proceso de tratamiento de datos personales en la institución se realiza con datos veraces?	
			28	¿Es importante que la institución cuente con datos personales veraces de sus colaboradores?	
		Finalidad	29	¿La institución le ha explicado cuál es la finalidad del tratamiento de sus datos personales?	
			30	¿La finalidad del tratamiento de los datos personales está claramente definida en la institución?	
	Principio de seguridad	Fidelidad	31	¿Cree que se cumple con la fidelidad ética del tratamiento de datos personales en la institución?	

TÍTULO: Ciberseguridad y su incidencia en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021

AUTOR: Miguel Martín Correa Coronel

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Polo (2020) y Vásquez (2019), amparados en el artículo 9° de la Ley N.º 29733 y el artículo 10º del Reglamento de la misma ley, la definen como el conjunto de procedimientos y normas que buscan garantizar que los datos personales sean protegidos contra el hurto, la adulteración y el tratamiento o procesamiento por terceros no autorizados.		32	¿Es importante mantener un ambiente institucional de fidelidad ética en el tratamiento de datos personales?	
		Conservación	33	¿Considera eficiente el proceso de conservación de datos personales que realiza la institución?	
			34	¿Son seguros los medios de conservación de datos personales de la institución?	
		Rectitud	35	¿Cree que se cumple con la rectitud legal del tratamiento de datos personales en la institución?	
			36	¿Es importante mantener un ambiente institucional de rectitud legal en el tratamiento de datos personales?	

Anexo 3: Instrumento de Recolección de Datos

Cuestionario para los colaboradores de la Municipalidad distrital de Lima Sur, 2021.

Edad: [ ] años **Sexo:** Femenino [ ] Masculino [ ]

Instrucciones: Marque con un aspa la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo al siguiente **ejemplo**: 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	¿El personal de la institución debe contar con la autorización necesaria para acceder a los datos personales de los colaboradores?	Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo
2	¿Está de acuerdo con que sólo personal autorizado acceda a sus datos personales?	Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo
3	¿Cuál es la unidad de la institución responsable del almacenamiento de sus datos personales?	No conozco en lo absoluto	Conozco vagamente	Indeciso	Conozco lo suficiente	Conozco totalmente
4	¿Sabe dónde se almacenan sus datos personales en la institución?	No conozco en lo absoluto	Conozco vagamente	Indeciso	Conozco lo suficiente	Conozco totalmente
5	¿Qué tan seguro es el tránsito virtual de sus datos personales en la institución?	Muy poco seguro	Poco seguro	Indeciso	Mayoritariamente seguro	Totalmente seguro
6	¿Qué tan frecuente es el tránsito virtual de sus datos personales en la institución?	Muy poco frecuentemente	Poco frecuentemente	Indeciso	Frecuente	Muy frecuente
7	¿Qué tan precisos son los datos personales que brindó a la institución?	Nada precisos	Poco precisos	Indeciso	Bastante precisos	Totalmente precisos
8	¿Cree que los datos personales que brindó a la institución permanecerán precisos en el tiempo?	Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo
9	¿Qué tan completos son los datos personales que brindó a la institución?	Nada completos	Poco completos	Indeciso	Mayoritariamente completos	Totalmente completos
10	¿Qué tan completos están los datos personales en la base de datos de la institución?	Nada completos	Poco completos	Indeciso	Mayoritariamente completos	Totalmente completos
11	¿Los colaboradores dan su conformidad sobre sus datos personales en la institución?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
12	¿Es importante que la institución cuente con la conformidad de sus colaboradores respecto de sus datos personales?	Sin importancia	De poca importancia	Indeciso	Importante	Muy importante
13	¿Los colaboradores pueden acceder a sus datos personales otorgados a la institución?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
14	¿Es importante que los colaboradores puedan acceder a sus datos personales alojados en la institución?	Sin importancia	De poca importancia	Indeciso	Importante	Muy importante

No	Pregunta	Valoración				
		1	2	3	4	5
15	¿Los colaboradores pueden agregar nuevos datos personales a la institución?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
16	¿Es importante que los colaboradores puedan agregar nuevos datos personales en la institución?	Sin importancia	De poca importancia	Indeciso	Importante	Muy importante
17	¿Qué tan factible es que los colaboradores puedan actualizar sus datos personales en la institución?	Nada factible	Poco factible	Indeciso	Factible	Muy factible
18	¿Qué tan rápido es el proceso de actualización de datos personales en la institución?	Nada rápido	Poco rápido	Indeciso	Rápido	Muy rápido
	Sobre tratamiento de datos personales					
19	¿Con qué frecuencia la institución solicita la autorización de los colaboradores para tratar sus datos personales?	Nunca	Raramente	Indeciso	Frecuentemente	Muy frecuentemente
20	¿Es importante que la institución solicite la autorización de sus colaboradores para tratar sus datos personales?	Sin importancia	De poca importancia	Indeciso	Importante	Muy importante
21	¿Considera eficiente el proceso de recopilación de datos personales que realiza la institución?	Nada eficiente	Poco eficiente	Neutral	Eficiente	Totalmente eficiente
22	¿Son seguros los medios de recopilación de datos personales de la institución?	Nada seguros	Poco seguros	Neutral	Seguros	Totalmente seguros
23	¿El tratamiento de datos personales que hace la institución cumple con lo que exige la ley?	No cumple	Cumple poco	Neutral	Cumple mayoritariamente	Cumple totalmente
24	¿Considera eficiente el proceso de tratamiento de datos personales que realiza la institución?	Nada eficiente	Poco eficiente	Neutral	Eficiente	Totalmente eficiente
25	¿El proceso de tratamiento de datos personales en la institución se realiza con datos precisos?	Nada precisos	Poco precisos	Neutral	Precisos	Totalmente precisos
26	¿Es importante que la institución cuente con datos personales precisos de sus colaboradores?	Sin importancia	De poca importancia	Neutral	Importante	Muy importante
27	¿El proceso de tratamiento de datos personales en la institución se realiza con datos veraces?	Nada veraces	Poco veraces	Neutral	Muy veraces	Totalmente veraces
28	¿Es importante que la institución cuente con datos personales veraces de sus colaboradores?	Sin importancia	De poca importancia	Neutral	Importante	Muy importante
29	¿La institución le ha explicado cuál es la finalidad del tratamiento de sus datos personales?	Nunca	Raramente	Neutral	Frecuentemente	Muy frecuentemente
30	¿La finalidad del tratamiento de los datos personales está claramente definida en la institución?	Nada definida	Poco definida	Neutral	Muy definida	Totalmente definida
31	¿Cree que se cumple con la fidelidad ética del tratamiento de datos personales en la institución?	Nunca	Raramente	Neutral	Frecuentemente	Muy frecuentemente

No	Pregunta	Valoración				
		1	2	3	4	5
32	¿Es importante mantener un ambiente institucional de fidelidad ética en el tratamiento de datos personales?	Sin importancia	De poca importancia	Neutral	Importante	Muy importante
33	¿Considera eficiente el proceso de conservación de datos personales que realiza la institución?	Nada eficiente	Poco eficiente	Neutral	Muy eficiente	Totalmente eficiente
34	¿Son seguros los medios de conservación de datos personales de la institución?	Nada seguros	Poco seguros	Neutral	Muy seguros	Totalmente seguros
35	¿Cree que se cumple con la rectitud legal del tratamiento de datos personales en la institución?	Nunca	Raramente	Neutral	Frecuentemente	Muy frecuentemente
36	¿Es importante mantener un ambiente institucional de rectitud legal en el tratamiento de datos personales?	Sin importancia	De poca importancia	Neutral	Importante	Muy importante

¡Gracias por su tiempo!

Anexo 4: Certificado de validación del instrumento de recolección de datos

Validación del experto N°1

VARIABLE: Ciberseguridad

N.º	DIMENSIONES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	CONSERVACION DE LA CONFIDENCIALIDAD	SI	NO	SI	NO	SI	NO	
1	¿El personal de la institución debe contar con la autorización necesaria para acceder a los datos personales de los colaboradores?	x		x		x		-
2	¿Está de acuerdo con que sólo personal autorizado acceda a sus datos personales?	x		x		x		-
3	¿Cuál es la unidad de la institución responsable del almacenamiento de sus datos personales?	x		x		x		-
4	¿Sabe dónde se almacenan sus datos personales en la institución?	x		x		x		-
5	¿Qué tan seguro es el tránsito virtual de sus datos personales en la institución?	x		x		x		-
6	¿Qué tan frecuente es el tránsito virtual de sus datos personales en la institución?	x		x		x		-
	INTEGRIDAD	SI	NO	SI	NO	SI	NO	
7	¿Qué tan precisos son los datos personales que brindó a la institución?	x		x		x		-
8	¿Cree que los datos personales que brindó a la institución permanecerán precisos en el tiempo?	x		x		x		-
9	¿Qué tan completos son los datos personales que brindó a la institución?	x		x		x		-
10	¿Qué tan completos están los datos personales de en la base de datos de la institución?	x		x		x		-
11	¿Los colaboradores dan su conformidad sobre sus datos personales en la institución?	x		x		x		-
12	¿Es importante que la institución cuente con la conformidad de sus colaboradores respecto de sus datos personales?	x		x		x		-
	DISPONIBILIDAD	SI	NO	SI	NO	SI	NO	
13	¿Los colaboradores pueden acceder a sus datos personales otorgados a la institución?	x		x		x		-
14	¿Es importante que los colaboradores puedan acceder a sus datos personales alojados en la institución?	x		x		x		-
15	¿Los colaboradores pueden agregar nuevos datos personales a la institución?	x		x		x		-
16	¿Es importante que los colaboradores puedan agregar nuevos datos personales en la institución?	x		x		x		-
17	¿Qué tan factible es que los colaboradores puedan actualizar sus datos personales en la institución?	x		x		x		-
18	¿Qué tan rápido es el proceso de actualización de datos personales en la institución?	x		x		x		-

VARIABLE: Tratamiento de Datos Personales

N.°	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PRINCIPIO DE CONSENTIMIENTO	SI	NO	SI	NO	SI	NO	
19	¿Con qué frecuencia la Institución solicita la autorización de los colaboradores para tratar sus datos personales?	x		x		x		-
20	¿Es importante que la Institución solicite la autorización de sus colaboradores para tratar sus datos personales?	x		x		x		-
21	¿Considera eficiente el proceso de recopilación de datos personales que realiza la Institución?	x		x		x		-
22	¿Son seguros los medios de recopilación de datos personales de la Institución?	x		x		x		-
23	¿El tratamiento de datos personales que hace la Institución cumple con lo que exige la ley?	x		x		x		-
24	¿Considera eficiente el proceso de tratamiento de datos personales que realiza la Institución?	x		x		x		-
	PRINCIPIO DE CALIDAD	SI	NO	SI	NO	SI	NO	
25	¿El proceso de tratamiento de datos personales en la Institución se realiza con datos precisos?	x		x		x		-
26	¿Es importante que la Institución cuente con datos personales precisos de sus colaboradores?	x		x		x		-
27	¿El proceso de tratamiento de datos personales en la Institución se realiza con datos veraces?	x		x		x		-
28	¿Es importante que la Institución cuente con datos personales veraces de sus colaboradores?	x		x		x		-
29	¿La Institución le ha explicado cuál es la finalidad del tratamiento de sus datos personales?	x		x		x		-
30	¿La finalidad del tratamiento de los datos personales está claramente definida en la Institución?	x		x		x		-
	PRINCIPIO DE SEGURIDAD	SI	NO	SI	NO	SI	NO	
31	¿Cree que se cumple con la fidelidad ética del tratamiento de datos personales en la Institución?	x		x		x		-
32	¿Es importante mantener un ambiente institucional de fidelidad ética en el tratamiento de datos personales?	x		x		x		-
33	¿Considera eficiente el proceso de conservación de datos personales que realiza la Institución?	x		x		x		-
34	¿Son seguros los medios de conservación de datos personales de la Institución?	x		x		x		-
35	¿Cree que se cumple con la rectitud legal del tratamiento de datos personales en la Institución?	x		x		x		-
36	¿Es importante mantener un ambiente institucional de rectitud legal en el tratamiento de datos personales?	x		x		x		-

Observaciones (precisar si hay suficiencia): NINGUNA

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

Apellidos y nombres del juez evaluador: Melgar Allaga, Freud Enrique **DNI: 10583345**

Especialista: Metodólogo [ ] Temático [X]

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 el componente o dimensión específica del constructo
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Fecha: 04 de octubre de 2021

Firma del Experto Informante

Validación del experto N°2

VARIABLE: Ciberseguridad

N.º	DIMENSIONES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	CONSERVACIÓN DE LA CONFIDENCIALIDAD	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	-
1	¿El personal de la institución debe contar con la autorización necesaria para acceder a los datos personales de los colaboradores?	x		x		x		-
2	¿Está de acuerdo con que sólo personal autorizado acceda a sus datos personales?	x		x		x		-
3	¿Cuál es la unidad de la institución responsable del almacenamiento de sus datos personales?	x		x		x		-
4	¿Sabe dónde se almacenan sus datos personales en la institución?	x		x		x		-
5	¿Qué tan seguro es el tránsito virtual de sus datos personales en la institución?	x		x		x		-
6	¿Qué tan frecuente es el tránsito virtual de sus datos personales en la institución?	x		x		x		-
	INTEGRIDAD	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	
7	¿Qué tan precisos son los datos personales que brindó a la institución?	x		x		x		-
8	¿Cree que los datos personales que brindó a la institución permanecerán precisos en el tiempo?	x		x		x		-
9	¿Qué tan completos son los datos personales que brindó a la institución?	x		x		x		-
10	¿Qué tan completos están los datos personales de en la base de datos de la institución?	x		x		x		-
11	¿Los colaboradores dan su conformidad sobre sus datos personales en la institución?	x		x		x		-
12	¿Es importante que la institución cuente con la conformidad de sus colaboradores respecto de sus datos personales?	x		x		x		-
	DISPONIBILIDAD	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	
13	¿Los colaboradores pueden acceder a sus datos personales otorgados a la institución?	x		x		x		-
14	¿Es importante que los colaboradores puedan acceder a sus datos personales alojados en la institución?	x		x		x		-
15	¿Los colaboradores pueden agregar nuevos datos personales a la institución?	x		x		x		-
16	¿Es importante que los colaboradores puedan agregar nuevos datos personales en la institución?	x		x		x		-
17	¿Qué tan factible es que los colaboradores puedan actualizar sus datos personales en la institución?	x		x		x		-
18	¿Qué tan rápido es el proceso de actualización de datos personales en la institución?	x		x		x		-

VARIABLE: Tratamiento de Datos Personales

N.º	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PRINCIPIO DE CONSENTIMIENTO	SI	NO	SI	NO	SI	NO	
19	¿Con qué frecuencia la institución solicita la autorización de los colaboradores para tratar sus datos personales?	x		x		x		-
20	¿Es importante que la institución solicite la autorización de sus colaboradores para tratar sus datos personales?	x		x		x		-
21	¿Considera eficiente el proceso de recopilación de datos personales que realiza la institución?	x		x		x		-
22	¿Son seguros los medios de recopilación de datos personales de la institución?	x		x		x		-
23	¿El tratamiento de datos personales que hace la institución cumple con lo que exige la ley?	x		x		x		-
24	¿Considera eficiente el proceso de tratamiento de datos personales que realiza la institución?	x		x		x		-
	PRINCIPIO DE CALIDAD	SI	NO	SI	NO	SI	NO	
25	¿El proceso de tratamiento de datos personales en la institución se realiza con datos precisos?	x		x		x		-
26	¿Es importante que la institución cuente con datos personales precisos de sus colaboradores?	x		x		x		-
27	¿El proceso de tratamiento de datos personales en la institución se realiza con datos veraces?	x		x		x		-
28	¿Es importante que la institución cuente con datos personales veraces de sus colaboradores?	x		x		x		-
29	¿La institución le ha explicado cuál es la finalidad del tratamiento de sus datos personales?	x		x		x		-
30	¿La finalidad del tratamiento de los datos personales está claramente definida en la institución?	x		x		x		-
	PRINCIPIO DE SEGURIDAD	SI	NO	SI	NO	SI	NO	
31	¿Cree que se cumple con la fidelidad ética del tratamiento de datos personales en la institución?	x		x		x		-
32	¿Es importante mantener un ambiente institucional de fidelidad ética en el tratamiento de datos personales?	x		x		x		-
33	¿Considera eficiente el proceso de conservación de datos personales que realiza la institución?	x		x		x		-
34	¿Son seguros los medios de conservación de datos personales de la institución?	x		x		x		-
35	¿Cree que se cumple con la rectitud legal del tratamiento de datos personales en la institución?	x		x		x		-
36	¿Es importante mantener un ambiente institucional de rectitud legal en el tratamiento de datos personales?	x		x		x		-

Observaciones (precisar si hay suficiencia): NINGUNA

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

Apellidos y nombres del juez evaluador: Quispe Laguna, Waldir Enrique **DNI:** 09449377

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

Fecha: 03 de octubre de 2021

Firma del Experto Informante

Validación del experto N°3

VARIABLE: Ciberseguridad

N.º	DIMENSIONES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	CONSERVACIÓN DE LA CONFIDENCIALIDAD	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	-
1	¿El personal de la institución debe contar con la autorización necesaria para acceder a los datos personales de los colaboradores?	x		x		x		-
2	¿Está de acuerdo con que sólo personal autorizado acceda a sus datos personales?	x		x		x		-
3	¿Cuál es la unidad de la institución responsable del almacenamiento de sus datos personales?	x		x		x		-
4	¿Sabe dónde se almacenan sus datos personales en la institución?	x		x		x		-
5	¿Qué tan seguro es el tránsito virtual de sus datos personales en la institución?	x		x		x		-
6	¿Qué tan frecuente es el tránsito virtual de sus datos personales en la institución?	x		x		x		-
	INTEGRIDAD	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	
7	¿Qué tan precisos son los datos personales que brindó a la institución?	x		x		x		-
8	¿Cree que los datos personales que brindó a la institución permanecerán precisos en el tiempo?	x		x		x		-
9	¿Qué tan completos son los datos personales que brindó a la institución?	x		x		x		-
10	¿Qué tan completos están los datos personales de en la base de datos de la institución?	x		x		x		-
11	¿Los colaboradores dan su conformidad sobre sus datos personales en la institución?	x		x		x		-
12	¿Es importante que la institución cuente con la conformidad de sus colaboradores respecto de sus datos personales?	x		x		x		-
	DISPONIBILIDAD	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	
13	¿Los colaboradores pueden acceder a sus datos personales otorgados a la institución?	x		x		x		-
14	¿Es importante que los colaboradores puedan acceder a sus datos personales alojados en la institución?	x		x		x		-
15	¿Los colaboradores pueden agregar nuevos datos personales a la institución?	x		x		x		-
16	¿Es importante que los colaboradores puedan agregar nuevos datos personales en la institución?	x		x		x		-
17	¿Qué tan factible es que los colaboradores puedan actualizar sus datos personales en la institución?	x		x		x		-
18	¿Qué tan rápido es el proceso de actualización de datos personales en la institución?	x		x		x		-

VARIABLE: Tratamiento de Datos Personales

N.º	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PRINCIPIO DE CONSENTIMIENTO	SI	NO	SI	NO	SI	NO	
19	¿Con qué frecuencia la institución solicita la autorización de los colaboradores para tratar sus datos personales?	x		x		x		-
20	¿Es importante que la institución solicite la autorización de sus colaboradores para tratar sus datos personales?	x		x		x		-
21	¿Considera eficiente el proceso de recopilación de datos personales que realiza la institución?	x		x		x		-
22	¿Son seguros los medios de recopilación de datos personales de la institución?	x		x		x		-
23	¿El tratamiento de datos personales que hace la institución cumple con lo que exige la ley?	x		x		x		-
24	¿Considera eficiente el proceso de tratamiento de datos personales que realiza la institución?	x		x		x		-
	PRINCIPIO DE CALIDAD	SI	NO	SI	NO	SI	NO	
25	¿El proceso de tratamiento de datos personales en la institución se realiza con datos precisos?	x		x		x		-
26	¿Es importante que la institución cuente con datos personales precisos de sus colaboradores?	x		x		x		-
27	¿El proceso de tratamiento de datos personales en la institución se realiza con datos veraces?	x		x		x		-
28	¿Es importante que la institución cuente con datos personales veraces de sus colaboradores?	x		x		x		-
29	¿La institución le ha explicado cuál es la finalidad del tratamiento de sus datos personales?	x		x		x		-
30	¿La finalidad del tratamiento de los datos personales está claramente definida en la institución?	x		x		x		-
	PRINCIPIO DE SEGURIDAD	SI	NO	SI	NO	SI	NO	
31	¿Cree que se cumple con la fidelidad ética del tratamiento de datos personales en la institución?	x		x		x		-
32	¿Es importante mantener un ambiente institucional de fidelidad ética en el tratamiento de datos personales?	x		x		x		-
33	¿Considera eficiente el proceso de conservación de datos personales que realiza la institución?	x		x		x		-
34	¿Son seguros los medios de conservación de datos personales de la institución?	x		x		x		-
35	¿Cree que se cumple con la rectitud legal del tratamiento de datos personales en la institución?	x		x		x		-
36	¿Es importante mantener un ambiente institucional de rectitud legal en el tratamiento de datos personales?	x		x		x		-

Observaciones (precisar si hay suficiencia): NINGUNA

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

Apellidos y nombres del juez evaluador: Franco Castro, Darío Waldyr **DNI: 44592864**

Fecha: 10 de octubre de 2021

Especialista: Metodólogo [ ] Temático [X]

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

Anexo 5: Base de datos

Encuesta	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	5	4	5	4	4	5	5	5	4	4	5	5	5	5	4	5	5	5	4	4	4	5	5	5	5	4	5	4	5	5	5	4	4	4	4	4
2	1	4	4	5	5	4	5	5	4	5	5	5	5	5	4	5	5	5	4	5	5	5	5	4	5	4	5	5	4	5	5	5	5	4	5	5	5
3	1	4	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	4	4	4	5	4	4	4	4	5	5	5	5	5	5	4	5	4	5
4	1	5	5	5	5	4	5	5	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	5
5	2	5	5	5	4	5	5	5	5	4	5	5	5	5	4	5	5	4	5	5	5	5	4	5	5	4	5	5	5	5	5	5	5	5	4	4	4
6	2	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	4	4	4	5	4	4	5	5	5	5	5	5	4	5	5	5	4
7	1	5	4	5	4	4	4	4	5	4	3	4	4	4	5	3	4	5	5	5	5	5	5	4	5	4	4	5	5	5	5	4	5	5	4	5	5
8	1	5	5	4	5	5	5	4	5	4	4	5	5	4	4	5	4	5	5	5	5	4	5	5	4	4	5	5	4	5	4	5	5	4	4	5	5
9	2	5	4	5	5	4	5	4	4	4	4	5	4	4	5	5	5	4	5	5	4	5	5	5	5	5	4	4	5	4	5	5	5	4	4	4	5
10	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
11	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	4	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
12	2	5	5	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	5	5	5	5	5	4	5	5	5	4
13	1	5	4	4	5	5	5	5	5	4	4	5	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	4	4	4	4	4	5	5	4	4	5
14	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	4	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5
15	1	5	4	5	5	5	5	5	5	4	4	4	4	4	4	4	4	4	4	5	4	4	4	5	5	4	4	4	5	5	4	4	5	5	5	5	4
16	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
17	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5
18	2	5	4	5	4	4	4	5	5	4	5	5	5	4	4	4	4	4	4	5	5	5	5	3	5	4	5	5	5	4	5	4	4	5	5	5	5
19	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	4	5	5	4	4	4	5	4	5	5	4	4
20	2	5	5	5	5	4	4	4	4	4	5	5	4	5	5	4	4	4	4	4	4	5	5	5	4	4	4	4	4	5	5	5	5	4	5	4	4
21	1	5	4	5	5	4	5	4	5	5	4	4	5	4	4	5	5	5	4	4	4	5	5	5	5	4	4	4	4	5	5	4	4	5	5	4	5
22	1	5	4	5	4	5	4	4	4	5	4	4	5	5	5	5	4	4	4	5	4	4	4	4	4	4	4	4	4	5	5	5	4	4	5	4	4
23	2	4	5	5	4	5	4	4	5	4	4	5	4	4	4	5	4	4	4	5	5	4	4	5	4	4	4	5	4	4	5	5	4	5	4	5	5

Encuesta	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	2	5	4	5	4	4	4	5	5	4	4	5	5	4	4	5	4	5	5	5	5	4	4	4	4	4	4	4	4	4	5	4	4	5	4	5	4
25	1	5	5	5	5	4	4	5	4	4	5	5	4	5	4	4	4	5	5	4	4	4	4	4	5	5	4	4	4	5	4	4	5	5	5	5	4
26	1	5	4	4	4	5	5	5	5	5	4	4	4	4	4	4	4	4	5	5	5	5	5	5	4	5	4	4	4	4	5	5	5	5	5	5	4
27	1	5	4	5	4	5	4	4	4	4	5	5	5	5	4	4	4	4	4	5	5	5	5	5	5	5	5	4	5	4	5	5	5	5	4	5	5
28	2	5	5	5	4	4	4	4	4	4	4	4	4	5	5	5	4	4	4	5	5	4	4	5	5	4	4	4	4	4	5	5	4	5	5	4	4
29	1	5	4	4	4	5	5	5	4	4	5	5	4	4	5	4	4	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4	5	5	5	5	5
30	1	5	5	4	5	4	4	5	5	4	4	4	4	5	4	4	5	5	4	5	5	4	5	4	5	5	4	4	4	5	5	4	4	4	5	4	5
31	2	5	4	4	5	4	5	4	5	4	4	5	5	4	4	5	4	5	5	4	4	5	5	4	4	5	4	4	5	5	4	4	5	4	4	4	5
32	1	4	4	3	5	5	4	4	3	5	5	5	4	4	4	5	4	4	4	5	5	5	5	4	4	4	4	4	4	4	5	5	5	5	5	4	5
33	2	5	4	4	5	5	5	4	4	5	5	4	5	4	4	5	5	4	5	4	4	5	5	4	4	4	5	5	5	5	4	4	5	5	4	5	4
34	1	4	4	4	5	5	4	5	5	4	4	5	5	5	5	5	4	5	4	4	4	5	5	5	4	5	4	4	4	5	5	5	5	4	4	4	4
35	2	5	5	4	5	5	5	5	4	4	4	4	5	5	4	5	4	4	4	5	4	4	5	5	4	4	5	5	4	5	5	5	4	4	5	4	5
36	1	5	5	5	4	4	4	5	5	4	5	4	4	4	4	4	5	5	5	4	5	4	5	4	4	5	5	5	4	4	5	5	4	5	5	5	4
37	1	5	4	4	3	4	4	4	4	5	4	4	5	5	4	4	5	5	5	5	5	4	4	4	4	5	4	4	4	4	4	5	5	4	5	5	5
38	2	5	5	4	4	4	4	4	4	5	4	5	5	4	4	4	4	4	4	4	4	4	4	4	5	5	5	4	4	4	4	4	5	4	4	5	5
39	2	4	5	4	4	4	5	4	4	4	3	4	4	4	4	4	4	3	4	5	5	5	5	5	5	5	4	5	5	5	5	4	5	5	5	4	5
40	1	5	4	5	5	5	5	5	4	4	3	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	5	5	5	5	4	3	5	3	4
41	2	4	4	5	3	4	5	5	4	4	4	4	3	3	4	3	3	4	4	5	5	4	4	5	5	5	4	5	4	4	4	4	4	4	4	3	3
42	2	5	4	5	5	4	4	3	4	3	4	4	5	4	4	5	4	4	5	4	4	5	5	4	5	4	5	5	5	4	5	4	4	3	3	4	4
43	1	5	5	3	5	5	4	4	4	4	4	4	4	4	5	4	5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
44	1	4	4	4	4	4	4	3	3	4	3	4	5	5	4	4	4	4	4	4	4	4	5	4	5	4	5	4	5	4	5	4	4	5	4	4	4
45	1	4	4	4	4	3	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	5	4	4
46	1	4	5	5	5	5	5	5	5	4	4	5	5	5	5	4	4	4	4	4	4	4	4	4	4	4	5	5	4	4	4	4	5	4	5	5	5
47	1	5	5	4	4	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4

Encuesta	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
48	2	4	5	4	4	4	4	4	4	5	4	3	4	4	5	4	4	4	4	4	4	4	3	4	3	3	4	3	4	4	5	4	4	4	4	4	2
49	2	5	4	5	4	5	4	4	4	4	4	5	4	4	4	4	4	5	4	5	5	4	5	5	5	4	4	4	4	5	5	5	4	5	4	5	5
50	2	5	4	4	5	4	4	4	4	4	5	4	4	4	5	4	4	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4
51	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	5	4	4	5	5	4	5	5	4	4	4	4
52	2	4	4	4	5	5	5	4	4	4	4	4	5	5	4	4	4	4	4	5	5	4	4	5	4	4	5	5	5	4	4	4	4	4	4	4	4
53	2	4	4	5	4	4	4	4	4	4	4	5	4	4	4	4	4	5	4	5	4	4	4	5	4	5	5	4	5	4	5	5	5	4	5	4	4
54	1	5	4	5	4	4	5	5	4	5	4	4	5	5	5	4	4	5	4	5	5	4	5	5	4	4	5	5	4	4	5	4	4	5	5	4	5
55	2	5	4	5	5	5	4	4	5	5	4	4	5	5	4	4	4	5	5	5	4	5	4	5	5	4	4	5	5	4	4	4	5	4	5	4	5
56	2	5	4	5	4	5	4	5	4	5	5	4	4	5	5	4	4	5	5	5	4	4	5	4	4	5	5	4	5	5	4	4	5	4	5	5	4
57	1	4	5	5	4	5	4	4	5	5	4	4	5	5	4	5	5	4	4	5	4	5	4	4	5	4	4	5	5	5	4	5	5	4	5	5	4
58	1	4	5	5	4	4	5	5	4	5	5	4	5	5	5	4	5	4	4	5	5	4	5	5	5	5	5	4	5	4	5	4	5	5	4	4	5
59	2	5	4	5	4	5	5	4	4	4	5	5	5	4	4	4	5	5	4	5	5	4	4	5	5	5	4	5	4	5	5	4	4	5	5	4	4
60	2	5	4	5	5	4	5	5	5	4	4	5	5	4	5	5	5	4	4	5	5	4	5	4	4	5	5	4	5	5	4	5	5	4	4	4	5
61	1	4	5	4	5	5	4	5	5	4	5	4	5	5	5	5	4	4	4	4	5	4	5	5	5	4	4	5	5	5	5	5	4	4	4	4	4
62	1	5	4	5	5	4	5	4	5	5	4	5	4	5	4	5	4	5	5	4	5	5	4	4	5	5	5	5	4	5	5	5	4	5	5	4	4
63	2	5	5	4	4	5	4	4	4	4	4	4	5	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4
64	1	5	4	4	4	5	4	4	4	5	4	5	4	5	4	5	4	5	5	5	4	4	5	4	5	4	4	4	5	4	5	4	4	5	4	5	4
65	1	5	5	4	4	4	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	4	5	5	4	4	5	5	5	5	4	5
66	1	5	4	5	4	5	5	4	5	5	5	4	4	5	5	5	5	5	4	5	4	5	5	5	4	4	5	5	5	5	4	5	4	5	4	4	5
67	2	5	4	5	5	5	4	5	4	5	4	4	4	4	4	4	4	4	5	4	5	5	5	4	5	4	4	4	4	4	4	4	4	4	4	5	4
68	1	5	5	4	5	5	4	4	5	4	4	5	4	5	5	5	4	4	5	4	5	5	4	4	5	5	5	4	5	4	5	5	4	5	4	5	5
69	2	5	5	5	4	5	4	5	5	4	5	5	5	4	5	4	5	5	5	5	4	5	5	5	5	4	5	5	5	5	5	5	4	4	4	5	5
70	2	5	5	4	5	4	5	4	5	4	5	5	4	5	5	4	5	4	5	4	5	5	4	5	4	5	5	4	4	5	5	5	4	4	5	5	4
71	2	5	5	5	4	4	4	4	4	5	4	5	5	5	5	5	5	5	4	4	4	4	4	4	5	5	5	5	4	4	4	4	5	5	5	5	4

Encuesta	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
72	1	5	5	5	5	5	4	4	5	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	4	4	4	5	5	5	4	5	5	5	5	5	5
73	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
74	1	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
75	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
76	1	5	4	5	5	4	5	5	4	4	5	5	5	4	5	5	4	5	4	5	4	5	5	5	4	5	4	5	4	4	5	5	4	4	5	5	5
77	1	5	4	5	4	5	4	5	4	5	4	5	5	4	5	4	5	5	5	4	4	5	4	5	4	5	5	4	5	4	5	4	5	5	4	5	5
78	2	5	4	3	4	4	4	5	5	4	4	5	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4
79	1	5	4	5	4	5	4	5	4	5	5	4	4	5	5	4	5	4	5	5	4	5	5	5	5	5	4	4	4	5	5	5	4	5	4	4	5
80	2	5	4	5	5	4	5	5	4	4	5	5	4	5	4	5	4	5	4	5	5	5	4	5	4	5	5	5	4	5	4	5	5	5	4	5	5
81	1	5	4	5	5	4	4	5	4	5	5	4	5	4	4	5	5	4	5	4	5	4	5	5	4	4	5	5	4	5	4	5	4	5	5	5	5
82	2	5	4	5	4	5	5	5	4	5	4	5	4	5	4	5	5	4	5	4	5	4	5	4	5	5	4	5	4	5	4	5	4	5	4	5	5
83	1	5	4	5	5	4	4	4	4	5	5	4	5	5	4	5	5	4	5	5	5	4	4	4	5	4	5	4	5	5	5	5	5	5	5	4	5
84	1	4	5	5	5	5	4	4	4	5	5	5	5	4	4	4	5	5	5	4	5	4	4	4	4	4	5	4	5	5	5	5	4	4	4	5	5
85	1	4	5	4	5	5	4	5	5	4	5	4	5	5	5	4	4	4	5	5	4	5	5	4	4	5	4	5	4	5	4	5	5	5	4	4	5
86	2	5	4	4	5	5	5	5	4	4	5	5	5	4	4	5	5	5	4	4	5	5	5	4	5	4	5	5	4	5	5	4	5	4	4	4	5
87	1	5	4	5	4	5	4	5	5	4	4	5	5	5	4	4	5	5	4	5	5	4	5	4	5	5	4	5	5	4	5	4	5	5	4	5	5
88	1	4	5	4	5	5	4	5	5	4	5	5	4	5	5	4	5	4	5	5	4	5	4	4	4	5	5	4	5	5	4	4	4	5	5	5	5
89	1	4	5	5	4	4	5	5	4	4	5	5	5	4	4	4	5	5	4	5	5	5	4	5	5	4	5	5	4	5	4	5	5	5	5	4	5
90	2	4	5	4	5	4	5	4	5	5	4	5	4	5	4	5	4	4	5	5	5	4	5	5	4	5	5	4	5	4	4	5	5	4	5	5	5
91	1	4	5	5	4	4	5	4	5	5	5	5	4	4	5	4	4	5	5	5	5	5	5	5	5	5	4	4	4	4	5	5	4	4	4	5	5
92	1	5	4	5	4	5	4	5	4	5	5	4	5	4	5	5	5	5	4	5	4	4	5	5	5	4	5	4	5	4	5	5	4	5	5	4	5
93	2	4	5	4	4	5	5	5	4	4	5	5	4	5	4	4	4	5	5	4	4	5	5	5	5	5	4	5	5	4	4	4	5	5	5	5	4
94	1	4	4	5	4	4	4	4	5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
95	1	4	4	4	4	4	4	3	4	4	4	5	5	5	5	4	5	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4

Encuesta	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
96	1	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	5	4	4	5	5	5	4	4	5	4	4	4	4	4
97	2	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	3	3	4	4	4	3	4
98	1	5	5	4	4	4	4	4	4	4	4	4	4	5	5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
99	1	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4
100	2	5	5	5	5	5	5	4	4	4	4	4	4	4	4	5	5	5	5	5	4	5	4	5	5	4	4	5	4	5	4	5	4	4	5	5	4
101	2	4	5	5	5	5	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	5	4	5	5	5	4	5	5	4	4
102	1	4	4	3	4	4	4	4	4	5	4	4	4	4	4	5	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
103	2	4	5	4	5	5	5	5	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
104	1	5	5	4	4	5	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	4	4	4	4	4	5	4	5	5	5	5	5	4	4	5	4
105	2	5	5	4	4	5	5	5	4	5	5	4	4	4	5	5	4	4	4	4	5	5	4	5	4	4	4	4	4	5	5	4	5	4	5	5	4
106	2	5	5	5	4	4	4	5	5	4	4	4	5	5	4	4	4	5	4	4	5	5	5	4	5	4	4	4	4	5	5	5	5	4	4	4	5
107	1	5	5	5	4	4	4	4	5	4	4	5	5	5	4	4	5	5	4	4	5	5	5	4	4	5	4	5	4	4	4	4	5	4	4	4	5
108	1	5	5	4	4	5	5	4	4	5	4	5	4	5	4	4	5	4	5	4	4	5	4	4	5	5	5	4	5	4	3	5	4	4	4	5	5
109	1	5	5	4	4	5	4	4	5	5	5	5	5	5	4	4	4	4	5	5	5	4	4	4	5	5	5	5	4	4	4	5	5	5	5	4	4
110	2	5	4	5	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
111	1	4	4	5	4	4	4	4	5	5	5	5	4	4	5	4	4	5	5	5	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4
112	1	5	5	5	5	5	5	5	5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
113	1	3	3	4	3	3	3	3	4	4	3	4	3	3	3	4	3	3	3	4	4	3	3	3	3	4	3	4	4	3	3	3	3	3	3	4	3
114	2	4	3	3	3	4	3	4	3	3	3	3	4	3	3	3	3	3	3	4	3	3	3	3	3	4	3	3	2	3	3	4	3	3	4	3	3
115	1	4	3	3	3	3	2	3	4	3	4	3	3	3	3	4	4	3	3	4	3	4	3	4	4	4	3	3	3	3	4	3	4	3	3	4	3
116	1	4	3	3	4	4	3	3	3	3	3	3	3	3	4	3	3	3	3	3	4	4	3	4	3	3	3	3	3	4	3	3	4	3	3	3	4
117	2	3	3	3	2	3	3	3	4	3	3	3	4	4	3	3	3	3	3	4	3	3	3	3	4	3	3	3	4	3	3	3	3	3	4	3	3
118	2	4	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	4	3	3	3	2	3	3	3	2	3	3	3	3	3	3	3
119	1	3	4	3	4	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	4	4	3	3	3	4	3	3	3	3	3	3	3

Encuesta	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
120	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
121	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
122	1	3	3	3	3	3	3	3	3	3	3	3	3	3	4	4	4	3	3	4	4	4	4	3	4	4	4	3	4	4	3	4	4	4	4	4	4
123	2	3	3	3	3	2	2	2	2	3	3	3	3	3	3	4	3	4	3	3	4	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3
124	1	3	4	4	3	3	4	3	4	3	4	3	4	4	3	3	3	4	3	4	4	4	3	4	3	4	3	4	3	4	3	4	4	3	3	3	4
125	2	4	3	4	3	3	4	3	4	3	4	4	3	3	4	4	3	4	3	4	3	3	4	4	3	4	3	4	4	3	4	3	4	3	3	4	3
126	1	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	3	3	4	4	4	4	3	4	4	4	4	4	4	3	4	4	4	4	4	4
127	2	4	3	4	4	3	4	3	4	3	4	3	4	3	4	3	3	4	4	3	4	4	3	4	3	4	4	3	4	3	4	3	4	3	4	3	4
128	2	3	4	3	4	3	4	3	3	4	4	4	3	3	4	4	3	4	4	3	4	4	3	3	4	4	3	4	4	4	3	4	4	4	3	4	3
129	1	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4
130	2	4	3	4	3	4	3	3	4	4	3	3	3	4	3	4	3	4	4	3	4	3	4	3	4	4	3	3	3	4	3	4	4	3	4	3	4
131	2	4	3	4	4	3	3	4	3	4	4	3	3	4	4	3	4	3	4	4	3	3	4	4	3	4	4	3	4	3	4	4	3	3	3	4	4
132	1	4	3	3	4	4	4	4	3	3	4	4	3	3	3	4	4	3	4	4	3	4	4	3	4	3	4	4	4	3	4	3	4	3	4	4	4
133	1	4	3	4	3	3	4	3	4	3	3	4	4	3	3	3	4	4	4	3	4	4	3	4	4	4	3	4	4	3	4	4	3	4	3	4	3
134	2	3	4	3	3	3	4	4	3	3	4	3	4	4	4	3	4	3	4	4	3	3	4	3	4	4	4	3	3	4	4	3	4	3	4	3	4
135	2	4	3	3	4	4	3	3	4	3	4	4	3	4	4	3	4	4	3	4	3	4	4	4	3	3	4	4	4	4	3	4	3	4	4	4	3
136	2	4	3	4	4	3	4	3	3	4	4	4	3	4	3	3	4	4	3	4	4	3	4	4	3	3	3	4	4	3	4	4	3	4	4	3	4
137	2	4	3	4	4	3	4	4	3	4	3	4	4	4	3	3	3	4	4	3	4	3	3	4	4	3	3	3	3	4	3	3	4	4	3	4	3
138	2	3	4	3	4	3	3	4	4	4	3	4	3	3	4	3	3	4	3	4	3	4	4	3	3	3	3	3	4	4	3	3	3	4	4	3	3
139	1	4	4	3	3	4	3	4	3	4	3	4	4	3	3	4	4	4	4	3	4	4	3	4	3	3	3	3	4	3	4	3	3	4	4	3	3
140	2	4	3	4	3	4	4	3	3	4	3	4	4	4	4	4	3	3	4	3	4	3	3	4	4	3	3	4	3	4	4	3	4	4	3	4	4
141	2	4	3	4	4	3	4	3	4	4	3	4	4	4	3	4	3	4	3	4	4	3	4	4	3	4	3	3	4	4	4	4	3	3	4	4	3
142	2	4	3	4	4	4	3	3	4	4	3	3	4	3	4	3	3	4	3	4	4	3	4	4	3	4	3	3	4	4	3	4	4	3	4	3	4
143	2	4	3	3	4	3	4	4	3	4	3	3	4	4	3	3	4	3	4	3	4	3	4	4	3	4	3	3	3	4	4	3	4	4	3	4	3

Encuesta	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
144	1	3	4	3	4	3	4	3	4	3	4	4	3	4	3	4	3	4	4	3	4	3	4	4	4	3	3	4	3	3	4	4	3	4	3	4	4
145	1	4	3	4	3	4	4	3	4	4	3	4	4	3	3	4	4	4	3	4	3	3	4	4	3	4	3	4	3	3	3	4	4	3	4	3	4
146	1	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	3	4	3	3	3	4	3	3	3	4	3	4	4	3	4	4	3	3
147	1	4	3	4	4	3	4	3	4	3	3	4	4	4	4	3	3	4	4	4	3	4	3	4	3	4	4	4	3	3	3	3	4	4	4	4	3
148	2	4	3	4	3	4	3	4	4	3	3	4	3	3	4	4	3	3	4	4	3	4	3	4	4	3	4	3	3	4	4	3	3	4	3	4	3
149	2	4	4	3	4	4	4	4	3	4	4	3	3	4	3	4	4	3	3	4	4	3	4	3	3	4	4	3	4	4	3	4	3	4	3	3	4
150	2	4	3	4	4	4	3	3	3	3	3	4	4	3	4	3	3	4	3	3	3	3	3	4	4	4	3	3	4	3	3	4	4	3	4	3	4
151	1	3	4	4	3	4	4	4	4	4	4	4	3	3	3	4	3	4	3	4	3	3	3	4	3	3	3	4	4	4	4	3	3	4	3	3	4
152	1	4	4	3	4	3	3	3	4	3	4	4	4	3	4	3	3	4	4	4	3	4	3	3	4	4	4	3	4	4	3	4	3	4	3	3	4
153	2	4	3	4	3	3	3	4	4	4	3	4	4	4	3	4	4	4	3	4	3	4	3	4	4	4	3	3	4	4	3	3	4	4	3	3	4
154	1	3	4	3	4	4	4	3	3	3	3	3	4	3	3	3	3	4	4	4	4	4	3	3	4	3	4	3	3	3	4	3	4	3	4	3	3
155	1	3	3	4	4	4	3	4	3	3	4	4	3	3	4	3	4	4	3	3	3	4	4	3	4	3	3	4	3	3	4	4	4	4	4	4	3
156	1	4	3	4	4	3	3	4	3	4	3	3	4	3	3	4	4	4	3	4	4	3	4	4	3	4	4	4	3	4	3	4	3	4	3	4	4
157	2	4	3	4	4	3	3	4	3	4	4	3	3	3	4	4	4	4	3	3	3	3	3	3	4	3	3	3	3	4	4	3	4	3	3	4	4
158	1	4	3	4	3	4	4	3	3	4	4	4	4	4	4	3	3	4	4	3	4	4	3	4	3	3	4	3	3	3	3	4	4	3	3	4	4
159	1	4	4	3	3	3	4	4	3	3	4	4	3	3	4	3	4	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	3
160	2	4	3	4	3	3	4	4	3	3	4	3	4	4	4	3	4	3	3	4	3	3	4	3	3	4	3	3	3	3	3	4	3	3	3	4	4
161	1	4	3	4	4	3	4	3	4	3	3	4	4	4	3	3	4	4	3	4	3	3	4	3	4	3	4	4	4	3	3	4	3	4	3	3	4
162	2	3	4	4	4	3	4	3	4	3	4	3	4	4	3	3	4	3	4	4	3	4	3	4	3	4	4	3	3	4	4	3	4	3	4	4	4
163	2	3	4	3	4	4	3	3	4	4	4	3	3	4	3	4	3	4	3	4	3	4	3	3	4	4	3	4	3	3	4	4	4	3	3	3	4
164	1	4	3	4	4	3	3	4	4	3	4	3	4	3	3	4	4	3	4	3	4	4	4	3	3	4	3	3	3	4	3	4	3	4	3	4	3
165	2	4	4	3	3	4	4	3	3	4	3	4	4	3	4	3	4	4	4	3	3	4	4	3	3	4	3	4	4	3	3	4	4	3	3	3	4
166	1	4	3	4	3	4	3	4	4	3	4	4	4	3	3	3	3	4	3	4	4	4	3	4	4	4	3	3	4	3	3	4	3	4	4	3	4
167	1	4	3	4	3	3	4	3	4	4	3	4	4	3	3	3	3	4	3	4	3	4	4	3	3	3	3	3	3	3	4	4	3	4	3	3	4

Encuesta	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
168	2	4	3	4	4	4	3	3	3	4	3	3	4	4	4	3	4	4	3	3	4	3	4	3	4	3	4	4	3	4	3	4	4	4	3	3	3
169	2	4	3	3	4	3	3	4	4	3	3	3	4	4	4	4	3	3	4	3	3	4	4	4	3	3	4	3	4	4	3	3	4	4	3	4	3
170	1	4	3	4	4	3	4	4	3	4	3	4	3	3	3	3	4	4	3	4	3	4	3	3	4	4	4	4	3	3	3	4	3	4	4	4	3
171	1	4	4	3	3	4	3	4	3	3	4	4	3	4	3	4	4	3	3	4	4	3	4	3	3	3	4	4	3	3	4	3	4	3	4	4	3
172	2	3	4	4	3	4	4	3	3	4	3	3	3	4	4	4	3	4	3	3	3	4	4	3	3	4	3	4	4	4	4	3	3	3	3	4	3
173	2	4	4	3	3	4	4	3	3	4	4	4	3	3	3	4	3	4	3	4	3	3	3	4	4	4	4	4	4	4	3	3	4	4	4	3	3
174	2	3	3	3	3	3	4	4	3	3	3	4	3	4	4	3	4	4	4	4	3	3	4	4	4	3	4	3	4	4	3	4	3	4	3	4	3
175	2	4	4	3	4	3	3	3	3	4	4	4	3	4	3	4	3	3	4	4	3	3	3	4	3	3	4	3	3	3	4	4	4	3	3	4	3
176	2	3	4	3	4	3	4	3	3	4	3	4	3	3	4	3	4	4	3	3	4	4	4	3	3	3	4	4	4	3	4	3	3	3	3	4	4
177	2	4	3	4	4	3	3	4	4	4	3	4	3	4	4	4	3	3	4	3	4	3	3	3	3	4	3	4	4	4	3	4	3	3	4	4	4
178	2	4	3	3	3	4	4	4	3	4	4	3	3	4	4	4	3	4	3	4	4	3	4	3	4	3	3	4	4	3	4	4	4	3	3	4	3
179	1	4	4	3	3	4	4	4	4	3	4	4	4	3	3	3	3	3	4	4	3	4	4	3	3	4	4	3	4	4	3	4	3	3	4	3	4
180	2	3	4	3	4	3	4	4	3	4	3	4	4	3	3	4	3	4	3	4	3	4	4	3	3	4	4	3	3	4	4	3	4	4	3	3	4
181	1	4	3	3	3	4	4	4	3	3	4	3	3	4	4	3	4	3	4	3	3	3	4	3	4	4	4	3	4	3	4	4	3	4	2	4	4
182	2	4	3	3	3	4	4	4	4	3	3	3	4	4	4	4	3	4	3	4	3	3	4	3	4	4	3	3	3	4	3	4	4	3	3	4	3
183	2	4	3	3	3	4	4	4	4	3	3	4	4	4	3	3	4	4	3	4	3	4	4	3	4	3	4	3	3	3	3	4	4	4	3	3	4
184	1	4	3	3	3	4	4	4	4	3	4	3	3	4	4	3	3	4	3	4	3	4	3	3	4	4	4	3	4	3	3	4	4	4	3	3	4
185	1	3	4	4	4	3	3	3	3	4	3	3	4	3	4	3	4	3	4	4	3	4	4	3	4	3	4	3	4	5	3	4	3	4	3	3	4
186	1	4	3	3	4	4	3	3	4	4	3	3	4	4	4	3	4	4	4	3	3	4	4	4	4	4	3	3	4	4	3	4	3	4	4	3	3
187	2	3	4	3	4	3	4	3	4	4	3	3	4	4	3	4	3	3	4	3	3	4	4	4	3	3	3	3	4	4	4	3	4	3	3	4	4
188	2	3	4	3	3	3	4	3	3	3	3	4	3	3	2	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3
189	1	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3	4	3	4	3	3	3	4	4	3
190	1	4	3	3	2	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	4	3	3	4	3	3	4	3	3	3	3	3
191	1	4	4	4	3	3	4	3	4	3	3	4	4	4	3	3	4	4	3	3	3	4	3	4	3	4	3	4	3	3	3	4	3	4	4	4	3

Encuesta	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
192	2	4	3	4	3	3	3	4	3	4	3	4	4	3	3	4	4	3	4	4	4	3	3	3	3	3	3	4	4	4	4	4	3	4	3	4	4
193	1	4	4	3	3	4	3	3	3	4	4	4	4	4	4	4	4	3	4	4	4	3	4	4	3	4	3	3	3	4	3	4	3	4	4	3	4
194	2	4	3	3	4	4	4	4	3	4	4	3	4	3	3	4	3	4	4	3	3	3	4	4	4	3	3	4	4	4	4	4	3	4	3	4	4
195	1	4	3	3	3	3	4	4	4	3	4	3	3	3	4	4	4	3	4	4	4	4	3	3	3	4	4	4	3	4	4	3	4	3	4	4	3
196	1	3	3	4	3	4	3	3	4	3	3	3	2	3	3	4	3	3	4	3	3	3	3	4	3	4	3	3	3	4	3	3	3	4	3	4	3
197	2	3	3	4	4	4	3	3	3	3	3	3	2	2	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	4	3	4	3	4	3	3
198	1	4	4	3	3	3	3	3	2	3	3	3	3	4	3	3	3	3	2	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	2
199	2	4	3	3	3	4	3	3	3	4	3	3	3	2	2	3	3	3	3	3	4	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
200	1	3	3	4	3	4	3	3	3	4	4	4	4	3	3	3	3	2	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3	3	4
201	2	3	3	3	4	3	4	4	4	3	3	3	3	4	3	3	3	4	3	3	3	4	4	3	3	3	3	3	4	3	3	3	4	4	3	3	3
202	1	3	3	3	4	3	3	4	3	3	3	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3
203	1	3	3	3	3	4	3	4	3	4	4	4	4	4	4	4	5	3	3	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4
204	2	3	3	3	3	4	4	3	3	3	3	3	4	3	2	4	4	3	3	2	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	4
205	1	4	3	4	3	4	4	4	3	3	4	4	3	4	3	4	4	3	4	4	3	3	4	4	3	4	3	4	4	4	3	4	3	4	3	4	4
206	1	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	3	3	3	3	3	4	4	4	4	4	3	4	4	3	4	4	4	4	4	3
207	1	3	3	3	3	3	4	3	3	3	3	3	3	3	3	4	4	3	3	4	4	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
208	1	3	3	3	4	3	4	3	3	3	3	4	4	4	4	4	4	3	3	3	3	3	4	3	4	3	3	3	4	4	3	4	4	3	4	4	4
209	2	3	3	3	3	3	3	3	3	4	3	4	4	4	4	4	4	4	3	4	4	3	4	4	4	3	4	3	3	3	3	4	4	3	3	4	4
210	1	3	3	3	3	3	4	3	3	3	3	3	3	4	4	4	4	3	3	2	4	3	4	3	3	4	4	3	4	4	4	4	4	3	4	4	4
211	1	3	3	3	3	4	3	3	3	3	3	4	4	4	4	4	4	3	3	3	4	3	4	4	3	3	4	4	4	2	3	4	4	3	3	3	3
212	1	3	3	3	3	3	3	3	3	3	3	4	4	3	4	4	4	3	3	4	4	3	4	3	4	4	3	3	4	3	3	3	4	4	3	4	4
213	2	3	3	3	3	3	4	3	3	3	3	3	4	4	4	4	4	3	3	4	4	4	4	3	3	3	4	4	4	4	3	3	4	3	4	4	4
214	2	4	3	4	3	4	3	4	4	3	4	3	3	3	4	3	4	3	4	4	3	4	4	3	4	4	3	4	3	3	4	4	3	3	3	4	4
215	1	4	3	4	3	3	4	3	4	3	4	3	4	3	4	4	3	3	4	3	4	3	3	4	3	4	4	4	3	3	4	4	3	4	4	3	4

Encuesta	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
216	1	3	3	3	3	3	3	3	3	3	3	3	4	4	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	4	3	3	3	4
217	1	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3
218	2	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4
219	1	4	3	3	3	3	3	3	3	3	3	3	4	3	3	3	4	3	3	3	4	3	4	3	3	3	3	3	4	4	3	3	3	3	3	3	4
220	1	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3
221	1	3	4	4	3	3	4	3	3	4	4	3	4	3	4	4	3	4	3	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4
222	2	3	4	3	4	3	4	3	3	4	4	3	3	3	4	4	3	4	3	3	4	4	3	4	3	4	4	3	4	3	4	3	4	3	4	3	4
223	2	3	3	4	4	3	3	4	4	4	3	4	3	4	3	3	4	4	3	3	3	4	3	4	4	4	3	4	3	4	3	4	4	3	4	3	3
224	2	3	4	4	4	3	4	3	3	4	3	3	4	4	3	3	4	3	4	4	3	4	4	3	4	3	4	4	3	4	3	4	3	4	4	3	3
225	2	4	3	3	3	4	3	4	3	4	3	3	4	3	4	4	3	4	3	4	4	4	3	3	4	3	4	3	4	4	4	3	3	4	3	4	4
226	2	3	4	3	4	3	4	3	4	3	4	4	4	3	3	3	4	3	3	4	4	3	4	3	4	3	3	3	3	4	3	3	3	4	4	4	3
227	2	4	3	4	3	3	4	4	3	4	3	4	3	4	4	3	4	3	4	3	4	4	3	3	4	4	3	3	4	3	4	3	4	3	4	3	3
228	1	3	4	4	4	4	3	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	3	3	4	3	3	3	3	4	3	3	4	4	3	4	3
229	2	3	4	3	4	3	4	3	4	3	3	4	3	3	4	3	4	3	4	3	4	3	3	3	3	3	3	3	4	4	4	3	3	4	3	4	3
230	2	4	3	4	4	3	4	3	4	3	4	4	3	4	3	4	3	4	3	4	4	3	4	3	3	4	3	3	3	3	3	4	3	4	3	4	4
231	1	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	3	3	3	3	3	3	4	3	3	3	4	3	4	4	3	4	4	4	3	3	3
232	2	4	3	3	4	3	4	3	4	3	4	3	4	3	3	4	4	3	4	3	4	3	3	4	4	4	3	4	3	4	3	4	3	4	3	3	4
233	2	3	4	3	3	4	3	4	3	4	4	3	3	4	4	3	4	3	3	4	4	3	4	3	3	4	3	4	3	4	3	3	4	3	4	3	3
234	1	3	4	4	3	4	4	3	4	4	4	3	3	4	3	4	3	3	4	3	4	3	3	4	4	3	4	3	4	4	3	4	3	3	4	4	4
235	2	4	3	4	4	3	4	4	3	4	3	4	4	3	4	3	3	4	4	3	4	3	4	3	4	3	4	3	4	3	3	4	3	4	4	3	4
236	1	4	3	4	3	4	3	3	4	4	3	3	4	3	4	3	4	3	3	4	3	4	3	4	4	4	3	3	3	3	4	3	3	4	3	4	3
237	2	3	3	3	3	3	4	3	3	3	3	4	4	4	4	4	4	3	3	3	4	3	4	3	3	4	4	2	4	4	3	4	4	3	3	3	4
238	2	4	4	3	3	4	3	3	4	4	3	4	3	4	3	4	3	4	3	4	3	3	4	3	4	3	4	2	3	4	3	4	3	4	3	3	4
239	2	4	3	3	3	4	3	4	3	3	4	4	3	4	4	3	3	4	3	3	3	4	3	3	4	3	4	2	4	3	3	4	3	4	3	3	4

Encuesta	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
240	2	4	4	4	3	3	4	3	4	3	4	3	4	3	4	4	4	4	3	4	4	3	3	3	4	3	3	2	3	4	3	4	4	3	3	4	3
241	1	4	4	3	3	4	4	3	4	4	3	4	3	3	4	3	4	4	3	4	4	3	4	3	4	3	4	2	4	3	3	3	4	4	3	3	4
242	1	4	4	3	4	3	4	4	3	3	4	4	3	4	3	4	4	3	4	4	3	4	4	3	4	3	4	3	3	4	3	3	4	3	3	4	3
243	2	4	3	4	3	3	4	4	3	3	4	3	3	4	3	4	4	3	3	4	3	4	3	3	3	4	3	3	4	3	3	3	3	3	3	4	4
244	1	3	3	3	3	3	3	3	3	3	3	4	4	3	4	4	4	3	3	3	3	3	4	3	3	4	3	2	4	4	3	4	3	3	3	3	4
245	1	1	2	1	2	2	2	1	1	2	2	1	1	1	2	1	2	1	2	2	2	1	1	1	2	2	2	1	1	2	2	2	1	2	3	1	2
246	2	1	2	2	1	2	1	1	2	2	1	2	1	2	2	1	2	2	1	2	2	2	1	2	2	2	2	2	2	1	2	2	2	2	3	4	3
247	1	1	2	1	2	1	1	2	1	1	1	2	2	2	1	2	1	2	2	3	2	1	1	1	3	1	2	1	1	1	1	1	1	1	2	1	1
248	2	1	2	2	2	1	1	2	1	1	2	2	2	2	1	1	2	2	2	1	2	2	2	2	2	2	2	1	3	2	1	3	2	1	2	2	1
249	1	2	1	1	2	2	1	2	2	2	1	2	2	2	1	2	2	1	2	2	2	1	2	2	2	1	2	2	2	1	2	1	2	1	2	2	1
250	2	2	1	1	1	2	1	1	2	1	2	2	2	1	1	2	1	2	2	1	2	2	2	1	2	1	2	2	1	1	2	2	1	2	2	2	1
251	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
252	2	1	1	1	1	1	1	1	2	1	2	2	1	2	2	1	2	1	2	2	2	2	2	2	1	2	1	2	2	1	1	2	2	1	1	2	1
253	1	3	2	1	2	1	2	1	2	2	1	1	1	1	2	2	2	1	2	1	2	1	2	2	1	1	1	2	1	2	2	2	1	2	1	1	1
254	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
255	1	1	1	2	1	1	1	2	1	1	1	1	2	1	2	1	2	1	1	1	2	1	2	1	1	2	1	1	1	1	1	2	2	2	1	1	1
256	2	1	1	1	1	2	2	1	1	2	2	2	2	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	2	1	1	1	1	2	2
257	2	1	1	2	2	2	2	2	2	1	3	2	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	1	1	2	2	2	2	1	2	2	1
258	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	2	1	1	1	2	1	1	1	2	1	1
259	2	2	1	2	2	1	2	2	1	1	2	1	1	2	2	1	2	2	1	2	1	2	2	1	2	1	1	2	2	1	1	1	2	2	1	1	2
260	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
261	1	1	2	2	1	1	2	2	1	1	1	2	2	2	1	1	2	1	1	2	2	2	1	1	2	1	1	1	2	2	2	1	1	2	2	2	1
262	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	1	2	1	1	1	1	1	1

Encuesta	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
263	2	2	1	2	1	1	2	2	1	1	1	2	2	2	1	1	1	1	2	2	2	1	2	1	1	2	2	2	1	1	1	1	2	2	2	1	2
264	1	2	1	2	2	2	1	1	1	2	2	2	2	1	1	2	1	2	2	2	1	2	2	1	1	1	2	2	2	1	2	1	2	1	1	1	2
265	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1
266	2	2	1	2	1	2	1	2	1	1	2	2	2	1	2	1	1	2	2	1	2	2	2	1	1	1	1	1	2	1	2	1	1	1	1	2	2
267	2	1	2	1	1	2	2	1	2	1	2	1	2	2	1	2	2	1	1	2	1	2	1	2	1	2	2	2	1	1	1	2	2	1	2	1	2
268	1	2	1	1	2	1	2	2	1	1	2	2	1	1	2	2	2	2	1	1	1	1	2	2	2	2	1	2	2	1	1	2	2	1	2	2	1
269	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
270	2	2	1	1	2	2	1	1	2	1	2	2	1	2	1	2	1	1	2	2	2	2	1	1	2	1	1	2	2	1	2	2	1	1	2	1	1
271	1	2	2	1	2	1	2	2	1	1	2	2	1	1	2	2	1	2	1	2	2	2	1	2	2	1	2	1	2	1	2	1	2	1	2	1	2
272	2	2	1	2	1	1	1	2	2	1	1	1	2	2	1	2	2	1	2	1	1	2	2	2	2	2	1	2	2	1	2	1	2	1	1	2	5
273	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
274	2	1	2	2	2	1	1	1	1	1	2	2	1	1	2	2	1	1	2	1	1	1	1	2	2	1	2	1	1	2	2	1	1	1	2	2	2
275	1	1	1	2	2	1	2	2	1	2	1	2	1	2	1	2	2	1	1	2	1	2	1	2	1	2	2	2	1	2	2	1	2	2	1	2	2
276	2	1	2	1	2	2	1	2	2	1	1	1	2	2	2	1	1	1	1	2	2	2	1	1	2	2	2	2	2	2	1	2	1	1	1	1	2
277	1	1	2	1	2	1	2	1	2	1	2	1	1	2	2	2	1	2	2	2	1	2	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2
278	2	2	1	1	2	2	1	1	1	1	1	2	2	1	2	2	1	1	1	1	2	2	2	1	2	2	2	2	2	1	2	2	2	1	2	2	2
279	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
280	2	1	2	2	2	1	1	2	2	2	2	2	1	1	1	1	2	2	1	1	1	2	2	1	2	2	1	1	1	2	2	2	2	2	1	2	2
281	2	1	1	2	1	2	1	2	1	2	2	1	2	2	1	2	1	2	2	2	2	1	2	1	2	1	2	1	2	2	1	2	1	2	1	2	2
282	1	1	2	2	1	1	1	1	2	2	2	1	2	2	1	1	1	2	2	1	1	2	2	2	1	1	2	2	1	2	1	2	1	2	2	1	2