UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Ciberseguridad y su incidencia en el Teletrabajo en una entidad pública, Lima 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:
MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE INFORMACIÓN

AUTOR:

Marin Puris, Luis Enrique (orcid.org/0000-0002-2126-3753)

ASESOR:

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

CO-ASESOR:

Dr. Pereyra Acosta, Manuel Antonio (orcid.org/0000-0002-2593-5772)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

Dedicatoria

A Dios, pues es quién me guía y cuida en cada paso de mi vida; me fortalece y me ayuda a desarrollarme en lo personal y profesional y con quien vivo agradecido siempre en cada momento.

Agradecimiento

Agradezco a Dios por brindarme siempre las fuerzas necesarias para seguir adelante y poder alcanzar mi objetivo propuesto; a mis padres y hermana por ser soporte importante en mi vida. A los docentes de cada curso en esta maestría por sus conocimientos compartidos y a mi asesor por su apoyo riguroso y profesional en el desarrollo de mi tesis.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

La presente investigación tuvo como objetivo general determinar la incidencia de la Ciberseguridad en el Teletrabajo de una entidad pública, Lima 2022. El tipo de investigación que se empleo fue de tipo básica, con un diseño no experimental de tipo transversal de nivel correlacional causal; con el propósito de comprobar la incidencia de las variables estudiadas en un momento especifico. Asimismo, la población estuvo compuesta por 150 trabajadores que están ejerciendo sus labores en la modalidad del teletrabajo en la entidad pública, del cual, al aplicar el muestreo probabilístico aleatorio simple, se estableció una muestra de 108 trabajadores.

En el análisis descriptivo se utilizó tablas cruzadas e histogramas, del cual se evidencia que el Teletrabajo tendrá un nivel bueno ante la incidencia óptima de la Ciberseguridad; mientras que en análisis inferencial se usó la regresión logística ordinal, de cual se pudo concluir que existe incidencia significativa de la Ciberseguridad en el Teletrabajo; lo cual se fundamentó al tener obtener un valor de significancia de 0.000 menor a 0.05 el cual confirma la anterior conclusión. Además, se obtuvo un valor de R2 de Nagelkerke igual a 0.764, el cual representa el grado de incidencia entre las variables en un 76.4%.

Palabras clave: Ciberseguridad, Teletrabajo, Ciberespacio, Ataque cibernético.

Abstract

The present investigation had as general objective to determine the incidence of the Cybersecurity in the Teleworking of a public entity, Lima 2022. The type of research was used of basic kind, with a non-experimental design of transversal type of causal correlational level; with the purpose of verifying the incidence of the variables studied at a specific time. Also, the population was composed of 150 workers who are exercising their work in the modality of teleworking in the public entity, of which, by applying the simple random probability sampling, a sample of 108 workers was established.

In the descriptive analysis was used cross tables and histograms, from which it is evident that teleworking will have a good level before the optimal incidence of Cybersecurity; while in inferential analysis was used ordinal logistic regression, from which it could be concluded that there is significant incidence of Cybersecurity in Teleworking; which was based on having obtained a significance value of 0.000 less than 0.05 which confirms the previous conclusion. In addition, a value of R^2 of Nagelkerke equal to 0.764 was obtained, which represents the degree of incidence between the variables in 76.4%.

Keywords: Cybersecurity, Teleworking, Cyberspace, Cyberattack.

I. INTRODUCCIÓN

El teletrabajo ha sido una modalidad de realizar el trabajo que se originó en la década de los 70’s, siendo Estados Unidos y Europa los primeros en implementarlo. Esta modalidad se fundamenta principalmente en el uso de las tecnologías para la realización de la actividad laboral desde un espacio físico diferente al de la Institución.

A nivel internacional; con la venida de la pandemia del Covid-19 el uso de las tecnologías ha sido de esencial soporte para la economía y la sociedad global, el teletrabajo ha sido una de las herramientas primordiales para subsistencia de algunas empresas a nivel mundial, por lo cual como consecuencia gran cantidad de las personas pasaron a optar a esta forma de trabajo; en ese sentido la OIT (2020) indicó que solo una porción de la población laboral realizaba sus actividades desde sus hogares antes de que se produjera la pandemia, el teletrabajo en la Unión Europea solo era del 30%, en Dinamarca, Suecia y Países Bajos poco más del 35%, en Republica Checa, Italia, Polonia y Grecia apenas llegaban al 10% ,en EE. UU era el 20%, el 16% de la población laboral japonesa y el 1,6% de la población laboral argentina aplicaba esta modalidad de trabajo; con la llegada de la pandemia estos datos aumentaron en cada nación, se calcula que de cada 10 empleados 4 empezaron a laborar mediante el teletrabajo; en Finlandia el 60% de sus trabajadores pasaron a la modalidad de teletrabajo, del mismo modo en Luxemburgo, Bélgica, Dinamarca y Países Bajos más del 50%; igualmente en Irlanda, Suecia, Italia y Austria el 40%. En otras palabras, el 24% de los empleados europeos que nunca habían teletrabajado comenzaron hacerlo, a diferencia del 56% que teletrabajaba de vez en cuando. Este aumento de cantidades demuestra que, con el empleo adecuado de la tecnología y la reorganización del trabajo, se pueden realizar más trabajos de manera remota de lo que antes se pensaba.

A nivel nacional, nuestro país no se ha visto indiferente a esta nueva modalidad de trabajo y la necesidad de regularla como una nueva forma de prestación de servicios, en ese sentido Culqui et al. (2016) indicaron que en el Perú el teletrabajo se regula por

medio de la ley N° 30036, la cual se promulgó el 05 de junio del 2013, aprobada luego mediante DS N° 017-2015-TR el 03 de noviembre del 2015. Asimismo, dada la actual realidad pandémica debido a la Covid-19, el cual nos obligó a tener que modificar nuestro modo de vida habitual, provocando la necesidad de optar por el trabajo no presencial aprobado mediante el DU N° 026-2020, el cual estableció que las entidades del estado implementen el teletrabajo, provocando un cambio inesperado y acelerado de dicha modalidad de trabajo. En tal sentido, el MTPE (2020) indicó que en el mes de marzo 2,345 trabajadores laboraron bajo la modalidad del teletrabajo, luego en abril se incrementó a 45,595 trabajadores. Lo cual refleja un gran aumento de los empleados en la modalidad del teletrabajo a causa del contexto de pandemia, siempre que la naturaleza de sus labores se lo permitan.

Por otro lado, con la implementación de este nuevo modo de trabajo mediante los cuales los empleados puedan realizar sus labores en lugares que no son propios de la organización, este trajo como consecuencia una gran cantidad de ciberataques en el Perú. Según analistas de Eset (2021) indicaron que el Perú tuvo de nuevo la mayor cantidad de ataques informáticos por ransomware con respecto a las empresas de América Latina en el 2020 representando el 30% de estas, llevándose por delante el 14,9% de México, el 13,2% de Venezuela y el 11,3% de Brasil. De igual forma, los especialistas de Fortinet (2022) manifestaron que el Perú experimento en el 2021 más de 11,500 millones de intentos de ataques informáticos, lo que sería equivalente a 32 millones de intentos de ciberataques por día o un promedio de 1,3 millones por hora.

A nivel local, el teletrabajo ha generado grandes retos a las organizaciones para proteger toda información de los atacantes informáticos, con la finalidad de salvaguardar de manera efectiva la información que se accede mediante redes externas dentro del ciberespacio, dando un mayor compromiso al campo de la ciberseguridad, es por ello que las instituciones deben poner mucho énfasis en el tema de ciberseguridad, ya que los cibercriminales no descansan y siempre están buscando la oportunidad de vulnerar o dañar los activos de información importantes para las empresas y más cuando se ejercen sus labores en la modalidad del teletrabajo. Esta

situación no es ajena a la entidad pública, que durante el contexto de la modalidad del teletrabajo debido a la pandemia del Covid-19, la entidad ha presentado una mayor cantidad de ciberataques, provocando perdida o secuestro de información, bloqueo de los sistemas y caída de los servicios; esta situación compromete al personal del área de Soporte de Sistemas de Información, pues son ellos quienes canalizan todas las incidencias y reclamos de los usuarios. Es por ello que; mediante los resultados que se conseguirán de esta investigación, se podrá poner en práctica medidas para fortalecer y mejorar el teletrabajo tomando en cuenta la ciberseguridad, además de proporcionar datos y fomentar este tipo de investigaciones en otras instituciones.

Dado que existen 9 relaciones posibles conformadas por las dimensiones de la Ciberseguridad y el Teletrabajo, solo se realizó el análisis de 3 relaciones en esta investigación a consideración del investigador, sin perder el foco del objetivo de investigación, ni la naturaleza del método científico.

Ante todo lo indicado, se señaló el problema general: ¿De qué manera la Ciberseguridad incide en el Teletrabajo en una entidad pública, Lima 2022?, y como problemas específicos las siguientes interrogantes: ¿De qué manera la dimensión preservación de la confidencialidad de la Ciberseguridad incide en la dimensión espacio físico del Teletrabajo en una entidad pública, Lima 2022?, ¿De qué manera la dimensión preservación de la integridad de la Ciberseguridad incide en la dimensión uso de las TIC del Teletrabajo en una entidad pública, Lima 2022?, ¿De qué manera la dimensión preservación de la disponibilidad de la Ciberseguridad incide en la dimensión cambio organizacional del Teletrabajo en una entidad pública, Lima 2022?.

Concerniente a las justificaciones de la investigación; se justificó epistemológicamente, puesto que se utilizó teorías y conceptos científicos válidos con la finalidad de establecer adecuadamente el problema de investigación; además se empleó el método científico, el cual nos permitió validar las hipótesis propuestas tomando en cuenta los criterios de la razón y veracidad científica, así emitir un nuevo conocimiento a partir de los resultados conseguidos del trabajo de investigación. Además, se justificó

teóricamente, pues se fundamentó sobre una base teórica y conceptualizaciones de las variables estudiadas y de sus dimensiones, considerando la documentación científica relevante, para llegar a un entendimiento apropiado de la investigación que entregue un aporte significativo sobre la ciberseguridad y el teletrabajo. Así también se tuvo una justificación práctica, que se basa en la importancia de la implementación de la ciberseguridad de manera adecuada, con la finalidad de asegurar el correcto funcionamiento del teletrabajo en la entidad pública. Por último; se justificó metodológicamente, pues se aplicó un estudio no experimental, pues se llevó a cabo sin una intervención premeditada en las variables y sus fenómenos se analizaron en su medio natural.

Referente al objetivo general se señaló: Determinar la incidencia de la Ciberseguridad en el Teletrabajo de una entidad pública, Lima 2022. Además, los objetivos específicos: Determinar la incidencia de la dimensión preservación de la confidencialidad de la Ciberseguridad en la dimensión espacio físico del Teletrabajo en una entidad pública, Lima 2022. Determinar la incidencia de la dimensión preservación de la integridad de la Ciberseguridad en la dimensión uso de las TIC del Teletrabajo en una entidad pública, Lima 2022. Determinar la incidencia de la dimensión preservación de la disponibilidad de la Ciberseguridad en la dimensión cambio organizacional del Teletrabajo en una entidad pública, Lima 2022.

Respecto a la hipótesis general se señaló: La Ciberseguridad incide significativamente en el Teletrabajo de una entidad pública, Lima 2022. Asimismo, las siguientes hipótesis específicas: La dimensión preservación de la confidencialidad de la Ciberseguridad incide significativamente en la dimensión espacio físico del Teletrabajo de una entidad pública, Lima 2022. La dimensión preservación de la integridad de la Ciberseguridad incide significativamente en la dimensión uso de las TIC del Teletrabajo de una entidad pública, Lima 2022. La dimensión preservación de la disponibilidad de la Ciberseguridad incide significativamente en la dimensión cambio organizacional del Teletrabajo de una entidad pública, Lima 2022. (Ver Anexo 1).

II. MARCO TEÓRICO.

La presente investigación tuvo como fundamento las siguientes investigaciones previas, las cuales están relacionadas con las variables en estudio.

En los antecedentes nacionales se considera a Bohorquez (2021) en su estudio realizado sobre ciberseguridad y gestión de tecnologías de información, cuyo propósito fue demostrar la correlación de variables en la empresa I & T Electric; se hizo uso de la metodología cuantitativa y el diseño no experimental, considerando para su análisis estadístico un tamaño muestral de 71 miembros del personal laboral de la empresa, demostrando que existe una presencia correlacional significativa y positiva de las variables estudiadas, es decir, presentan un valor de correlación muy fuerte entre ellas; justificado con el estadístico Rho de Spearman obtenido de 0,832 milésimos. Asimismo, concluye que dicha empresa debería dar mayor prioridad en materia de ciberseguridad para poder tratar adecuadamente un ataque cibernético, capacitando a todo su personal en materia de ciberseguridad.

Además, Sánchez (2017) en su investigación referente a las estrategias de ciberseguridad y la protección de información, cuya intención fue comprobar el nivel en que inciden ambas variables en la oficina de economía del ejército, utilizó el enfoque metodológico cuantitativo, con el diseño de investigación no experimental, analizando a 152 personas como muestra de dicha institución, concluyendo como resultado que, al aplicar estrategias de ciberseguridad influyen en un grado significativo en la protección de la información. Asimismo, concluye que se debe priorizar desde los planes de concientización, capacitaciones, planes de protección contra ataques cibernéticos y contar la última tecnología en materia de ciberseguridad para tener una mayor protección de los activos de la institución.

También Inoguchi et al. (2017) con su estudio sobre la gestión de la ciberseguridad y la prevención de los ataques cibernéticos, cuya finalidad fue comprobar el grado en que inciden ambas variables en las pymes del Perú, hizo uso del enfoque metodológico

cuantitativo y un diseño no experimental, concluyendo que la gestión de la ciberseguridad evidencia una relación significativa en la prevención de ataques cibernéticos, ya que la ciberseguridad implica el análisis de riesgos y amenazas, decidiendo y tomando acciones con el propósito de prevenir y reducir los riesgos a un nivel aceptable y costo razonable; asimismo la ciberseguridad empleada en las organizaciones para salvaguardar y proteger los activos informáticos físicos y virtuales, debe ser de alta prioridad para la gerencia general; responsabilidad que también debe ser partícipe a todos los trabajadores de cualquier grado jerárquico.

Asimismo, Correa (2022) en su investigación tratada sobre ciberseguridad y el tratamiento de datos personales, cuyo fin fue corroborar el grado en que se correlacionan ambas variables en una municipalidad distrital perteneciente a lima sur; hizo uso del enfoque metodológico cuantitativo y un esquema de diseño no experimental, consideró para su análisis una muestra de 282 colaboradores de dicha municipalidad, se concluyó que la ciberseguridad evidencia una influencia significativa sobre el tratamiento de datos personales, justificado con el modelo RLO (Regresión Logística Ordinal) para obtener el grado en que inciden la variables, teniendo un valor de 9.256 milésimos, obteniendo un grado de significancia tendiente a cero, siendo menor a 0.05, afirmando así la incidencia significativa entre las variables analizadas. Finalmente, mediante la aplicación de la ciberseguridad en las propiedades de conservación de la confidencialidad, integridad y disponibilidad permite asegurar el tratamiento de datos personales en los principios de consentimiento, calidad y seguridad.

De igual importancia, Suarez (2020) con su trabajo de investigación tratado sobre la implementación del teletrabajo en la calidad de servicio, cuya finalidad fue demostrar la correlación evidente en la calidad de servicio mediante la implementación del teletrabajo en la UGEL San Pablo; hizo uso del enfoque metodológico cuantitativo y el diseño no experimental, consideró una capacidad muestral de 40 empleados; se concluyó que la implementación del teletrabajo evidencia una influencia significativa sobre la calidad de servicio, comprobándose estadísticamente con el estadístico Rho

de Spearman igual a 0.654 milésimos, evidenciando la relación significativa de las variables, además demostró que mediante la implementación del teletrabajo la institución logra brindar un servicio de calidad.

Así también Gutiérrez (2020), en su estudio relacionado al teletrabajo como estrategia empresarial sostenible, cuyo propósito principal fue comprobar la relación de causal de las variables estudiadas dentro de una empresa de consultoría, hizo uso del enfoque metodológico cuantitativo y el diseño no experimental. Dicho estudio finalizó concluyendo que, con la implementación del teletrabajo se generará resultados beneficiosos que favorecerán el aspecto de sostenibilidad empresarial en términos económicos, pues hay una ahorro significativo al no utilizar los servicios de las instalaciones de la empresa, ambientales, pues se evita la emisión de gases tóxicos la no tener que trasladarse al centro de labores y sociales, pues los trabajadores se sienten satisfechos al trabajar de esta modalidad, porque encuentran un equilibrio entre la vida relacionada a la actividad laboral y su vida íntima personal.

Con respecto a los antecedentes de tipo internacional mencionamos a Choejey et al. (2017), con su estudio de investigación relacionado a la percepción de la ciberseguridad en las organizaciones gubernamentales, realizada en Bután, cuya finalidad fue demostrar la efectividad de la ejecución de la ciberseguridad en las instituciones; hizo uso del enfoque metodológico cuantitativo con un esquema de tipo no experimental, con un alcance correlacional transversal. Dicha investigación concluye que la ciberseguridad en las organizaciones se está implementando de forma inadecuada, lo cual crea una brecha para definir un estado ideal de ciberseguridad organizacional. En tal sentido se determina que la implantación de la ciberseguridad en las organizaciones influencia en 40% sobre las políticas de ciberseguridad de las organizaciones.

De manera similar, Luh et al. (2020) con su estudio sobre ciberseguridad en ciencia y medicina: Amenazas y desafíos, estudio realizado en Estados Unidos, tuvo como objetivo demostrar el grado en que inciden las variables ciberseguridad y los problemas sobre la privacidad de información de los pacientes clínicos. La metodología empleada

fue cuantitativa de diseño de investigación no experimental. Esta investigación concluyó que, la ciberseguridad sanitaria evidencia una influencia positiva sobre la seguridad de información de los pacientes clínicos. Asimismo, se demuestra que, el uso apropiado de la información documentada de los pacientes en entornos de atención médica, requiere de una mayor coordinación y cooperación de los expertos en salud, instituciones gubernamentales competentes y la ciudadanía en general. Finalmente, se recomienda aplicar buenas prácticas y soluciones basadas en las necesidades de los pacientes involucrados en estudios en que se facilitan y exponen datos individuales de salud asociados implícitamente a la protección de información.

Además, Ronquillo et al. (2018), en su investigación tratada sobre tecnologías de la información sanitaria, piratería informática y ciberseguridad: tendencias nacionales en las violaciones de datos de información sanitaria protegida, realizada en Estados Unidos, cuya intención fue comprobar el nivel en que influye la ciberseguridad sobre la infraestructura TI de salud; esta investigación hizo uso del enfoque metodológico cuantitativo y el diseño no experimental, concluyendo que, la ciberseguridad influye significativamente sobre la infraestructura TI de salud; asimismo argumenta que mediante la acelerada adopción de tecnologías de información en materia de salud y los crecientes ataques cibernéticos de ransomware, la ciberseguridad ha pasado a ser prioritario en materia de salud y finalmente señala que la ciberseguridad debe mejorarse significativamente para que las infraestructuras TI de salud puedan ser efectivas y seguras, en tanto que la medicina esta más conectada e impulsada por la tecnología.

Asimismo, Pérez et al. (2020) con su estudio referente a la proposición de una política de ciberseguridad y la influencia de su implantación en las fuerzas armadas, realizado en Ecuador, cuya finalidad fue brindar una política de ciberseguridad referente a la protección de la información virtual; por medio de la colaboración y organización de las entidades encargadas de la seguridad informática en dicho país. Hizo uso del enfoque metodológico cuantitativo con diseño no experimental. La conclusión de este estudio se basa en el hecho de que, la propuesta de políticas de seguridad informática sustentadas por la investigación promueve un clima estable en aspectos relacionados a la

ciberseguridad, combinando prácticas vinculadas a las nuevas tecnologías emergentes en Ecuador; asimismo concluye que, una política de ciberseguridad influye de manera positiva en la protección de la información virtual.

Por último, Arias et al. (2015) con su estudio realizado sobre el modelo experimental de ciberseguridad y ciberdefensa, realizado en Colombia, estudio cuyo propósito fue elaborar un modelo de referencia que permita al gobierno de Colombia la parametrización de las condiciones de defensa dentro del ciberespacio en contestación a los ataques informáticos. Esta investigación llegó a concluir que, mediante el empleo de un modelo internacional de ciberseguridad se puede brindar un alto grado de protección de la información virtual en las organizaciones, minimizando el riesgo destructivo de los ciberataques.

Respecto a las teorías que fundamentan la investigación, mencionamos la Teoría General de Sistemas propuesta por Ludwig Von Bertalanffy, el cual estudia conceptos de sistemas las cuales se pueden aplicar en cualquier nivel y ámbito de estudio. Asimismo, Ñeco et al. (2018) indicaron que dicha teoría establece que un sistema es una red cuyas partes interactúan en función de su estructura y función. Además, especificaron que la teoría general de sistemas define diferentes niveles de complejidad y también utiliza términos relacionados con procesos técnicos que son de naturaleza social, pero que pueden transmitir el punto de vista requerido para la composición de un análisis. Además, Maldonado (2017) manifestó que esta teoría se compone de metodologías y métodos que útilmente se refieren a una vista prismática del universo en curso, generando un conjunto de soluciones a lo desconocido, en ese aspecto proporciona una dinámica donde las ideas se propagan con facilidad para permitir contribuciones. En ese sentido la sociedad y la ciencia se beneficiarán por igual. Así también, según Broks (2016) mencionó que todos los fenómenos se manifiestan como sistemas que funcionan como un todo, los cuales tienen elementos que se encuentran interrelacionados, siendo parte del entorno que lo rodea, relacionándose con otros sistemas de forma categórica; y es la unidad organizativa del pensamiento sistémico, y tal conocimiento es actualmente el significado elemental de la teoría de sistemas.

Asimismo, De la Peña et al. (2018) indicaron nuevos elementos, componentes y relaciones para la operatividad de los sistemas relacionados con novedosos logros científicos en la era digital, dando como resultado interpretaciones de fenómenos y procesos que permitan acercarse a la realidad objetiva de una forma más precisa y ofrece una representación más compleja de la mera realidad.

Por otro lado, la teoría de la agencia según Contreras et al. (2016) indicó que, desde esta perspectiva se reconocen dos protagonistas esenciales dentro de la institución, el principal o propietario, sujeto que debe contratar a un trabajador o empleado al cual se califica como agente, con el que necesitará compartir distinta información y situaciones de intercambio con diversos beneficios. Asimismo, Joaquim et al. (2017) dieron a conocer que esta teoría pretende especificar la correlación entre el dueño y el agente a partir de un punto de vista razonable, dicha relación se fundamenta en la obligación del agente al ejecutar una tarea para el principal en compensación de un pago previo acuerdo en relación al trabajo realizado, en ese contexto dicho acuerdo debe estar fundamentado en un contrato, el cual servirá como un medio de negociación entre ellos.

Así también, la teoría del comportamiento planeado según Seyal et al. (2017) mencionaron que esta teoría proporciona una base para la investigación de actitudes, principios subjetivos y el control conductual percibido, los cuales encaminan a intentos de conducta, provocando el comportamiento. Además, Zhang et al. (2018) indicaron que las personas con distintos marcos culturales actuarán de forma distinta con respecto a la seguridad de la información, permitiendo determinar patrones de comportamiento respecto a la seguridad de la información, logrando conocer el comportamiento de las personas ante problemas de seguridad, abarcando las tecnologías de información, la asignación de personal, el empleo de recursos, la administración pública entre otros aspectos.

Referente a la conceptualización de la variable independiente ciberseguridad, ISO/IEC 27032 (2012), estableció que la ciberseguridad se fundamenta en la preservación de la confidencialidad, integridad y disponibilidad de toda información almacenada en

computadores, sistemas de redes digitales y transmisión en grandes cantidades a nivel global, denominada como el ciberespacio. Asimismo, Wessels et al. (2021), expresaron que ciberseguridad reúne e implementa elementos, métodos, procesos y tecnologías para la seguridad de los activos digitales como sistemas y servicios contenidos en el ciberespacio, de manera que la seguridad esté enfocada a proteger de toda amenaza cibernética, sea esta una vulnerabilidad en la red o ataques por ciberdelincuentes. Además, Becerril (2019) expresó que ciberseguridad es la colección de herramientas, definiciones, normas, consejos, enfoques de gestión de riesgos, actos, enseñanzas, buenas praxis y tecnologías utilizadas para garantizar la seguridad cibernética y salvaguardar los activos informáticos institucionales y de los usuarios. Por último, Turk et al. (2021) y Rashid et al. (2021) manifestaron respecto a ciberseguridad, es la que combina un grupo de elementos tecnológicos, los cuales tienen como finalidad la protección los sistemas informáticos establecidos por ordenadores, red de datos, hardware, software y todo recurso tecnológico que se encuentra interactuando en el ciberespacio; asimismo indican que los ataques más frecuentes que se afronta mediante la ciberseguridad es el phishing, ransomware, malware, ataques mediante ingeniería social, entre otros.

Respecto a las dimensiones de la variable independiente ciberseguridad, este estudio de investigación propone a las dimensiones preservación de la confidencialidad, preservación de la integridad y la preservación de la disponibilidad; las cuales se expondrán a continuación. En cuanto a la dimensión preservación de la confidencialidad; Kaila et al. (2018) expresaron que preservación de la confidencialidad es el principio encargado de garantizar la protección de los datos, con el objetivo de que solo los usuarios autorizados puedan acceder a ellos. Además, Goucher (2016) indicó que preservación de la confidencialidad es lo que habitualmente se señala con la calificación de secreto, a tal efecto de que prohíbe a quienes no tienen permisos para acceder a dicha información, puesto que dicha información es de gran importancia para las organizaciones y por lo tanto debe asegurarse que esta sea reservada. Asimismo, De Oliveira et al. (2014) indicaron que la preservación de la confidencialidad de la información se caracteriza al encargarse de garantizar de impedir que se revele la

información no autorizada, es por ello que esta característica debe asegurar que solamente las personas con autorización logren tener acceso a dicha información crítica. Asimismo, Wright (2016) manifestó que la preservación de la confidencialidad debe asegurar que la información crítica de las organizaciones no se extravíe ni se difunda de manera no autorizada. Finalmente, Pawlicka et al. (2021), argumentaron que, preservación de la confidencialidad es un criterio estrechamente vinculado con la ciberseguridad y a la administración de la privacidad. Entonces, de lo anterior podemos deducir que la preservación de la confidencialidad es una de los medios que utiliza la ciberseguridad para combatir el ciberdelito.

En relación a la dimensión preservación de la integridad; Botta et al (2021) indicaron que, preservación de la integridad es la manera de asegurar, defender y confirmar que los datos e información contenido en los sistemas de seguridad primario no pueda ser alterada por agentes que no autorizados. Además, Pal et al. (2021) y Mohammadpourfard et al. (2020) señalaron que, preservación de la integridad tiene por finalidad proteger y mantener intacta los datos e información, sin que esta pueda ser alterada a través de su flujo en el ciberespacio; además recalcan que la preservación de la integridad debe garantizar imposibilitar toda forma de alteración de datos que no haya sido autorizada. Asimismo, Campbell (2016) mencionó que la preservación de la integridad es la característica que asegura que la información no haya sido manipulada por eventos intencionales, no autorizados o accidentales, con el propósito de que la información sea siempre correcta y precisa. Además, Argyropoulos et al. (2019) indicó que la preservación de la integridad es la responsable de proteger la información frente a cambios inapropiados, impidiendo las alteraciones no autorizadas, accidentales u intencionales en la data de los sistemas. Finalmente, Ameziane et al. (2015) mencionaron que la preservación de la integridad se refiere a garantizar la propiedad de la completitud, la cual es característica de la información para ser completa de inicio a fin, en tal sentido se debe impedir cualquier alteración irregular o ejecutada por una persona que no esté autorizada, y asegurando también que se permita realizar los cambios autorizados de la información.

Referente a la dimensión preservación de la disponibilidad; De Oliveira et al. (2014), se refirió a la preservación de la disponibilidad como la característica que debe asegurar que la información deba obtenerse de manera oportuna cuando sea necesario; asimismo menciona que tal propiedad debe estar presente en todos los activos de información, a los que deberán tener acceso solo los usuarios autorizados. Además, Kilovaty (2020) mencionó que la preservación de la disponibilidad es una característica que garantiza el acceso autorizado a las computadoras, datos y redes digitales los cuales son atacados por delincuentes informáticos al crearse escenarios por denegación de los servicios. Es tal aspecto, se puede entender que la preservación de la disponibilidad garantizar que los sistemas, aplicaciones y datos estén a disposición cuando se los requiera oportunamente. Del mismo modo, Vacca (2017) y Fosch-Villaronga et al. (2021) manifestaron que, preservación de la disponibilidad es una función esencial para el apoyo a la ciberseguridad; asimismo mencionaron que la preservación de la disponibilidad está absolutamente vinculada a un apropiado diseño sistemático compuesto por hardware, software, redes, normas y reglas de acceso a los datos, con el apoyo de indicadores estadísticos que aseguren el correcto rendimiento de los sistemas y servicios. Finalmente, según Najmi et al. (2021) indicaron que la preservación de la disponibilidad desde la óptica de la ciberseguridad, se consigue al garantizar poder acceder de manera completa, necesaria y debidamente autorizada a los sistemas y servicios contenidos dentro del ciberespacio.

Así también, referente al concepto de la variable dependiente del teletrabajo, mencionamos a LLamosas (2015), el cual manifestó que el teletrabajo es la manera de realizar la labor profesional desde un lugar diferente de la institución, y está compuesta por elementos como el espacio físico, el uso de las TIC y el cambio organizacional. Asimismo, la Organización Internacional del Trabajo (2020) definió al teletrabajo como el trabajo ejecutado por una persona denominado teletrabajador, el cual realizará dicha actividad desde su hogar o en otro establecimiento diferente del local laboral del empleador, a cambio de un sueldo, con la finalidad de entregar un resultado según lo señalado por el empleador. En ese sentido, según Eurofound (2017), indicó que es el aquel trabajo que no requiere del desplazamiento a un lugar físico, el cual se aplica con

el soporte de las TIC; en otras palabras, es la práctica laboral realizada mediante las TIC desde fuera de las instalaciones del empleador o desde su hogar. Del mismo modo Belzunegui et al. (2020), plantearon que el teletrabajo significa trabajar desde fuera de los establecimientos del empleador, apoyándose en las TIC; es así que esta labor puede realizarse en varios lugares, empleando diversas tecnologías y en distintas frecuencias. Finalmente, según Golden et al. (2019) mencionaron que el teletrabajo es el estilo de trabajo donde las personas dejan los lugares de trabajo habitual para trabajar desde casa e interactuar mediante las TIC.

Por lo expuesto anteriormente y tomando el concepto de la variable dependiente teletrabajo proporcionado por LLamosas (2015), en este estudio de investigación se propone como dimensiones a el espacio físico, el uso de las TIC y el cambio organizacional. Respecto a la dimensión espacio físico; Gallastegui (2016) mencionó que es el espacio donde se ubica el sujeto en fuente de estudio, dicho espacio está delimitado físicamente y su percepción está condicionada a los sentidos humanos, cuya composición está vinculada a la correlación entre el cuerpo y el espacio mediante las acciones que el cuerpo realiza sobre esta. Por otro lado, Fava (2020) argumentó que la distribución de los espacios físicos en cualquier institución, favorece de manera significativa en los temas respecto a la satisfacción de los colaboradores y el desempeño integral. Finalmente, Ural (2019) manifestó que la creación del espacio físico hace que la información de naturaleza sensorial proceda de ese espacio, logrando que dicha información sea significativa, o sea los hace existentes. No obstante, la representación del espacio físico no está condicionada a la información sensorial. Las características de los objetos que se sitúan en dicho espacio no son independientes de los rasgos existenciales deducidos.

Referente a la dimensión uso de las TIC; Quiroga-Parra et al. (2017) afirmaron que el uso de las TIC es la causa principal de cambios en el aspecto tecnológico de los países desarrollados, es por ello que el uso de las TIC es un nuevo insumo de información en todos los procesos organizacionales, para que las organizaciones puedan lograr su progreso. Además, Pinto-Fernández et al. (2018) manifestaron que el uso de las TIC es

una parte importante de las cualidades elementales de las personas, la cual hoy en día es una característica necesaria para formar una población más cualificada. Del mismo modo Faik et al. (2020) argumentaron que el uso de las TIC en la actualidad es consecuencia de un rápido progreso y de la capacidad de participación en la mayor parte de los aspectos de la sociedad, lo cual ha provocado una transformación digital de manera masiva. Así también, Carter et al. (2020) mencionaron que, el papel que desempeña el uso de las TIC después de la implementación de las TIC permite crear buenas prácticas en las organizaciones que intentan conseguir el máximo valor. Finalmente, según Peñates (2014) indicó que las TIC forman parte de una serie de tecnologías utilizadas para almacenar, sistematizar y difundir información, donde su uso contribuye a las tareas de las personas y de las organizaciones tanto sector público como del privado.

Referente a la dimensión cambio organizacional; Duque (2014) expresó que el cambio organizacional no debe ser una circunstancia que sorprenda a las organizaciones, sino ser un producto de procesos en continuo progreso, los que deben ser debidamente evaluados con la probabilidad de acontecimientos inesperados; por eso las organizaciones deben tener una cultura flexible para obtener mejores resultados. Asimismo, Saiyadain et al. (2017) argumentaron que el cambio organizacional es el resultado de la organización como un sistema cultural, en el que las personas cooperan entre sí, por lo que ante el cambio es necesario que cada representante de la cultura contribuya al logro de la armonía, tanto en el ambiente interno como externo. Así también, Kühl (2013) indicó que las organizaciones en la sociedad actual utilizan sus características, las cuales son establecidas por cualquier organización, ya sea empresarial o de la gestión pública, para enfocarse en metas que conlleven al bienestar de todos sus integrantes. Finalmente, Aujla et al. (2020) lo describieron como la introducción de nuevas ideas o procesos en una organización, ya sea interna o externa, a través de mejoras estructurales y de capacidad que resultan de ajustes en la organización de la dirección del proceso o de la capacidad de asimilar ante circunstancias imprevistas.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

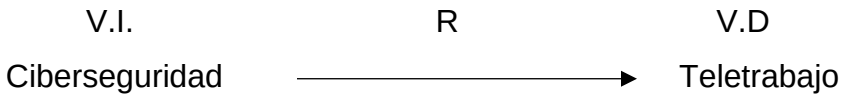
3.1.1. Tipo de investigación

El tipo básico fue empleado en este estudio; tomando en cuenta a Behar (2008), mencionó que una investigación del tipo básica se encarga de desarrollar nuevas teorías o modificar teorías existentes con el propósito de incrementar el conocimiento científico. De la misma forma, según la Ley Nº 31250 (2021), Ley del Sistema Nacional de Ciencia, Tecnología e Innovación, estableció que la investigación básica busca obtener un conocimiento más completo mediante la habilidad de comprender los aspectos elementales de los fenómenos, de los hechos observados y de las relaciones establecidas por los objetos que se estudian.

3.1.2. Diseño de investigación

Se empleó el diseño no experimental de tipo transversal de nivel correlacional causal; tomando en cuenta a Hernández et al. (2018), expresaron sobre el diseño no experimental, que es aquella que se da a cabo sin una intervención premeditada en las variables y donde los fenómenos se perciben solo en sus medios naturales para su análisis. De igual importancia, mencionaron que es transversal cuando los datos se recogen en un solo instante y para concluir indicaron que es correlacional causal pues su fin es conocer el valor correlacional evidente entre las variables estudiadas o fenómenos de una situación en específico, tanto en términos de correlación o como una relación de causalidad.

Esquema:



Donde:

VI: Variable Independiente Ciberseguridad

VD: Variable Dependiente Teletrabajo

R: Correlación causal entre V.I y V.D.

3.2. Variables y Operacionalización

Variable independiente: Ciberseguridad

De acuerdo con su naturaleza, se caracteriza por ser del tipo cualitativa y ordinal; tal como expresó Ríos (2017), indicó que una variable es de tipo cualitativa cuando manifiestan una cualidad, particularidad o propiedad que puede medirse numéricamente; por otra parte, mencionó que es ordinal puesto que muestra un criterio de ordenación entre sus categorías.

Definición Conceptual de la variable Ciberseguridad

Teniendo en cuenta a la ISO/IEC 27032 (2012), mencionó que la ciberseguridad se fundamenta en la preservación de la confidencialidad, integridad y disponibilidad de toda información almacenada en computadores, sistemas de redes digitales y transmisión en grandes cantidades a nivel global, denominada como el ciberespacio.

Definición Operacional de la variable Ciberseguridad

En cuanto a su operacionalización, se consideró 3 dimensiones definidas como preservación de la confidencialidad, preservación de la integridad y preservación de la disponibilidad; las cuáles fueron medidas a través de un cuestionario utilizando la escala de Likert, aplicando 5 categorías: (1) Muy en desacuerdo, (2) En desacuerdo, (3) Ni de acuerdo, ni en desacuerdo, (4) De acuerdo, (5) Muy de acuerdo. (Ver Anexo 2).

Variable dependiente: Teletrabajo

De acuerdo con su naturaleza, se caracteriza por ser del tipo cualitativa y ordinal; tal como señaló Ríos (2017), indicó que una variable es de tipo cualitativa cuando

manifiestan una cualidad, particularidad o propiedad que puede medirse numéricamente; además mencionó que es ordinal puesto que muestra un criterio de ordenación entre sus categorías.

Definición Conceptual de la variable Teletrabajo

Teniendo en cuenta a LLamosas (2015), manifestó que teletrabajo es la manera de realizar la labor profesional desde un lugar diferente de la institución, y está compuesta por elementos como el espacio físico, el uso de las TIC y el cambio organizacional.

Definición Operacional de la variable Teletrabajo

En cuanto a su operacionalización, se consideró 3 dimensiones, definidas como el espacio físico, el uso de las TIC y el cambio organizacional; las cuáles fueron medidas a través de un cuestionario utilizando la escala de Likert, aplicando 5 categorías: (1) Muy en desacuerdo, (2) En desacuerdo, (3) Ni de acuerdo, ni en desacuerdo, (4) De acuerdo, (5) Muy de acuerdo. (Ver Anexo 2).

3.3. Población, muestra y muestreo

3.3.1. Población

Teniendo en cuenta a Sánchez et al. (2018), indicaron que la agrupación compuesta por una colección de elementos u ocurrencias, los cuales pueden ser personas, objetos o eventos que tienen en común ciertas características o criterios, se denomina población; y puedan ser identificados en el área de investigación de interés, por lo cual contribuirán a las hipótesis de investigación. La población considerada en este trabajo de investigación fue de 150 miembros del personal laboral de la entidad pública (funcionarios públicos, servidores públicos) los cuales están realizando sus labores en la modalidad del teletrabajo; dicha distribución se especifica en la tabla 1.

Con respecto a ello se consideró como criterios de inclusión, a los trabajadores de la entidad pública que estén ejerciendo sus labores en la modalidad del teletrabajo a través de contrato fijo y temporáneo. De la misma forma, referente a los criterios de

exclusión, se exceptuó a los trabajadores de la entidad pública que no estén ejerciendo sus labores en la modalidad del teletrabajo, se encuentren de vacaciones o en descanso médico y al personal de limpieza.

Tabla 1

Detalle poblacional

Población	Cantidad
Funcionarios Públicos	30
Servidores Públicos	120
Total	150

Nota: Elaborado por el investigador.

3.3.2. Muestra

Teniendo en cuenta a Hernández et al. (2018), mencionaron que la parte representativa de una población en investigación, se denomina muestra; en donde se recogen los datos para generalizar los resultados. Para esta investigación el tamaño muestral se calculó mediante programa Decision Analyst STATS, contemplando un margen de error de 5%, un nivel de porcentaje estimado de 50%, un nivel de confianza de 95% y un valor poblacional de 150 trabajadores; resultando una muestra de 108 trabajadores.

Tabla 2

Detalle muestral

Muestra	Cantidad
Funcionarios Públicos	22
Servidores Públicos	86
Total	108

Nota: Elaborado por el investigador.

3.3.3. Muestreo

Con relación al muestreo considerado, fue el probabilístico aleatorio simple; teniendo en cuenta a Hernández et al. (2018), explicaron que dicho muestreo se distingue en que todas las unidades que componen la población, poseen igual viabilidad de ser escogidos para establecer la parte muestral.

3.3.4. Unidad de Análisis

Esta investigación consideró a todos los trabajadores que estén ejerciendo sus labores mediante el teletrabajo.

3.4. Técnicas e instrumentos de recolección de datos

Técnica de recolección de datos

Esta investigación empleó la encuesta. Teniendo en cuenta a Hernández et al. (2018), mencionaron esta técnica se emplea para recoger datos mediante el planteamiento de un conjunto de interrogantes.

Instrumento de recolección de datos

Esta investigación empleó el cuestionario. Teniendo en cuenta a Hernández et al. (2018) manifestaron que este instrumento está compuesto por una cantidad limitada de preguntas respecto a una o más variables, las cuales se someterán a medición. (Ver anexo 3).

Tabla 3

Ficha técnica del instrumento de medición

Nombre del instrumento	Cuestionario para los trabajadores de la entidad pública
Autor:	Marin Puris, Luis Enrique
Año:	2022

Tipo de instrumento:	Cuestionario
Objetivo:	Determinar la incidencia de la Ciberseguridad en el Teletrabajo de una entidad pública, Lima 2022.
Población:	150 trabajadores de la entidad pública, los cuales están realizando sus labores en la modalidad del teletrabajo.
Número de ítems:	36 en total, distribuidos en: 18 (V.I.) y 18 (V.D.)
Aplicación:	Virtualmente
Tiempo de aplicación:	15 min
Escala:	Escala de Likert: (1) Muy en desacuerdo, (2) En desacuerdo, (3) Ni de acuerdo, ni en desacuerdo, (4) De acuerdo, (5) Muy de acuerdo.
Niveles y rangos:	Óptimo [68 – 90] Regular [43 – 67] Deficiente [18 – 42]

Nota: Elaborado por el investigador.

Validez

La validez por juicio de expertos fue aplicada para la validación del instrumento de recolección de datos, a partir de la evaluación de la claridad, relevancia y pertinencia de las preguntas propuestas del cuestionario, mediante el certificado de validez de contenido del instrumento. (Ver anexo 4). Desde el punto de vista de Hernández et al. (2018), indicaron que la validación por juicio de expertos es el procedimiento donde el instrumento será evaluado de acuerdo con especialistas en el tema, con la finalidad de verificar si dicho instrumento realmente medirá la variable en estudio adecuadamente.

Tabla 4

Validación del instrumento de recolección de datos.

DNI	Experto	Procedencia	Calificación
09656793	Lezama Gonzales, Pedro Martin	Universidad César Vallejo	Aplicable
07268839	Pereyra Acosta, Manuel Antonio	Universidad César Vallejo	Aplicable
41541647	Flores Zafra, David	Universidad César Vallejo	Aplicable

Nota: Elaborado por el investigador.

Confiabilidad

Teniendo en cuenta a Hernández et al. (2018), mencionaron sobre la confiabilidad del instrumento, que es la medida del uso repetido de un instrumento, el cual debe producir los mismos resultados o muy similares al aplicarse en la misma persona, caso o muestra. Asimismo, para medir dicha confiabilidad se hizo uso del estadístico Alfa de Cronbach; De acuerdo con Hernández et al. (2018), indicaron que es un coeficiente que varía entre cero y 1, y cuando dicho valor se aproxime más a la unidad entonces se podrá decir que el instrumento posee una alta confiabilidad. Por otra parte, Tuapanta et al. (2017), indicaron que valores mayores a 0.7 justifican una alta confiabilidad.

En la prueba piloto de la aplicación del instrumento conformada por 30 encuestados, se consiguió un valor del Alfa de Cronbach igual a 0.806 y posteriormente para la evaluación general se obtuvo un valor igual a 0.759, la cual se hizo con 108 encuestados; dicha valoración certifica la aplicabilidad del instrumento para la investigación, por consiguiente, según la teoría revisada dichos valores son muy similares y demuestran una alta confiabilidad.

Tabla 5

Prueba de confiabilidad

Prueba	Nro. encuestados	Nro. elementos	Alfa de Cronbach
Piloto	30	36	.806
General	108	36	.759

Nota: Elaborado por el investigador, asistido por el software SPSS V27.

3.5. Procedimientos

La recopilación de información contempló los siguientes pasos; elaboración de instrumento, validación por juicio de expertos, aplicación piloto, análisis de confiabilidad de la aplicación piloto, aplicación general, análisis de confiabilidad de la aplicación general y finalmente con la información recolectada de las encuestas, se procedió a la

realización de la base de datos mediante el MS Excel y luego se trasladaron al SPSS para el procesamiento final, con el objeto de demostrar las hipótesis planteadas.

3.6. Método de análisis de datos

Se recurrió al uso del análisis descriptivo e inferencial para cada indicador mediante el software IBM SPSS V27.

Para la elaboración del análisis descriptivo se hizo uso de tablas cruzadas, apoyándose para la explicación de los datos a través de tablas e histogramas.

En la realización del análisis inferencial se aplicó la RLO (Regresión Logística Ordinal), la cual según Heredia et al. (2014) y Valverde et al. (2022) indicaron que este método de regresión pretende buscar la relación lineal de variables investigadas mediante una ecuación, con la intención de demostrar el grado en que se correlacionan causalmente las variables independiente y dependiente.

3.7. Aspectos éticos

Alineado a los principios reglamentados por el código de ética de la Universidad César Vallejo dispuesto por la Resolución de Consejo Universitario Nº0340-2021-UCV. Como principios éticos se consideró las señaladas posteriormente:

Respeto de la propiedad intelectual, porque toda la información utilizada total o parcialmente de los libros, tesis y revistas indexadas publicadas de otros autores, se citó y referenció conforme a la norma APA; con la finalidad de respaldar y resaltar los aportes empleados para esta investigación.

Probidad, puesto que la elaboración de esta investigación se realizó con honestidad en todo momento, puesto que los resultados obtenidos se mostraron de manera fidedigna, se evitaron las alteraciones no autorizadas de los protocolos ya acreditados por el

comité de ética, así como la inclusión de autores que no hayan contribuido en la investigación.

Beneficencia, puesto que la investigación buscó como finalidad alcanzar un beneficio para la organización y su personal, demostrando mediante los resultados la importancia de aplicar, mejorar y concientizar sobre el aspecto de ciberseguridad para la realización segura del teletrabajo.

Autonomía, ya que en la ejecución de este trabajo de investigación se respetó la voluntad de participación de las personas, los cuales podrán decidir no participar si así lo decidieran.

IV. RESULTADOS

Análisis descriptivos

Análisis descriptivo de la variable Ciberseguridad y la variable Teletrabajo

Tabla 6

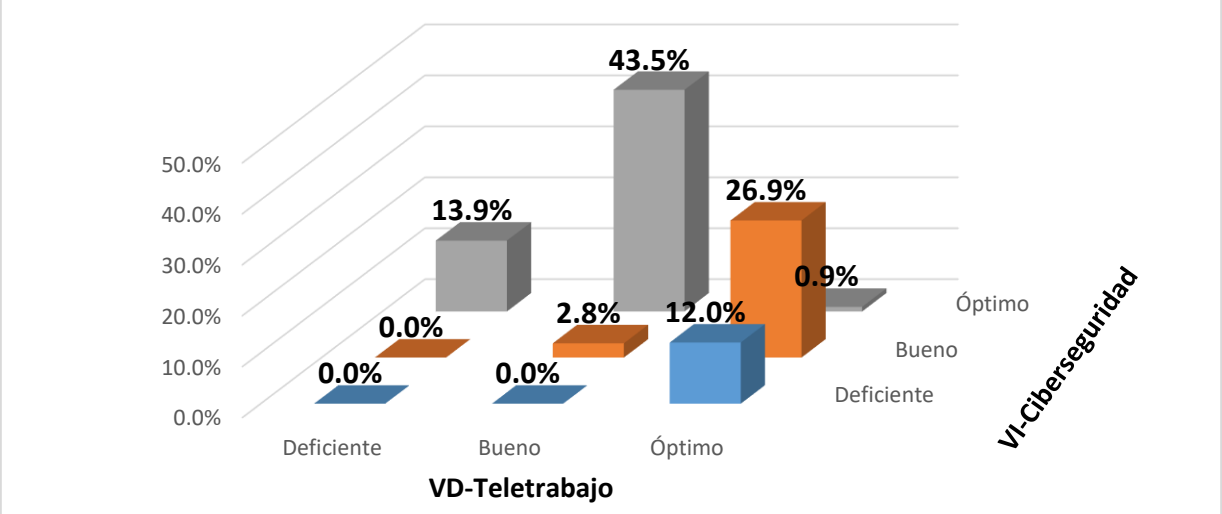
*Tabla cruzada VI-Ciberseguridad*VD-Teletrabajo*

		VD-Teletrabajo			
		Deficiente	Bueno	Óptimo	Total
VI-Ciberseguridad	Deficiente	0 (0.0%)	0 (0.0%)	13 (12.0%)	13 (12.0%)
	Bueno	0 (0.0%)	3 (2.8%)	29 (26.9%)	32 (29.7%)
	Óptimo	15 (13.9%)	47 (43.5%)	1 (0.9%)	63 (58.3%)
	Total	15 (13.9%)	50 (46.3%)	43 (39.8)	108 (100%)

Nota: Elaborado por el investigador, asistido por el software SPSS V27.

Figura 1

*Histograma VI-Ciberseguridad*VD-Teletrabajo*



Nota: Elaborado por el investigador, asistido por el programa MS Excel.

De la representación gráfica del histograma de la figura 1, se verifica que el mayor valor de frecuencia se manifiesta por la concurrencia que toma el nivel “Óptimo” de la Ciberseguridad y el nivel “Bueno” del Teletrabajo, teniendo 47 respuestas positivas que describen al 43.5% de la totalidad de los cuestionarios aplicados; por el contrario, el

menor valor de frecuencia se manifiesta por la concurrencia de los niveles “Deficiente” y “Bueno” de la Ciberseguridad y el nivel “Deficiente” del Teletrabajo, de igual forma se manifiesta por la concurrencia que toma el nivel “Deficiente” de la Ciberseguridad con el nivel “Bueno” del Teletrabajo, teniendo cero respuestas positivas que describen al 0.0% de la totalidad de los cuestionarios aplicados. También podemos visualizar una frecuencia intermedia considerable, como la que se manifiesta por la concurrencia que toma el nivel “Bueno” de la Ciberseguridad con el nivel “Óptimo” del Teletrabajo, teniendo 29 respuestas positivas que describen al 26.9% de la totalidad de los cuestionarios aplicados. Además, se presentan frecuencias intermedias de menor rango, como la que se manifiesta por la concurrencia que toma el nivel “Óptimo” de la Ciberseguridad con el nivel “Deficiente” del Teletrabajo, teniendo 15 respuestas positivas que describen al 13.9% de la totalidad de los cuestionarios aplicados, seguido por la concurrencia que toma el nivel “Deficiente” de la Ciberseguridad con el nivel “Óptimo” del Teletrabajo, teniendo 13 respuestas positivas que describen al 12.0% de la totalidad de los cuestionarios aplicados, seguidamente por la concurrencia que toma el nivel “Bueno” de la Ciberseguridad con el nivel “Bueno” del Teletrabajo, teniendo 3 respuestas positivas que describen al 2.8% de la totalidad de los cuestionarios aplicados, y finalmente la concurrencia que toma el nivel “Óptimo” de la Ciberseguridad con el nivel “Óptimo” del Teletrabajo, teniendo 1 respuestas positivas que describen al 0.9% de la totalidad de los cuestionarios aplicados. Por último, se logra verificar mediante la representación de la tabla 6, que el nivel “Óptimo” registra la mayor frecuencia de la Ciberseguridad, teniendo un acumulado de 63 respuestas positivas, que representan el 58.3% de la totalidad de los cuestionarios aplicados. De igual importancia el nivel “Bueno” registra la mayor frecuencia del Teletrabajo, teniendo un acumulado de 50 respuestas positivas, que representan el 46.3% de la totalidad de los cuestionarios aplicados.

Análisis descriptivo de la dimensión Preservación de la Confidencialidad de la variable Ciberseguridad y la dimensión Espacio Físico de la variable Teletrabajo

Tabla 7

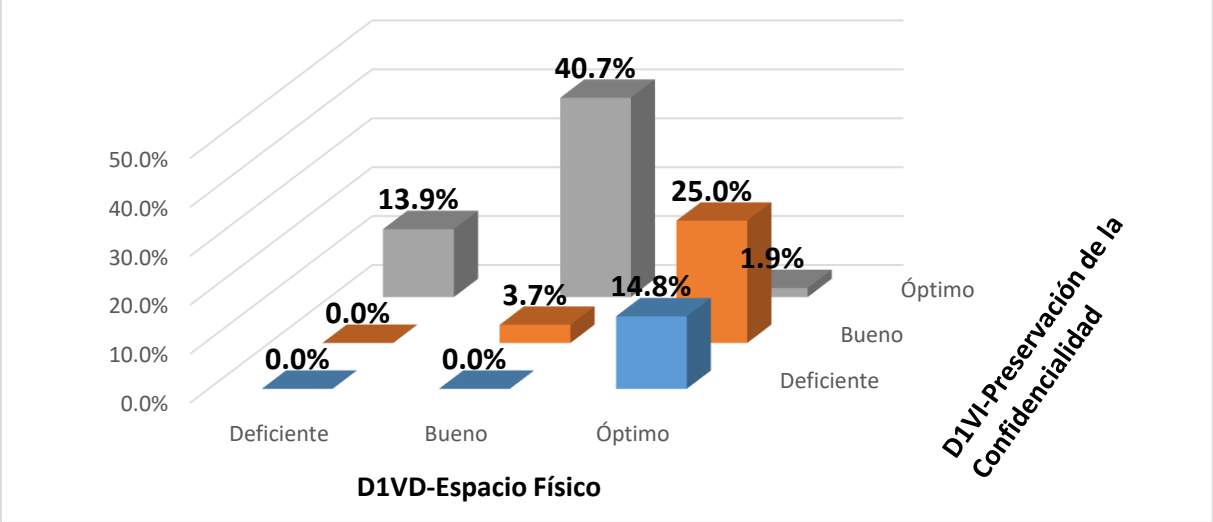
*Tabla cruzada D1VI-Preservación de la Confidencialidad*D1VD-Espacio Físico*

		D1VD-Espacio Físico			
		Deficiente	Bueno	Óptimo	Total
D1VI-Preservación de la Confidencialidad	Deficiente	0 (0.0%)	0 (0.0%)	16 (14.8%)	16 (14.8%)
	Bueno	0 (0.0%)	4 (3.7%)	27 (25.0%)	31 (28.7%)
	Óptimo	15 (13.9%)	44 (40.7%)	2 (1.9%)	61 (56.5%)
	Total	15 (13.9%)	48 (44.4%)	45 (41.7%)	108 (100%)

Nota: Elaborado por el investigador, asistido por el software SPSS V27.

Figura 2

*Histograma D1VI-Preservación de la Confidencialidad*D1VD-Espacio Físico*



Nota: Elaborado por el investigador, asistido por el programa MS Excel.

De la información presentada del histograma de la figura 2, se verifica que el mayor valor de frecuencia se manifiesta por la concurrencia que toma el nivel “Óptimo” de la dimensión Preservación de la Confidencialidad de la Ciberseguridad con el nivel “Bueno” de la dimensión Espacio Físico del Teletrabajo, teniendo 44 respuestas positivas que describen al 40.7% de la totalidad de los cuestionarios aplicados; por el contrario, el menor valor de frecuencia se manifiesta por la concurrencia de los niveles

“Deficiente” y “Bueno” de la dimensión Preservación de la Confidencialidad de la Ciberseguridad y el nivel “Deficiente” de la dimensión Espacio Físico del Teletrabajo, de igual forma se manifiesta por la concurrencia que toma el nivel “Deficiente” de la dimensión Preservación de la Confidencialidad de la Ciberseguridad con el nivel “Bueno” de la dimensión Espacio Físico del Teletrabajo, teniendo cero respuestas positivas que describen al 0.0% de la totalidad de los cuestionarios aplicados. También podemos visualizar una frecuencia intermedia considerable, como la que se manifiesta por la concurrencia que toma el nivel “Bueno” de la dimensión Preservación de la Confidencialidad de la Ciberseguridad con el nivel “Óptimo” de la dimensión Espacio Físico del Teletrabajo, teniendo 27 respuestas positivas que describen al 25.0% de la totalidad de los cuestionarios aplicados. Además, se presentan frecuencias intermedias de menor rango, como la que se manifiesta por la concurrencia que toma el nivel “Deficiente” de la dimensión Preservación de la Confidencialidad de la Ciberseguridad con el nivel “Óptimo” de la dimensión Espacio Físico del Teletrabajo, teniendo 16 respuestas positivas que describen al 14.8% de la totalidad de los cuestionarios aplicados, seguido por la concurrencia que toma el nivel “Óptimo” de la dimensión Preservación de la Confidencialidad de la Ciberseguridad con el nivel “Deficiente” de la dimensión Espacio Físico del Teletrabajo, teniendo 15 respuestas positivas que describen al 13.9% de la totalidad de los cuestionarios aplicados, seguidamente por la concurrencia que toma el nivel “Bueno” de la dimensión Preservación de la Confidencialidad de la Ciberseguridad con el nivel “Bueno” de la dimensión Espacio Físico del Teletrabajo, teniendo 4 respuestas positivas que describen al 3.7% de la totalidad de los cuestionarios aplicados, y finalmente la concurrencia que toma el nivel “Óptimo” de la dimensión Preservación de la Confidencialidad de la Ciberseguridad con el nivel “Óptimo” de la dimensión Espacio Físico del Teletrabajo, teniendo 2 respuestas positivas que describen al 1.9% de la totalidad de los cuestionarios aplicados. Por último, se logra verificar mediante la representación de la tabla 7, que el nivel “Óptimo” registra la mayor frecuencia en la dimensión Preservación de la Confidencialidad de la Ciberseguridad, teniendo un acumulado de 61 respuestas positivas, que representan el 56.5% de la totalidad de los cuestionarios aplicados. De igual importancia el nivel “Bueno” registra la mayor frecuencia en la dimensión de la dimensión Espacio Físico

del Teletrabajo, teniendo un acumulado de 48 respuestas positivas, que representan el 44.4% de la totalidad de los cuestionarios aplicados.

Análisis descriptivo de la dimensión Preservación de la Integridad de la variable Ciberseguridad y la dimensión Uso de las TIC de la variable Teletrabajo

Tabla 8

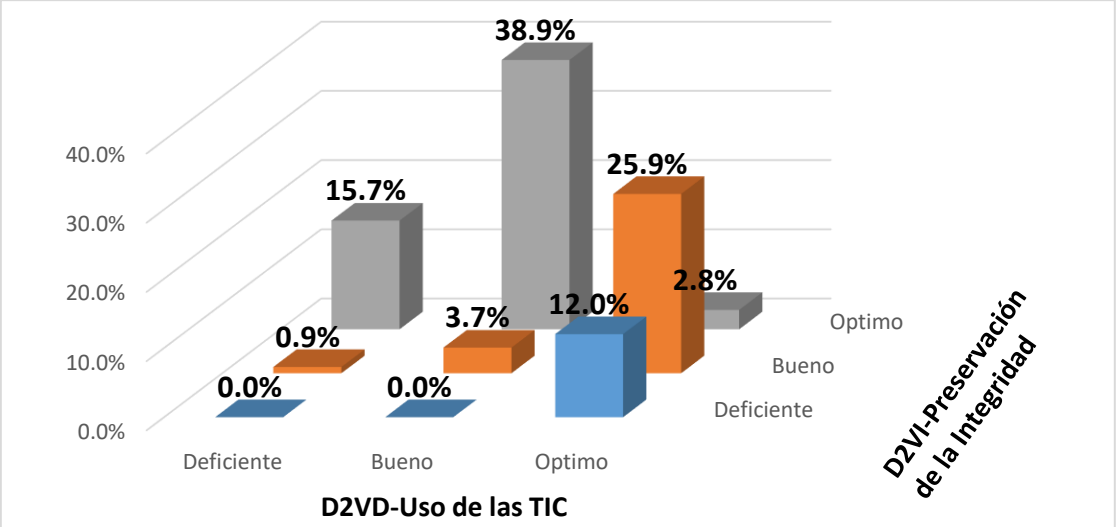
*Tabla cruzada D2VI-Preservación de la Integridad*D2VD-Uso de las TIC*

		D2VD-Uso de las TIC			
		Deficiente	Bueno	Optimo	Total
D2VI-Preservación de la Integridad	Deficiente	0 (0.0%)	0 (0.0%)	13 (12.0%)	13 (12.0%)
	Bueno	1 (0.9%)	4 (3.7%)	28 (25.9%)	33 (30.6%)
	Optimo	17 (15.7%)	42 (38.9%)	3 (2.8%)	62 (57.4%)
	Total	18 (16.7%)	46 (42.6%)	44 (40.7%)	108 (100%)

Nota: Elaborado por el investigador, asistido por el software SPSS V27.

Figura 3

*Histograma D2VI-Preservación de la Integridad*D2VD-Uso de las TIC*



Nota: Elaborado por el investigador, asistido por el programa MS Excel.

De la información presentada del histograma de la figura 3, se verifica que el mayor valor de frecuencia se manifiesta por la concurrencia que toma el nivel “Óptimo” de la dimensión Preservación de la Integridad de la Ciberseguridad con el nivel “Bueno” de

la dimensión Uso de las TIC del Teletrabajo, teniendo 42 respuestas positivas que describen al 38.9% de la totalidad de los cuestionarios aplicados; por el contrario, el menor valor de frecuencia se manifiesta por la concurrencia que toma el nivel "Deficiente" de la dimensión Preservación de la Integridad de la Ciberseguridad con los niveles "Deficiente" y "Bueno" de la dimensión Uso de las TIC del Teletrabajo, teniendo cero respuestas positivas que describen al 0.0% de la totalidad de los cuestionarios aplicados. También podemos visualizar una frecuencia intermedia considerable, como la que se manifiesta por la concurrencia que toma el nivel "Bueno" de la dimensión Preservación de la Integridad de la Ciberseguridad con el nivel "Óptimo" de la dimensión Uso de las TIC del Teletrabajo, teniendo 28 respuestas positivas que describen al 25.9% de la totalidad de los cuestionarios aplicados. Además, se presentan frecuencias intermedias de menor rango, como la que se manifiesta por la concurrencia que toma el nivel "Óptimo" de la dimensión Preservación de la Integridad de la Ciberseguridad con el nivel "Deficiente" de la dimensión Espacio del Teletrabajo, teniendo 17 respuestas positivas que describen al 15.7% de la totalidad de los cuestionarios aplicados, seguido por la concurrencia que toma el nivel "Deficiente" de la dimensión Preservación de la Integridad de la Ciberseguridad con el nivel "Óptimo" de la dimensión Uso de las TIC del Teletrabajo, teniendo 13 respuestas positivas que describen al 12.0% de la totalidad de los cuestionarios aplicados, seguidamente por la concurrencia que toma el nivel "Bueno" de la dimensión Preservación de la Integridad de la Ciberseguridad con el nivel "Bueno" de la dimensión Uso de las TIC del Teletrabajo, teniendo 4 respuestas positivas que describen al 3.7% de la totalidad de los cuestionarios aplicados, y finalmente la concurrencia que toma el nivel "Óptimo" de la dimensión Preservación de la Integridad de la Ciberseguridad con el nivel "Óptimo" de la dimensión Uso de las TIC del Teletrabajo, teniendo 3 respuestas positivas que describen al 2.8% de la totalidad de los cuestionarios aplicados. Por último, se logra verificar mediante la representación de la tabla 8, que el nivel "Óptimo" registra la mayor frecuencia en la dimensión Preservación de la Integridad de la Ciberseguridad, teniendo un acumulado de 62 respuestas positivas, que representan el 57.4% de la totalidad de los cuestionarios aplicados. De igual importancia el nivel "Bueno" registra la mayor frecuencia en la dimensión Uso de las TIC del Teletrabajo, teniendo un acumulado de

46 respuestas positivas, que representan el 42.6% de la totalidad de los cuestionarios aplicados.

Análisis descriptivo de la dimensión Preservación de la Disponibilidad de la variable Ciberseguridad y la dimensión Cambio Organizacional de la variable Teletrabajo

Tabla 9

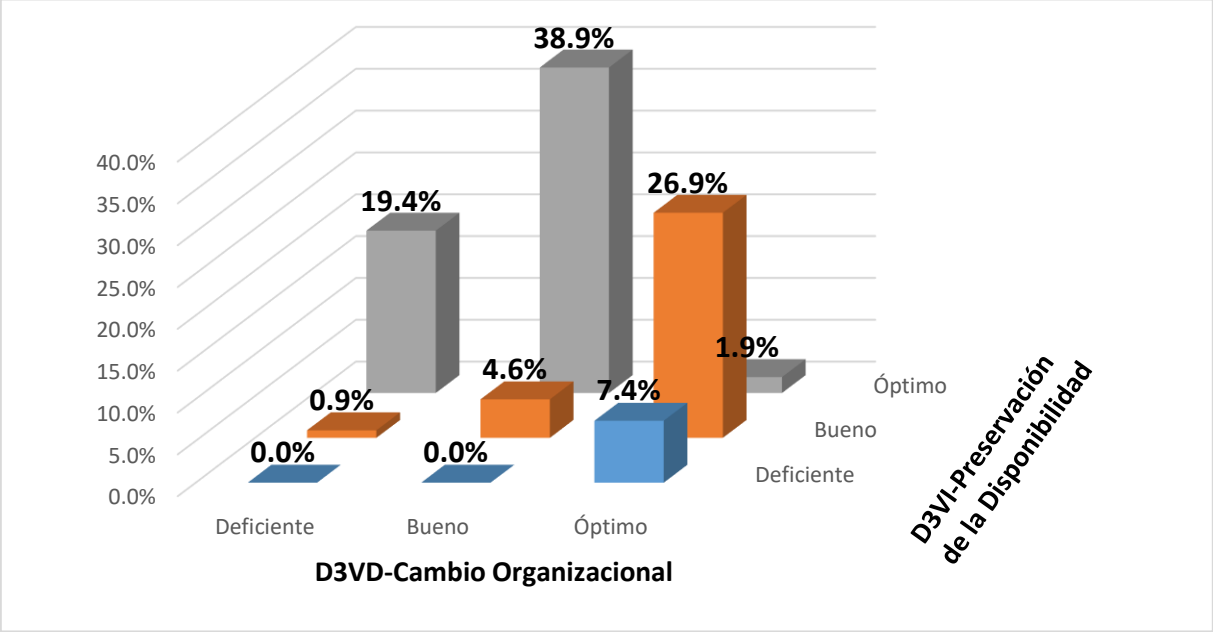
*Tabla cruzada D3VI-Preservación de la Disponibilidad*D3VD-Cambio Organizacional*

		D3VD-Cambio Organizacional			
		Deficiente	Bueno	Óptimo	Total
D3VI-Preservación de la Disponibilidad	Deficiente	0 (0.0%)	0 (0.0%)	8 (7.4%)	8 (7.4%)
	Bueno	1 (0.9%)	5 (4.6%)	29 (26.9%)	35 (32.4%)
	Óptimo	21 (19.4%)	42 (38.9%)	2 (1.9%)	65 (60.2%)
	Total	22 (20.4%)	47 (43.5%)	39 (36.1%)	108 (100%)

Nota: Elaborado por el investigador, asistido por el software SPSS V27.

Figura 4

*Histograma D3VI-Preservación de la Disponibilidad*D3VD-Cambio Organizacional*



Nota: Elaborado por el investigador, asistido por el programa MS Excel.

De la información presentada del histograma de la figura 4, se verifica que el mayor valor de frecuencia se manifiesta por la concurrencia que toma el nivel “Óptimo” de la dimensión Preservación de la Disponibilidad de la Ciberseguridad con el nivel “Bueno” de la dimensión Cambio Organizacional del Teletrabajo, teniendo 42 respuestas positivas que describen al 38.9% de la totalidad de los cuestionarios aplicados; por el contrario, el menor valor de frecuencia se manifiesta por la concurrencia que toma el nivel “Deficiente” de la dimensión Preservación de la Disponibilidad de la Ciberseguridad con los niveles “Deficiente” y “Bueno” de la dimensión Cambio Organizacional del Teletrabajo, teniendo cero respuestas positivas que describen al 0.0% de la totalidad de los cuestionarios aplicados. También podemos visualizar una frecuencia intermedia considerable, como la que se manifiesta por la concurrencia que toma el nivel “Bueno” de la dimensión Preservación de la Disponibilidad de la Ciberseguridad con el nivel “Óptimo” de la dimensión Cambio Organizacional del Teletrabajo, teniendo 29 respuestas positivas que describen al 26.9% de la totalidad de los cuestionarios aplicados. Además, se presentan frecuencias intermedias de menor rango, como la que se manifiesta por la concurrencia que toma el nivel “Óptimo” de la dimensión Preservación de la Disponibilidad de la Ciberseguridad con el nivel “Deficiente” de la dimensión Cambio Organizacional del Teletrabajo, teniendo 21 respuestas positivas que describen al 19.4% de la totalidad de los cuestionarios aplicados, seguido por la concurrencia que toma el nivel “Deficiente” de la dimensión Preservación de la Disponibilidad de la Ciberseguridad con el nivel “Óptimo” de la dimensión Cambio Organizacional del Teletrabajo, teniendo 8 respuestas positivas que describen al 7.4% de la totalidad de los cuestionarios aplicados, seguidamente por la concurrencia que toma el nivel “Bueno” de la dimensión Preservación de la Disponibilidad de la Ciberseguridad con el nivel “Bueno” de la dimensión Cambio Organizacional del Teletrabajo, teniendo 5 respuestas positivas que describen al 4.6% de la totalidad de los cuestionarios aplicados, y finalmente la concurrencia que toma el nivel “Óptimo” de la dimensión Preservación de la Disponibilidad de la Ciberseguridad con el nivel “Óptimo” de la dimensión Cambio Organizacional del Teletrabajo, teniendo 2 respuestas positivas que describen al 1.9% de la totalidad de los cuestionarios aplicados. Por último, se logra verificar mediante la representación de la tabla 9, que el

nivel “Óptimo” registra la mayor frecuencia en la dimensión Preservación de la Disponibilidad de la Ciberseguridad, teniendo un acumulado de 65 respuestas positivas, que representan el 60.2% de la totalidad de los cuestionarios aplicados. De igual importancia el nivel “Bueno” registra la mayor frecuencia en la dimensión Cambio Organizacional del Teletrabajo, teniendo un acumulado de 47 respuestas positivas, que representan el 43.5% de la totalidad de los cuestionarios aplicados.

Análisis Inferencial

Se hizo empleó la RLO (Regresión Logística Ordinal); Heredia et al. (2014) y Valverde et al. (2022) indicaron que este método de regresión pretende buscar la relación lineal de variables investigadas mediante una ecuación, con el propósito de comprobar la incidencia de la variable independiente sobre la variable dependiente, además este método se aplica siempre que la variable dependiente sea de tipo cualitativa y ordinal. Por otro lado, Heredia et al. (2014) indicaron que existirá una relación directa en la incidencia de la variable independiente sobre la variable dependiente, cuando dicho valor de estimación sea positivo y el valor de Wald diferente de cero.

Por otra parte, Juárez et al. (2016) indicó que coeficiente R^2 de Cox y Snell compara el modelo nulo solo con la constante con el modelo de “m” parámetros; dicho análisis se basa en el cálculo logarítmico de la verosimilitud de los 2 modelos, donde el mayor valor que puede tomar es menor a uno, aun cuando el modelo sea perfecto. El coeficiente R^2 de Nagelkerke es una versión mejorada del coeficiente R^2 de Cox y Snell, ya que este compara lo mismo que Cox y Snell, con la diferencia que esta cubre intervalos de cero a uno; por lo tanto, este coeficiente es más completo con respecto al anterior coeficiente y al de McFadden, pues este último también compara lo mismo que Cox y Snell. Además, señaló que el modelo tendrá un buen ajuste, cuando este valor tienda ser más cercano a uno.

Prueba de Hipótesis

Formulación de la hipótesis estadística:

H_0: La Ciberseguridad no incide significativamente en el Teletrabajo de una entidad pública, Lima 2022.

H_1: La Ciberseguridad incide significativamente en el Teletrabajo de una entidad pública, Lima 2022.

Contrastación de Hipótesis estadística:

Tabla 10

Información sobre el ajuste del modelo que explica la incidencia de la variable Ciberseguridad en la variable Teletrabajo

Modelo	Logaritmo de verosimilitud -2	X^2	gl	Sig.
Sólo intersección	125.800			
Final	9.192	116.608	2	.000

Función de enlace: Logit.

De la información presentada en la tabla 10, se logra verificar la significación estadística de 0.000, siendo este un valor inferior a 0.05; mediante el cual se logra determinar que la hipótesis nula (H_0) debe ser rechazada, aceptándose la hipótesis alterna (H_1). En ese sentido se certifica que, la variable Ciberseguridad si incide sobre la variable Teletrabajo, además se corrobora que el modelo se adapta a un análisis de RLO.

Tabla 11

Bondad de ajuste de la incidencia de la variable Ciberseguridad en la variable Teletrabajo

	X^2	gl	Sig.
Pearson	.017	2	.992
Desvianza	.033	2	.984

Función de enlace: Logit.

Conforme a la información presentada en la tabla 11, se logra verificar que el valor de X^2 de Pearson es 0.017 con una significancia de 0.992 el cual es mayor a 0.05, concluyendo que los datos analizados son consistentes con el modelo ajustado.

Tabla 12

Pseudo R^2 *de la incidencia de la variable Ciberseguridad en la variable Teletrabajo*

Coeficiente R^2	Valor
Cox y Snell	.660
Nagelkerke	.764
McFadden	.541

Función de enlace: Logit.

A partir de la información presentada en la tabla 12, se logra verificar el Pseudo R^2 de Nagelkerke es igual a 0.764, el cual es valor es muy cercano a la unidad; se toma a consideración dicho coeficiente por ser el más completo con respecto a los otros coeficientes mostrados en la tabla. Entonces podemos deducir que se tiene un modelo más ajustado que representa el comportamiento del grado en que incide la variable Ciberseguridad sobre la variable Teletrabajo, dicha incidencia equivaliendo a un 76.4%.

Tabla 13

Estimaciones de los parámetros de la incidencia de la variable Ciberseguridad en la variable Teletrabajo

		Estimación	Error estándar	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[Var2 = 1]	-1.164	.296	15.495	1	.000	-1.744	-.585
	[Var2 = 2]	4.144	1.008	16.900	1	.000	2.168	6.119
Ubicación	[Var1=1]	26.117	.000		1		26.117	26.117
	[Var1=2]	6.413	1.176	29.740	1	.000	4.108	8.718
	[Var1=3]	0[a]			0			

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

En función a la información presentada en la tabla 13, se logra verificar que el coeficiente de regresión estimado de la variable Ciberseguridad fue de 6.413, llegando

a obtener un valor de significancia igual a 0.000 y el coeficiente de Wald diferente de cero; demostrando una relación directa entre las variables analizadas, pues se tiene valores de estimación positivos y un valor de Wald distinto a cero. Seguidamente se puede inferir luego de usar la RLO, teniendo un valor de significancia inferior a 0.05 (error significativo); en conclusión, podemos indicar que se debe rechazar la hipótesis nula (H_0), aceptando la hipótesis alterna (H_1). Por esta razón, se logra afirmar que la Ciberseguridad incide significativamente en el Teletrabajo.

Prueba de Hipótesis especifica 1:

Formulación de la hipótesis estadística:

H_0: La dimensión Preservación de la Confidencialidad de la Ciberseguridad no incide significativamente en la dimensión Espacio Físico del Teletrabajo de una entidad pública, Lima 2022.

H_1: La dimensión Preservación de la Confidencialidad de la Ciberseguridad incide significativamente en la dimensión Espacio Físico del Teletrabajo de una entidad pública, Lima 2022.

Contrastación de Hipótesis estadística:

Tabla 14

Información sobre el ajuste del modelo que explica la incidencia de la dimensión Preservación de la Confidencialidad de la Ciberseguridad en la dimensión Espacio Físico del Teletrabajo

Modelo	Logaritmo de verosimilitud -2	X^2	gl	Sig.
Sólo intersección	117.492			
Final	10.074	107.418	2	.000

Función de enlace: Logit.

De la información presentada en la tabla 14, se logra verificar la significación estadística de 0.000, siendo este un valor inferior a 0.05; mediante el cual se logra determinar que la hipótesis nula (H_0) debe ser rechazada, aceptándose la hipótesis alterna (H_1). En ese

sentido se certifica que, la dimensión Preservación de la Confidencialidad de la Ciberseguridad si incide sobre la dimensión Espacio Físico del Teletrabajo, además se comprueba que el modelo se adapta a un análisis de RLO.

Tabla 15

Bondad de ajuste de la incidencia de la dimensión Preservación de la Confidencialidad de la Ciberseguridad en la dimensión Espacio Físico del Teletrabajo

	X^2	gl	Sig.
Pearson	.051	2	.975
Desvianza	.101	2	.951

Función de enlace: Logit.

Conforme a la información presentada en la tabla 15, se logra verificar que el valor de X^2 de Pearson es 0.051 con una significancia de 0.975 el cual es mayor al 0.05, concluyendo que los datos analizados son consistentes con el modelo ajustado.

Tabla 16

Pseudo R^2 de la incidencia de la dimensión Preservación de la Confidencialidad de la Ciberseguridad en la dimensión Espacio Físico del Teletrabajo

Coeficiente R^2	Valor
Cox y Snell	.630
Nagelkerke	.729
McFadden	.498

Función de enlace: Logit.

A partir de la información presentada en la tabla 16, se logra verificar el Pseudo R^2 de Nagelkerke es igual a 0.729, el cual es valor es muy cercano a la unidad; se toma a consideración dicho coeficiente por ser el más completo con respecto a los otros coeficientes mostrados en la tabla. Entonces podemos deducir que se tiene un modelo más ajustado que representa el comportamiento del grado en que incide la dimensión Preservación de la Confidencialidad de la Ciberseguridad sobre la dimensión Espacio Físico del Teletrabajo, dicha incidencia equivaliendo a un 72.9%.

Tabla 17

Estimaciones de los parámetros de la incidencia de la dimensión Preservación de la Confidencialidad de la Ciberseguridad en la dimensión Espacio Físico del Teletrabajo

		Estimación	Error estándar	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[D1Var2 = 1]	-1.124	.297	14.298	1	.000	-1.706	-.541
	[D1Var2 = 2]	3.409	.719	22.493	1	.000	2.00	4.818
Ubicación	[D1Var1=1]	25.386	.000		1		25.386	25.386
	[D1Var1=2]	5.321	.896	35.285	1	.000	3.565	7.076
	[D1Var1=3]	0[a]			0			

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

En función a la información presentada en la tabla 17, se logra verificar que el coeficiente de regresión estimado de la dimensión Preservación de la Confidencialidad de la Ciberseguridad fue de 5.321, llegando a obtener un valor de significancia de 0.000 y el coeficiente de Wald diferente de cero; demostrando una relación directa entre las variables analizadas, pues se tiene valores de estimación positivos y un valor de Wald distinto a cero. Seguidamente se puede inferir luego de usar la RLO, teniendo un valor de significancia inferior a 0.05 (error significativo); en conclusión, podemos que se debe rechazar la hipótesis nula (H_0), aceptando la hipótesis alterna (H_1). Por esta razón, se logra afirmar que la dimensión Preservación de la Confidencialidad de la Ciberseguridad incide significativamente en la dimensión Espacio Físico del Teletrabajo.

Prueba de Hipótesis especifica 2:

Formulación de la hipótesis estadística:

H_0: La dimensión Preservación de la Integridad de la Ciberseguridad no incide significativamente en la dimensión Uso de las TIC del Teletrabajo de una entidad pública, Lima 2022.

H_1: La dimensión Preservación de la Integridad de la Ciberseguridad incide significativamente en la dimensión Uso de las TIC del Teletrabajo de una entidad pública, Lima 2022.

Contrastación de Hipótesis estadística:

Tabla 18

Información sobre el ajuste del modelo que explica la incidencia de la dimensión Preservación de la Integridad de la Ciberseguridad en la dimensión Uso de las TIC del Teletrabajo

Modelo	Logaritmo de verosimilitud -2	X^2	gl	Sig.
Sólo intersección	106.475			
Final	14.865	91.610	2	.000

Función de enlace: Logit.

De la información presentada en la tabla 18, se logra verificar la significación estadística de 0.000, siendo este un valor inferior a 0.05; mediante el cual se logra determinar que la hipótesis nula (H_0) debe ser rechazada, aceptándose la hipótesis alterna (H_1). En ese sentido se certifica que, la dimensión Preservación de la Integridad de la Ciberseguridad si incide sobre la dimensión Uso de las TIC del Teletrabajo, además se confirma que el modelo se adapta a un análisis de RLO.

Tabla 19

Bondad de ajuste de la incidencia de la dimensión Preservación de la Integridad de la Ciberseguridad en la dimensión Uso de las TIC del Teletrabajo

	X^2	gl	Sig.
Pearson	4.977	2	.083
Desvianza	2.478	2	.290

Función de enlace: Logit.

Conforme información presentada en la tabla 19, se logra verificar que el valor de X^2 de Pearson es 4.977 con una significancia de 0.083 el cual es mayor al 0.05, concluyendo que los datos analizados son consistentes con el modelo ajustado.

Tabla 20

Pseudo R^2 de la incidencia de la dimensión Preservación de la Integridad de la Ciberseguridad en la dimensión Uso de las TIC del Teletrabajo

Coeficiente R^2	Valor
Cox y Snell	.572
Nagelkerke	.656
McFadden	.413

Función de enlace: Logit.

A partir de la información presentada en la tabla 20, se logra verificar el Pseudo R^2 de Nagelkerke es igual a 0.656, el cual es valor es muy cercano a la unidad; se toma a consideración dicho coeficiente por ser el más completo con respecto a los otros coeficientes mostrados en la tabla. Entonces podemos deducir que se tiene un modelo más ajustado que representa el comportamiento del grado en que incide la dimensión Preservación de la Integridad de la Ciberseguridad sobre la dimensión Uso de las TIC del Teletrabajo, dicha incidencia equivaliendo a un 65.6%.

Tabla 21

Estimaciones de los parámetros de la incidencia de la dimensión Preservación de la Integridad de la Ciberseguridad en la dimensión Uso de las TIC del Teletrabajo

		Estimación	Error estándar	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[D2Var2 = 1]	-.925	.281	10.846	1	.001	-1.475	-.374
	[D2Var2 = 2]	2.730	.520	27.542	1	.000	1.710	3.750
Ubicación	[D2Var1=1]	24.677	.000		1		24.677	24.677
	[D2Var1=2]	4.422	.706	39.232	1	.000	3.038	5.806
	[D2Var1=3]	0[a]			0			

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

En función a la información presentada en la tabla 21, se logra verificar que el coeficiente de regresión estimado de la dimensión Preservación de la Integridad de la Ciberseguridad fue de 4.422, llegando a obtener un valor de significancia de 0.000 y el coeficiente de Wald diferente de cero; demostrando una relación directa entre las variables analizadas, pues se tiene valores de estimación positivos y un valor de Wald distinto a cero. Seguidamente se puede inferir luego de usar la RLO, teniendo un valor de significancia inferior a 0.05 (error significativo); en conclusión, podemos indicar que se debe rechazar la hipótesis nula (H_0), aceptando la hipótesis alterna (H_1). Por esta razón, se puede afirmar que la dimensión Preservación de la Integridad de la Ciberseguridad incide significativamente en la dimensión Uso de las TIC del Teletrabajo.

Prueba de Hipótesis especifica 3:

Formulación de la hipótesis estadística:

H_0: La dimensión Preservación de la Disponibilidad de la Ciberseguridad no incide significativamente en la dimensión Cambio Organizacional del Teletrabajo de una entidad pública, Lima 2022.

H_1: La dimensión Preservación de la Disponibilidad de la Ciberseguridad incide significativamente en la dimensión Cambio Organizacional del Teletrabajo de una entidad pública, Lima 2022.

Contrastación de Hipótesis estadística:

Tabla 22

Información sobre el ajuste del modelo que explica la incidencia de la dimensión Preservación de la Disponibilidad de la Ciberseguridad en la dimensión Cambio Organizacional del Teletrabajo

Modelo	Logaritmo de verosimilitud -2	X^2	gl	Sig.
Sólo intersección	104.485			
Final	14.773	89.712	2	.000

Función de enlace: Logit.

De la información presentada en la tabla 22, se logra verificar la significación estadística de 0.000, siendo este un valor inferior a 0.05; mediante el cual se logra determinar que la hipótesis nula (H_0) debe ser rechazada, aceptándose la hipótesis alterna (H_1). En ese sentido se puede certificar que, la dimensión Preservación de la Disponibilidad de la Ciberseguridad si incide sobre la dimensión Cambio Organizacional del Teletrabajo, además se confirma que el modelo se adapta a un análisis de RLO.

Tabla 23

Bondad de ajuste de la incidencia de la dimensión Preservación de la Disponibilidad de la Ciberseguridad en la dimensión Cambio Organizacional del Teletrabajo

	X^2	gl	Sig.
Pearson	4.644	2	.098
Desvianza	2.411	2	.300

Función de enlace: Logit.

Conforme a la información presentada en la tabla 23, se logra verificar que el valor de X^2 de Pearson es 4.644 con una significancia de 0.098 el cual es mayor al 0.05, concluyendo que los datos observados son consistentes con el modelo ajustado.

Tabla 24

Pseudo R^2 de la incidencia de la dimensión Preservación de la Disponibilidad de la Ciberseguridad en la dimensión Cambio Organizacional del Teletrabajo

Coeficiente R^2	Valor
Cox y Snell	.564
Nagelkerke	.642
McFadden	.394

Función de enlace: Logit.

A partir de la información presentada en la tabla 24, se logra verificar el Pseudo R^2 de Nagelkerke es igual a 0.642, el cual es valor es muy cercano a la unidad; se toma a consideración dicho coeficiente por ser el más completo con respecto a los otros coeficientes mostrados en la tabla. Entonces podemos deducir que se tiene un modelo más ajustado que representa el comportamiento del grado en que incide la dimensión Preservación de la Disponibilidad de la Ciberseguridad sobre la dimensión Cambio Organizacional del Teletrabajo, dicha incidencia equivaliendo a un 64.2%.

Tabla 25

Estimaciones de los parámetros de la incidencia de la dimensión Preservación de la Disponibilidad de la Ciberseguridad en la dimensión Cambio Organizacional del Teletrabajo

		Estimación	Error estándar	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[D3Var2 = 1]	-.701	.263	7.104	1	.008	-1.216	-.185
	[D3Var2 = 2]	3.100	.595	27.169	1	.000	1.934	4.266
Ubicación	[D3Var1=1]	23.995	.000		1		23.995	23.995
	[D3Var1=2]	4.646	.740	39.456	1	.000	3.196	6.096
	[D3Var1=3]	0[a]			0			

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

En función a la información presentada en la tabla 25, se logra verificar que el coeficiente de regresión estimado de la dimensión Preservación de la Disponibilidad de la Ciberseguridad fue de 4.646, llegando a obtener un valor de significancia de 0.000 y el coeficiente de Wald diferente de cero; demostrando una relación directa entre las variables analizadas, pues se tiene valores de estimación positivos y un valor de Wald distinto a cero. Seguidamente se puede inferir luego de usar RLO, teniendo un valor significancia inferior a 0.05 (error significativo); en conclusión, podemos indicar que se debe rechazar la hipótesis nula (H_0), aceptando la hipótesis alterna (H_1). Por esta razón, se puede afirmar que la dimensión Preservación de la Disponibilidad de la Ciberseguridad incide significativamente en la dimensión Cambio Organizacional del Teletrabajo.

V. DISCUSIÓN

Concerniente al Objetivo General; tomando en cuenta los resultados alcanzados del análisis descriptivo, indican que la frecuencia más alta se da en la concurrencia del nivel óptimo de la Ciberseguridad con el nivel bueno del Teletrabajo, mientras que la menor frecuencia se da en la concurrencia del nivel deficiente de la Ciberseguridad con los niveles deficiente y bueno del Teletrabajo.

Además, del análisis inferencial se consiguió un valor R^2 de Nagelkerke igual a 0.764 (76.4%) que representa el grado en que incide la Ciberseguridad sobre el Teletrabajo, asimismo, mediante la prueba de Wald se llegó a obtener una significancia de 0.000 el cual es inferior a 0.05; por lo cual se comprueba que existen incidencia significativa de la Ciberseguridad en el Teletrabajo.

Los resultados antes señalados coinciden con los conseguidos por Bohorquez (2021), quien concluye de su investigación en la evidencia de la correlación significativa y positiva de la Ciberseguridad en la Gestión de Tecnologías de Información, justificándose en el estadístico de Spearman con un valor igual a 0.832, el cual determina un nivel de correlación muy alta de las variables investigadas, además indicó que se debe de dar mayor prioridad a la Ciberseguridad para afrontar de manera adecuada un ataque cibernético. Asimismo, Sánchez (2017), quien en su investigación concluye que se influye en un grado significativo en la protección de la información al aplicar estrategias de ciberseguridad, asimismo, concluye que se debe dar prioridad a los planes de concientización, capacitaciones, planes de protección contra ataques cibernéticos y contar la última tecnología en materia de ciberseguridad para tener una mayor protección de los activos de la institución. De la misma forma, Inoguchi et al. (2017), quienes concluyen de su estudio que la gestión de la ciberseguridad se relaciona significativamente con la prevención de los ataques cibernéticos, puesto que la ciberseguridad realizar un análisis de riesgos y amenazas, decidiendo y tomando acciones con el propósito de prevenir y reducir los riesgos a un nivel aceptable y costo razonable. De igual modo, Correa (2022), quien en su investigación concluye que la

ciberseguridad influye de manera significativa sobre el tratamiento de datos personales, comprobándose mediante la RLO para realización del cálculo de la incidencia, obteniendo un valor igual a 9.256 milésimos, y un grado de significancia tendiente a cero, siendo menor a 0.05; afirmando así la incidencia significativa entre las variables analizadas. De forma similar, Choejey et al. (2017), quienes en su investigación concluyen que la implantación de la ciberseguridad en las organizaciones influencia en 40% sobre las políticas de ciberseguridad de dichas organizaciones. Además, Luh et al. (2020), quienes concluyen de su estudio que existe una influencia positiva de la ciberseguridad sanitaria sobre la seguridad de la información de los pacientes clínicos. Asimismo, Ronquillo et al. (2018), quienes concluyen de su investigación que la ciberseguridad incide significativamente sobre la infraestructura de TI de salud; asimismo señala que la ciberseguridad debe mejorarse significativamente para que las infraestructuras de TI de salud puedan ser efectivas y seguras, en tanto que la medicina esta más conectada e impulsada por la tecnología. Así también, Pérez et al. (2020), quienes concluyen de su estudio que la implementación de una política de ciberseguridad combinando prácticas vinculadas a nuevas tecnologías, influye de manera positiva en la protección de la información virtual. Por último, Arias y Celis (2015), quienes en su investigación concluyen que la ciberseguridad mediante el empleo de un modelo internacional de ciberseguridad se puede brindar un alto grado de protección de la información virtual en las organizaciones, minimizando el riesgo destructivo de los ciberataques.

Los resultados se relacionan con las definiciones de Ciberseguridad, las cuales según la norma ISO/IEC 27032 (2012), indica que la ciberseguridad se fundamenta en la preservación de la confidencialidad, integridad y disponibilidad de toda información que se encuentra en el ciberespacio, la cual está almacenada en computadores, sistemas de redes digitales y transmisión de la misma en grandes volúmenes a nivel mundial. Asimismo, Wessels et al. (2021), señalaron que ciberseguridad implementa elementos, métodos, procesos y tecnologías para brindar seguridad a los activos digitales como sistemas y servicios que se encuentran dentro del ciberespacio, de manera que se orienta a proteger de todo ataque cibernético, sea esta una debilidad en la red o ataques

por delincuentes cibernéticos. Además, se relacionan con el concepto del Teletrabajo, el cual según LLamosas (2015), indicó que el Teletrabajo es la forma de cumplir la actividad laboral profesional desde un lugar diferente de la institución, la cual se compone por elementos como el espacio físico, el uso de las TIC y el cambio organizacional.

En relación al Objetivo Específico 1; de acuerdo a los resultados alcanzados del análisis descriptivo, describen que la frecuencia más alta se da en la concurrencia del nivel óptimo de la dimensión Preservación de la Confidencialidad de la Ciberseguridad con el nivel bueno de la dimensión Espacio Físico del Teletrabajo, mientras que la menor frecuencia se da en la concurrencia del nivel deficiente y bueno de la dimensión Preservación de la Confidencialidad de la Ciberseguridad con los niveles deficiente y bueno de la dimensión Espacio Físico del Teletrabajo.

Además, del análisis inferencial se consiguió un valor R^2 de Nagelkerke igual a 0.729 (72.9%) que representa el grado en que incide la dimensión Preservación de la Confidencialidad de la Ciberseguridad en la dimensión Espacio Físico del Teletrabajo, asimismo, mediante la prueba de Wald se llegó a obtener una significancia de 0.000 el cual es inferior a 0.05; por lo cual se comprueba que existen incidencia significativa de la dimensión Preservación de la Confidencialidad de la Ciberseguridad en la dimensión Espacio Físico del Teletrabajo.

Los resultados antes señalados coinciden con los alcanzados por Correa (2022), quien evidencia en su estudio la importancia de la propiedad de la preservación de la confidencialidad de la ciberseguridad en el tratamiento de los datos personales de pacientes clínicos, ya que esta información es sumamente significativa y a la que solo se debe acceder por el personal que tenga autorización, la propiedad de la preservación de la confidencialidad de la ciberseguridad debe garantizar ello. De igual modo, Luh et al. (2020), quienes en su estudio demuestran que la ciberseguridad evidencia una incidencia significativa en los problemas de privacidad de información de los pacientes clínicos, asimismo, indican que el tratamiento apropiado de la información de los

pacientes clínicos, requiere de una mayor intervención de la ciberseguridad en aras de asegurar la privacidad. Además, Ronquillo et al. (2018), quienes en su investigación confirman la influencia significativa de la ciberseguridad sobre la infraestructura de TI, asimismo señala que la ciberseguridad debe mejorarse respecto a infraestructuras de TI de salud, para ser efectivas y seguras frente a los ataques cibernéticos de ransomware, que ponen en riesgo la confidencialidad de la información.

Los resultados se relacionan con la definición de la dimensión Preservación de la Confidencialidad, la cual según Kaila et al. (2018) expresaron que la preservación de la confidencialidad es el principio que garantiza la protección de los datos, el cual debe asegurar que solo los usuarios autorizados puedan tener el acceso correspondiente a ellos. Asimismo, se relacionan con el concepto de la dimensión espacio físico, el cual según Gallastegui (2016) mencionó que es el espacio donde se encuentra al sujeto de fuente de estudio, dicho espacio se encuentra establecido físicamente y su percepción se condiciona a los sentidos humanos, cuya composición está vinculada a la correlación entre el cuerpo y el espacio mediante las actividades que el cuerpo realiza sobre esta.

En cuanto al Objetivo Específico 2; en función a los resultados alcanzados del análisis descriptivo, describen que la frecuencia más alta se da en la concurrencia del nivel óptimo de la dimensión Preservación de la Integridad de la Ciberseguridad con el nivel bueno de la dimensión Uso de las TIC del Teletrabajo, mientras que la menor frecuencia se da en la concurrencia del nivel deficiente de la dimensión Preservación de la Integridad Ciberseguridad con los niveles deficiente y bueno de la dimensión Uso de las TIC del Teletrabajo.

Además, del análisis inferencial se obtuvo como resultado un valor Pseudo R^2 de Nagelkerke de 0.656 (65.6%) el cual evidencia el grado de incidencia la dimensión Preservación de la Integridad de la Ciberseguridad en la dimensión Uso de las TIC del Teletrabajo, asimismo de la prueba de Wald en el cual se obtuvo una significancia de 0.000 el cual es menor a 0.05; por consiguiente se comprueba que existen incidencia

significativa de la dimensión Preservación de la Integridad de la Ciberseguridad en la dimensión Uso de las TIC del Teletrabajo.

Los resultados antes señalados coinciden con los conseguidos por Correa (2022), quien en su investigación evidencia la importancia de la propiedad de la preservación de la integridad de la ciberseguridad en el tratamiento de los datos personales de pacientes clínicos, ya que esta información no debe ser alterada ni manipulada por eventos intencionales, no autorizados o accidentales, con el propósito de que la información sea siempre correcta y precisa, la propiedad de la preservación de la integridad de la ciberseguridad debe asegurar ello. Así también, Pérez et al. (2020) y Arias et al. (2015), quienes en sus investigaciones concluyen que la implementación de una política de ciberseguridad combinando prácticas vinculadas a nuevas tecnologías y el empleo de un modelo internacional de ciberseguridad respectivamente, influyen en un alto grado de protección de la información virtual en las organizaciones, minimizando el riesgo destructivo de los ciberataques, de esta forma evitar que la información sea alterada.

Los resultados se relacionan con las definiciones de la dimensión Preservación de la Integridad, las cuales según Campbell (2016) mencionó que la preservación de la integridad es el principio encargado de asegurar que la información no haya sido alterada por sucesos intencionales, no autorizados o accidentales, garantizando que la información sea siempre correcta y precisa. Además, Pal et al. (2021) y Mohammadpourfard et al. (2020), señalaron que la preservación de la integridad tiene como propósito proteger y mantener intacta la información, sin que esta pueda ser cambiada a través de su transferencia por el ciberespacio; además indican que la preservación de la integridad debe asegurar que no sea posible la realización de toda acción que implique una alteración de datos no autorizada. Asimismo, se relacionan con los conceptos de la dimensión uso de las TIC, las cuales según Quiroga-Parra et al. (2017), indicaron que el uso de las TIC es la raíz principal de cambios tecnológicos en los países desarrollados, por ello es que el uso de las TIC es el nuevo insumo de información que se tiene que tener en cuenta en los procesos organizacionales, para que estas puedan lograr su progreso continuo. Así también, Peñates (2014), indicó que

las TIC son parte de un conjunto de tecnologías destinadas para almacenar, sistematizar y difundir información, donde su empleo va contribuir a la realización de tareas de las personas y de las organizaciones tanto sector público como del privado.

Concerniente al Objetivo Específico 3; de acuerdo a los resultados conseguidos del análisis descriptivo, indican que la frecuencia más alta se da en la concurrencia del nivel óptimo de la dimensión Preservación de la Disponibilidad de la Ciberseguridad con el nivel bueno de la dimensión Cambio Organizacional del Teletrabajo, mientras que la menor frecuencia se da en la concurrencia del nivel deficiente de la dimensión Preservación de la Disponibilidad de la Ciberseguridad con los niveles deficiente y bueno de la dimensión Cambio Organizacional del Teletrabajo.

Además, del análisis inferencial se obtuvo como resultado un valor Pseudo R^2 de Nagelkerke de 0.642 (64.2%) el cual evidencia el grado de incidencia la dimensión Preservación de la Disponibilidad de la Ciberseguridad en la dimensión Cambio Organizacional del Teletrabajo, asimismo de la prueba de Wald en el cual se obtuvo una significancia de 0.000 el cual es menor a 0.05; por consiguiente se comprueba que existen incidencia significativa de la dimensión Preservación de la Disponibilidad de la Ciberseguridad en la dimensión Cambio Organizacional del Teletrabajo.

Los resultados antes mencionados coinciden con los alcanzados por Ronquillo et al. (2018), quienes en su investigación evidencian la relevancia de la propiedad de la preservación de la disponibilidad de la ciberseguridad en las infraestructuras de TI de salud; puesto que se debe asegurar que la información deba obtenerse de manera oportuna cuando sea necesario, a los que solo deberán tener acceso los usuarios autorizados, la propiedad de la preservación de la disponibilidad de la ciberseguridad debe asegurar ello. Por otro lado, Suarez (2020), quien en su investigación demostró que la implementación del teletrabajo incide significativamente en la calidad de servicio, comprobándose estadísticamente por el estadístico de Spearman con un valor de 0.654, el cual determina que las variables de investigación se correlacionan significativamente, además demostró que mediante la implementación del teletrabajo

la institución logra brindar un servicio de calidad. Asimismo, Gutiérrez (2020), quien en su investigación demostró que la implementación del teletrabajo genera resultados beneficiosos respecto a la sostenibilidad empresarial en términos económicos, pues se ahorra significativamente al no utilizar las instalaciones de la empresa, ambientales, pues se evita la emisión de gases tóxicos la no tener que trasladarse al centro de labores y sociales, pues los trabajadores se sienten satisfechos al trabajar de esta modalidad ya que encuentran un equilibrio entre lo laboral y lo personal.

Los resultados se relacionan con las definiciones de la dimensión Preservación de la Disponibilidad, las cuales según De Oliveira et al. (2014), mencionaron que la preservación de la disponibilidad garantiza que el acceso a la información debe ser oportuno y cuando sea necesario; de igual forma mencionaron que tal propiedad debe estar presente en todos los activos de información, a los que solo accederán el personal autorizado. Además, Najmi et al. (2021), indicaron que la preservación de la disponibilidad desde la visión de la ciberseguridad se logra al poder tener el acceso completo, necesario y formalmente acreditado a los sistemas y servicios dentro del ciberespacio. Asimismo, se relacionan con el concepto de la dimensión cambio organizacional, el cual según Aujla et al. (2020) indicaron que es la inserción de nuevas ideas o procesos en una organización, ya sean de origen interno o externo, por medio de mejoras estructurales y de capacidad, como resultado de arreglos en la organización de la dirección del proceso o de la capacidad de asimilación frente circunstancias imprevistas.

De acuerdo a la metodología recurrida para esta investigación, se fortalece al ser de tipo básica, pues esta permite dar sustento teórico a la realidad problemática estudiada, mediante la recopilación y análisis de diversas bases teóricas para asegurar el entendimiento de las variables en estudio, así como de sus respectivas dimensiones. Además, al ser de diseño no experimental de tipo transversal de nivel correlacional causal, su importancia reside en que las variables en estudio y su interacción se analizan en su medio natural, en un momento determinado y sin alguna manipulación sobre ellas; determinando la relación causal de las variables en estudio, sin la

necesidad de elaborar un pre y post prueba. En ese sentido se realizó la recopilación de datos recurriendo a la técnica de la encuesta, por intermedio del cuestionario como instrumento, el cual se aplicó de manera virtual como alternativa ante el actual contexto de pandemia; el cual ha sido de gran apoyo para la investigación, brindando a los encuestados la facilidad de poder realizarla sin importar el lugar, día y hora. Sin embargo, una debilidad presentada en este tipo de técnica radica en las respuestas obtenidas por el encuestado, ya que estas pueden estar influenciadas por el estado de ánimo del encuestado, grado de involucramiento con la investigación, conocimiento del tema entre otros. Así también es relevante indicar que los objetivos planteados y justificados en esta investigación, proporcionaron a la entidad pública conocer mejor la realidad relacional entre la Ciberseguridad y el Teletrabajo, en tal sentido esta investigación aportar científicamente en la comprensión de la variable tecnológica y social respectivamente.

Por otro lado, sobre el análisis inferencial sustentado principalmente en el coeficiente Pseudo R^2 de Nagelkerke por ser el más completo que Cox y Snell y McFadden; el cual sustenta el grado de incidencia entre las variables y sus respectivas dimensiones, el cual, al ser más cercano a uno representará mayor incidencia; asimismo se utilizó la RLO para determinar el contraste de hipótesis, fundamentando que un valor de estimación positivo demuestra una relación directa entre las variables y un valor de significancia menor a 0.05 demuestra la veracidad de la hipótesis del investigador.

VI. CONCLUSIONES

Primera Tomando en cuenta los resultados conseguidos, se determina que la Ciberseguridad incide significativamente en el Teletrabajo de una entidad pública, Lima 2022. En ese sentido se corrobora esta hipótesis, pues se obtuvo un valor de significancia igual a 0.000 en la prueba de Wald, certificando que se percibe una incidencia significativa entre las variables. De la misma forma, se obtuvo el valor de R^2 de Nagelkerke igual a 0.764 el cual representa un 76.4% de incidencia entre las variables. Además, descriptivamente se pudo determinar que el 43.5% de los encuestados considera que el Teletrabajo posee un nivel bueno con una incidencia óptima de la Ciberseguridad.

Segunda De acuerdo a los resultados conseguidos, se determina que la dimensión Preservación de la Confidencialidad de la Ciberseguridad incide significativamente en la dimensión Espacio Físico del Teletrabajo de una entidad pública, Lima 2022. En ese sentido se corrobora esta hipótesis, pues se obtuvo un valor de significancia igual a 0.000 en la prueba de Wald, certificando que se percibe una incidencia significativa entre las variables. De la misma forma, se obtuvo el valor de R^2 de Nagelkerke igual a 0.729 el cual representa un 72.9% de incidencia entre las variables. De igual importancia, descriptivamente se pudo determinar que el 40.7% de los encuestados considera que la dimensión Espacio Físico del Teletrabajo posee un nivel bueno con una incidencia óptima de la dimensión Preservación de la Confidencialidad de la Ciberseguridad.

Tercera En cuanto a los resultados conseguidos, se determina que la dimensión Preservación de la Integridad de la Ciberseguridad incide significativamente en la dimensión Uso de las TIC del Teletrabajo de una entidad pública, Lima 2022. En ese sentido se corrobora esta hipótesis,

pues se obtuvo un valor de significancia igual a 0.000 en la prueba de Wald, certificando que se percibe una incidencia significativa entre las variables. De la misma forma, se obtuvo el valor de R^2 de Nagelkerke igual a 0.656 el cual representa un 65.6% de incidencia entre las variables. De igual importancia, descriptivamente se pudo determinar que el 38.9% de los encuestados considera que la dimensión Uso de las TIC del Teletrabajo posee un nivel bueno con una incidencia óptima de la dimensión Preservación de la Integridad de la Ciberseguridad.

Cuarta Con relación a los resultados conseguidos, se determina que la dimensión Preservación de la Disponibilidad de la Ciberseguridad incide significativamente en la dimensión Cambio Organizacional del Teletrabajo de una entidad pública, Lima 2022. En ese sentido se corrobora esta hipótesis, pues se obtuvo un valor de significancia igual a 0.000 en la prueba de Wald, certificando que se percibe una incidencia significativa entre las variables. De la misma forma, se obtuvo el valor de R^2 de Nagelkerke igual a 0.642 el cual representa un 64.2% de incidencia entre las variables. De igual importancia, descriptivamente se pudo determinar que el 38.9% de los encuestados considera que la dimensión Cambio Organizacional del Teletrabajo posee un nivel bueno con una incidencia óptima de la dimensión Preservación de la Disponibilidad de la Ciberseguridad.

VII. RECOMENDACIONES

Primera Tomando en cuenta los resultados demostrados de análisis estadístico y con la finalidad de conservar y aumentar el grado en que incide positivamente la Ciberseguridad sobre el Teletrabajo, se recomienda al Gerente General en coordinación con el Gerente de tecnología, la implementación de buenas prácticas establecidas en un marco de trabajo ya comprobado en el campo de la Ciberseguridad, como el Framework NIST; con el propósito de poder asegurar el correcto funcionamiento del Teletrabajo, para evitar los diversos ataques cibernéticos o actuar de manera oportuna cuando estos se presenten.

Segunda Tomando en cuenta los resultados demostrados de análisis estadístico y con el propósito de conservar y aumentar el grado en que incide positivamente la dimensión Preservación de la Confidencialidad de la Ciberseguridad sobre la dimensión Espacio Físico del Teletrabajo, se recomienda al Gerente General en coordinación con el Gerente de tecnología y de recursos humanos, establecer planes de capacitación evaluadas para los trabajadores de la entidad, en temas relacionados a la confidencialidad de la información; con el fin de salvaguardar toda información que hagan uso los trabajadores en el proceso del Teletrabajo. De igual importancia, monitorear constantemente los controles de acceso en los ambientes que se ejerza el Teletrabajo.

Tercera Tomando en cuenta los resultados demostrados de análisis estadístico y con el propósito de conservar y aumentar el grado en que incide positivamente la dimensión Preservación de la Integridad de la Ciberseguridad sobre la dimensión Uso de las TIC del Teletrabajo, se recomienda al Gerente de tecnología, establecer un plan de evaluación y mejora de los controles y mecanismos tecnológicos que soportan la

integridad de información; con el propósito de proteger y mantener intacta la información, sin que esta pueda ser alterada a través de su flujo en el Teletrabajo.

Cuarta Tomando en cuenta los resultados demostrados de análisis estadístico y con el propósito de conservar y aumentar el grado en que incide positivamente la dimensión Preservación de la Disponibilidad de la Ciberseguridad sobre la dimensión Cambio Organizacional del Teletrabajo, se recomienda al Gerente de tecnología, establecer un plan de implementación y evaluación de tecnologías alternativas que garanticen el correcto funcionamiento del Teletrabajo.

REFERENCIAS

Ameziane, A., Abou, A., Bouhoula, A., Abassi, R. y Ait, A. (2015). Integrity-OrBAC: A new model to preserve critical infrastructures integrity. International Journal of Information Security, 14(4), 367-385. https://doi.org/10.1007/s10207-014-0254-9.

Argyropoulos, N., Mouratidis, H. y Fish, A. (2019). Enhancing secure business process design with security process patterns. Software and Systems Modeling, 1-23. http://dx.doi.org/10.1007/s10270-019-00743-y.

Arias, N. y Celis, J. (2015). Modelo experimental de ciberseguridad y ciberdefensa para Colombia. Facultad de Ingeniería. Universidad Libre. Colombia. https://repository.unilibre.edu.co/handle/10901/10904.

Aujla, S. y Mclarney, C. (2020). The Effects of Organizational Change on Employee Commitment. IUP Journal of Organizational Behavior, 19(1), 7-22. ISSN 0972-687X.

Becerril, A. (2019). La ciberseguridad en los Tratados de Libre Comercio: The cybersecurity in free trade agreements. Revista chilena de derecho y tecnología, 8(2), 111-137. https://doi.org/10.5354/0719-2584.2019.53447.

Behar, D. (2008). Introducción a la metodología de la investigación. (1era ed.). Bogotá, Colombia: Editorial Shalom. ISBN 978-959-212-783-7.

Belzunegui-Eraso, A. y Erro-Garcés, A. (2020). Teleworking in the Context of the Covid-19 Crisis. Sustainability, 12(9), 3662. MDPI AG. https://doi.org/10.3390/su12093662.

Bohorquez, A. (2021). Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. Escuela de Posgrado. Universidad César Vallejo. Perú. 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.

Broks, A. (2016). Systems theory of systems thinking: General and particular within modern science and technology education. Journal of Baltic Science Education, 15(4), 408-410. https://doi.org/10.33225/jbse/16.15.408.

Campbell T. (2016). Practical Information Security Management: A Complete Guide to Planning and Implementation. Burns Beach, Australia: Editorial Apress. ISBN: 978-1-4842-1684-2. https://dut.edu.ua/uploads/l_1888_50813661.pdf.

Carter, M., Petter, S., Grover, V. y Thatcher, J. (2020). Information Technology Identity: A Key Determinant of It Feature and Exploratory Usage. MIS Quarterly, 44(3), 983–1021. ISSN: 0276-7783. https://cpb-us-e1.wpmucdn.com/wordpressua.uark.edu/dist/f/860/files/2017/05/2020-MISQ1-2.pdf.

Choejey, P., Murray, D. y Che, Ch. (2017). Perceptions of Cybersecurity in Government Organizations: Case Study of Bhutan. World Academy of Science, Engineering and Technology, Open Science Index 121, International Journal of Computer and Information Engineering, 11(1), 152-155. https://publications.waset.org/10007724/perceptions-of-cybersecurity-in-government-organizations-case-study-of-bhutan.

Contreras, F., Castillo, J. y Uriguen, S. (2016). ¿Qué hay de nuevo en la Teoría de Agencia (TA)? algunos trabajos teóricos y empíricos aplicados a las organizaciones/What's new in the agency theory (AT)? some theoretical and empirical work applied to organizations. Prisma Social, (15), 685-707. https://www.proquest.com/docview/1759176527.

Correa, M. (2022). Ciberseguridad y su incidencia en el Tratamiento de Datos Personales en una Municipalidad Distrital de Lima Sur, 2021. Escuela de Posgrado. Universidad César Vallejo. Perú. https://hdl.handle.net/20.500.12692/85975.

Culqui, A. y González, A. (2016). El Teletrabajo: Una Innovadora Forma de Organización del Trabajo, una Herramienta de Inclusión Laboral y su Regulación Jurídica en el Perú. Derecho & Sociedad, 46, 95-109. https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/18823.

De la Peña, G. y Velázquez, R. (2018). Algunas reflexiones sobre la teoría general de sistemas y el enfoque sistémico en las investigaciones científicas: Some reflections about General Theory of Systems and Systemic Approach in scientific research. Revista Cubana de Educación Superior, 37(2), 31–44. http://www.rces.uh.cu/index.php/RCES/article/view/211/254.

De Oliveira, R., García, L., Sandoval, A., Buiati, F. y Tai-Hoon, K. (2014). A layered trust information security architecture. Sensors, 14(12), 22754–22772. https://doi.org/10.3390/s141222754.

Duque, J. (2014). Los procesos de cambio organizacional y la generación de valor/Organizational change processes and value creation/Os processos de mudança organizacional e a criação de valor. Estudios Gerenciales, 30(131), 162-171. https://doi.org/10.1016/j.estger.2014.04.005.

Eset Latinoamérica (2021). Eset Security Report Latinoamérica 2021. https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf.

Eurofound (2017). Working anytime, anywhere: The effects on the world of work, Publications Office of the European Union, Luxembourg, and the International Labour Office, Geneva. https://data.europa.eu/doi/10.2806/372726.

Faik, I., Barrett, M. y Oborn, E. (2020). How Information Technology Matters in Societal Change: An Affordance-Based Institutional Logics Perspective. MIS Quarterly, 44(3), 1359-1390. http://www.xwcbx.cn/zb_users/upload/2021/04/20210428161956793631294 8.pdf.

Fava, S. (2020). Adriano Olivetti's notion of "Community": transforming the factory and urban physical space into educational space. Ricerche di Pedagogia e Didattica. Journal of Theories and Research in Education, 15(1), 203-216. https://doi.org/10.6092/issn.1970-2221/10475.

Fortinet (2022). América Latina sufrió más de 289 mil millones de intentos de ciberataques en 2021. https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-reporte-ciberataques-america-latina-2021.

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://doi.org/10.1016/j.clsr.2021.105528.

Gallastegui, S. (2016). Between Immersion and Emersion: Orientating Digital Games Towards Virtual and Physical Spaces. IADIS International Journal on Computer Science & Information Systems, 11(1), 49–62. http://www.iadisportal.org/ijcsis/papers/2016190104.pdf.

Golden, T. y Gajendran, R. (2019). Unpacking the Role of a Telecommuter's Job in Their Performance: Examining Job Complexity, Problem Solving, Interdependence and Social Support. Journal of Business and Psychology, 34:55–69. https://doi.org/10.1007/s10869-018-9530-4.

Goucher, W. (2016). Information Security Auditor: Careers in Information Security. Swindon, United Kingdom. BCS, The Chartered Institute for IT. ISBNs: 9781780172163. 9781780172170. 9781780172187.

Gutiérrez, P. (2020). El teletrabajo como estrategia empresarial sostenible en una empresa de servicios de consultoría. Iberian Journal of Information System and Technologies. Revista Ibérica de Sistemas e Tecnologias de Informação, 31, 390-403. https://hdl.handle.net/20.500.12867/3077.

Heredia, J., Rodríguez, A., y Vilalta, J. (2014). Predicción del rendimiento en una asignatura empleando la regresión logística ordinal. Estudios pedagógicos (Valdivia), 40(1), 145-162. La Habana, Cuba.n ISSN 0718-0705. http://dx.doi.org/10.4067/S0718-07052014000100009.

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

Inoguchi, A. y Macha, E. (2017). Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las Pymes del Perú, 2016. Facultad de Ingeniería. Universidad San Ignacio de Loyola. Perú. http://repositorio.usil.edu.pe/handle/USIL/2810.

ISO 27032 (2012). ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. SecAware. https://www.iso27001security.com/html/27032.html.

Joaquim, O., de Lacerda, R. y João, B. (2017). Agency Theory: A study about scientific research in brazilian journals. Revista de Gestão, Finanças e Contabilidade, 7(3), 379-396. https://revistas.uneb.br/index.php/financ/article/view/3789/2450.

Juárez, P., Cañedo, R., Barragán, M. del C., y Juárez, O. (2016). Un modelo de regresión logística ordinal para la determinación de los principales factores que influyen en la percepción de la calidad de vida en dos comunidades de Acapulco, Guerrero. Denarius. Revista de economía y administración 1(30), 171 - 200. https://denarius.izt.uam.mx/index.php/denarius/article/view/53.

Kaila, U. y Nyman, L. (2018). Information Security Best Practices: First Steps for Startups and SMEs. Technology Innovation Management Review, 8(11), 32–42. https://doi.org/10.22215/timreview/1198.

Kilovaty, I. (2020). Availability's Law. Tennessee Law Review, 88, 69-115. Publicado por SSRN. https://papers.ssrn.com/abstract=3568790.

Kühl, S. (2013). Organizations: A Systems Approach. Farnham, Surrey: Routledge. Dorchester, United Kingdom: Published by Gower Publishing Company. ISBN 9781472413413.

Ley Nº 31250 (2021). Ley del Sistema Nacional de Ciencia, Tecnología e Innovación. Normas Legales N.º 16096. Diario Oficial El Peruano. https://busquedas.elperuano.pe/normaslegales/ley-del-sistema-nacional-de-ciencia-tecnologia-e-innovacion-ley-n-31250-1968664-1/.

Llamosas, A. (2015). Relaciones laborales y nuevas tecnologías de la información y de la comunicación. Una relación fructífera no exenta de dificultades. Madrid: Dykinson, S.L. ISBN: 978-84-9085-533-1. https://www.dykinson.com/cart/download/ebooks/7981/.

Luh, F. y Yen, Y. (2020). Cybersecurity in Science and Medicine: Threats and Challenges. Trends in Biotechnology, 38(8), 825-828. https://doi.org/10.1016/j.tibtech.2020.02.010.

Maldonado, C. (2017). Ciencia hecha realidad. Reseña de C. A. Ossa, Teoría general de sistemas. Conceptos y aplicaciones. INNOVAR. Revista de Ciencias Administrativas y Sociales, 27(64), 157-159. https://www.redalyc.org/articulo.oa?id=81850404014.

Mohammadpourfard, M., Weng, Y., Pechenizkiy, M., Tajdinian, M. y MohammadIvatloo, 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.

MTPE (2020-A). Boletín Mensual Leyendo Números JUNIO 2020. Ministerio de Trabajo y Promoción del Empleo. Perú. https://www.gob.pe/institucion/mtpe/informes-publicaciones/1002404 %20boletin-mensual-leyendo-numeros-junio-2020.

MTPE (2020-B). Boletín Mensual Leyendo Números JULIO 2020. Ministerio de Trabajo y Promoción del Empleo. Perú. https://www.gob.pe/institucion/mtpe/informes-publicaciones/1129996-boletin-mensual-leyendo-numeros-julio-2020.

Najmi, Y., AlZain, M., Masud, M., Jhanjhi, N., 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.

Ñeco, L., Baños, M., Bernal, I., Gonda, C., Guilló A., Amatriain, M., Leal, A., Martínez, L., Merafina, M., Pina, R., Valenciano, G. y Santamaría, S. (2018). Teorías sistémicas y paradigma de investigación performativa en los estudios superiores de danza. Guanajuato, México: El Artista, (15). https://www.redalyc.org/articulo.oa?id=87457958009.

OIT (2020). El teletrabajo durante la pandemia de COVID-19 y después de ella – Guía práctica. Ginebra: Oficina Internacional del Trabajo. ISBN: 978-92-2-033092-0 (impreso). ISBN: 978-92-2-033091-3 (PDF web). https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_758007.pdf.

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://www.cse.iitk.ac.in/users/amitangshu/Prekeying.pdf.

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, 64, 729-734. https://doi.org/10.1016/j.bushor.2021.07.010.

Peñates, V. (2014). Impacto del uso de las tecnologías de la información y la comunicación que apoyan la cadena de suministro (TICCS) sobre el desempeño organizacional. Bogotá, Colombia: Universidad & Empresa, 16(27), 111–144. https://www.redalyc.org/articulo.oa?id=187241606005.

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

Pinto-Fernández, S., Muñoz-Sepúlveda, M. y Leiva-Caro, J. (2018). Uso de tecnologías de información y comunicación en adultos mayores chilenos. Buenos Aires, Argentina: Revista Iberoamericana de Ciencia, Tecnologia y Sociedad, 13(39), 143-160. https://www.redalyc.org/journal/924/92457957007/92457957007.pdf.

Quiroga-Parra, D., Torrent-Sellens, J. y Murcia, C. (2017). Usos de las TIC en América Latina: una caracterización. Ingeniare. Revista Chilena de Ingeniería, 25(2), 289–305. https://dx.doi.org/10.4067/S0718-33052017000200289.

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.

Ríos, R. (2017). Metodología para la investigación y redacción. Málaga, España: Editorial Servicios Académicos Intercontinentales SL. ISBN-13:978-84-17211-23-3.

Ronquillo, J., Erik, J., Cwikla, K., Szymanski, R. y Levy, C. (2018). Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. JAMIA open, 1(1), 15-19. https://doi.org/10.1093/jamiaopen/ooy019.

RPP (2020) Anonymous hizo caer las páginas web del Congreso y varios sitios del gobierno. https://rpp.pe/tecnologia/redes-sociales/anonymous-paginas-web-del-congreso-y-varios-sitios-del-gobierno-se-restablecen-tras-caida-noticia-1304238.

Saiyadain, M. y Ali, S. (2017). Managing Organization. (1era ed.). Delhi, India: Editorial Trinity Press. Laxmi Publications Pvt Ltd. ISBN: 978-93-86202-07-9.

Sánchez, H., Reyes, C. y Mejia K. (2018). Manual de términos en investigación científica, tecnológica y humanística. (1era ed.). Lima, Perú: Editorial Universidad Ricardo Palma. ISBN 978-612-47351-4-1.

Sánchez, J. (2017). Adopción de estrategias de ciberseguridad en la protección de la información en la oficina de economía del ejército, San Borja-2017. Escuela de Posgrado. Instituto científico tecnológico del ejército. Perú. http://repositorio.icte.ejercito.mil.pe/handle/123456789/201.

Seyal, A. y Mohd, A. (2017). Theory of Planned Behavior: New Research. New York, United States: Editorial Nova Science Publishers, Inc. ISBN: 9781536113105.

Suarez, L. (2020). Implementación del teletrabajo y calidad de servicio de la unidad de gestión educativa local San Pablo, 2020. Escuela de Posgrado. Universidad César Vallejo. Perú. https://hdl.handle.net/20.500.12692/46386.

Tuapanta, J., Duque, M., y Mena, A. (2017). Alfa de Cronbach para validar un cuestionario de uso de TIC en Docentes Universitarios. Revista mktDescrubre, 1(10), 37 - 48. ISSN 2602-8522. https://doi.org/10.36779/mktdescubre.v10.141.

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.

Ural, S. (2019). Solipsism, Physical Things and Personal Perceptual Space: Solipsist Ontology, Epistemology and Communication. Istanbul, Turkey: Editorial Vernon Press. ISBN: 9781622735624.

Vacca, J. (2017). Computer and Information Security Handbook (3era ed.). Cambridge, United States: Editorial Morgan Kaufmann. 2017(11), 4. https://doi.org/10.1016/S1353-4858(17)30090-9.

Valverde, A., Bardales, L., y Solis, B. (2022). Modelo Logístico Ordinal de los Factores Asociados al Nivel de Uso de Recursos Digitales en Docentes Universitarios en el Contexto de la COVID-19. Memorias de la Décima Segunda Conferencia Iberoamericana de Complejidad, Informática y Cibernética: CICIC 2022, pp. 74-78 (2022); https://doi.org/10.54808/CICIC2022.01.74

Wessels, M., van den Brink, P., Verburgh, T., Cadet, B. y Van, T. (2021). Understanding incentives for cybersecurity investments: Development and application of a typology. Digital Business, 1(2), 100014. http://dx.doi.org/10.1016/j.digbus.2021.100014.

Wright, C. (2016). Fundamentals of Information Security Risk Management Auditing: An introduction for managers and auditors. Cambridgeshire, United Kingdom: Published by IT Governance Publishing. ISBN: 9781849288170.

Zhang, X. y Yang, H. (2018). Impact of Cross-Culture on Behavioral Information Security. Journal of Integrated Design & Process Science, 22(2), 63–80. https://doi.org/10.3233/jid-2018-0003.

ANEXOS

Anexo 1: Matriz de Consistencia

TÍTULO: Ciberseguridad y su incidencia en el Teletrabajo en una entidad pública, Lima 2022

AUTOR: Marin Puris, Luis Enrique

PROBLEMA	OBJETIVOS	HIPÓTESIS
Problema principal: ¿De qué manera la Ciberseguridad incide en el Teletrabajo en una entidad pública, Lima 2022? **Problemas específicos:** PE1: ¿De qué manera la dimensión preservación de la confidencialidad de la Ciberseguridad incide en la dimensión espacio físico del Teletrabajo en una entidad pública, Lima 2022? PE2: ¿De qué manera la dimensión preservación de la integridad de la Ciberseguridad incide en la dimensión uso de las	**Objetivo principal:** Determinar la incidencia de la Ciberseguridad en el Teletrabajo de una entidad pública, Lima 2022. **Objetivos específicos:** OE1: Determinar la incidencia de la dimensión preservación de la confidencialidad de la Ciberseguridad en la dimensión espacio físico del Teletrabajo en una entidad pública, Lima 2022. OE2: Determinar la incidencia de la dimensión preservación de la integridad de la Ciberseguridad en la	**Hipótesis principal:** La Ciberseguridad incide significativamente en el Teletrabajo de una entidad pública, Lima 2022. **Hipótesis específicas:** HE1: La dimensión preservación de la confidencialidad de la Ciberseguridad incide significativamente en la dimensión espacio físico del Teletrabajo de una entidad pública, Lima 2022. HE2: La dimensión preservación de la integridad de la Ciberseguridad incide significativamente en la

VARIABLES E INDICADORES

Variable - 1: Ciberseguridad

Dimensiones	Indicadores	Ítems	Niveles
Preservación de la confidencialidad	Control	1,2	Óptimo [68-90] Regular [43-67] Deficiente [18-42]
	Autorización	3,4	
	Protección	5,6	
Preservación de la integridad	Precisión	7,8	
	Fiabilidad	9,10	
	Seguridad	11,12	
Preservación de la disponibilidad	Accesibilidad	13,14	
	Tiempo	15,16	
	Seguridad	17,18	

Variable - 2: Teletrabajo

Dimensiones	Indicadores	Ítems	Niveles
Espacio Físico	Accesibilidad	19,20	

TÍTULO: Ciberseguridad y su incidencia en el Teletrabajo en una entidad pública, Lima 2022

AUTOR: Marin Puris, Luis Enrique

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
TIC del Teletrabajo en una entidad pública, Lima 2022? PE3: ¿De qué manera la dimensión preservación de la disponibilidad de la Ciberseguridad incide en la dimensión cambio organizacional del Teletrabajo en una entidad pública, Lima 2022?	dimensión uso de las TIC del Teletrabajo en una entidad pública, Lima 2022. OE3: Determinar la incidencia de la dimensión preservación de la disponibilidad de la Ciberseguridad en la dimensión cambio organizacional del Teletrabajo en una entidad pública, Lima 2022.	dimensión uso de las TIC del Teletrabajo de una entidad pública, Lima 2022. HE3: La dimensión preservación de la disponibilidad de la Ciberseguridad incide significativamente en la dimensión cambio organizacional del Teletrabajo de una entidad pública, Lima 2022.		Seguridad	21,22	Óptimo [68-90]
				Controles	23,24	
			Uso de las TIC	Conocimiento	25,26	Regular [43-67]
				Disponibilidad	27,28	
				Seguridad	29,30	
			Cambio organizacional	Metas	31,32	Deficiente [18-42]
				Controles	33,34	
				Documentación	35,36	

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Investigación Básica **Diseño:** No experimental de tipo Transversal de nivel Correlacional causal	**Población:** 150 trabajadores de la entidad pública. **Tamaño de muestra:** 108 trabajadores de la entidad pública. **Muestreo:** muestreo probabilístico aleatorio simple.	**Técnicas:** Encuesta **Instrumentos:** Cuestionario	**Descriptiva:** Para el análisis descriptivo se utilizarán tablas de contingencia o también llamadas tablas cruzadas, apoyándose para la interpretación de los datos a través de tablas e histogramas. **Inferencial:** Para el análisis inferencial se aplicará la regresión logística ordinal, para demostrar el grado de correlación casual existente de la variable independiente sobre la variable dependiente.

Anexo 2: Matriz de Operacionalización de Variables

TÍTULO: Ciberseguridad y su incidencia en el Teletrabajo en una entidad pública, Lima 2022

AUTOR: Marin Puris, Luis Enrique

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Ciberseguridad: Según la norma ISO/IEC 27032 (2012), menciona que la ciberseguridad se fundamenta en la preservación de la confidencialidad, integridad y disponibilidad de toda información almacenada en computadores y sistemas de redes digitales y transmisión a gran magnitud a nivel global, denominado ciberespacio.	**Preservación de la confidencialidad:** Según Kaila y Nyman (2018) expresan que la preservación de la confidencialidad es el principio encargado de garantizar la protección de los datos, con la finalidad de que solo los usuarios autorizados puedan acceder a ellos.	Control	1	¿Considera usted que las políticas de ciberseguridad garantizan el acceso autorizado a los sistemas?	Óptimo [68-90] Regular [43-67] Deficiente [18-42]
			2	¿Considera usted que los métodos para establecer contraseñas seguras son los más adecuados?	
		Autorización	3	¿Considera usted que solo el personal autorizado debe acceder a los sistemas, base de datos e información digital de la institución?	
			4	¿Considera usted que los mecanismos de autorización son los adecuados frente a alguna amenaza informática?	
		Protección	5	¿Considera usted que se deben realizar copias de seguridad periódicamente?	
			6	¿Cree usted que se ha perdido información importante debido a algún ataque informático?	
	Preservación de la integridad: Según Mohammadpourfard et al. (2020) y Pal et al. (2021) señalaron que la preservación de la integridad tiene como finalidad proteger y mantener intacta la información, sin que esta pueda ser alterada a través de su flujo en el ciberespacio; además recalcan que la preservación de la integridad debe garantizar imposibilitar toda forma de alteración de datos no autorizada.	Precisión	7	¿Considera usted que la información que proporciona los sistemas y bases de datos es precisa?	
			8	¿La información contenida en los sistemas y base de datos se mantiene precisa a través del tiempo?	
		Fiabilidad	9	¿Los métodos aplicados para que la información permanezca completa en la base de datos cumplen su función?	
			10	¿Alguna vez los sistemas han fallado al grabar información o han mostrado datos errados al ser consultados?	
		Seguridad	11	¿Los procedimientos para realizar una modificación en los sistemas y base de datos son adecuados?	
			12	¿Considera usted imposible realizar una modificación de datos no autorizada en los sistemas?	

TÍTULO: Ciberseguridad y su incidencia en el Teletrabajo en una entidad pública, Lima 2022

AUTOR: Marin Puris, Luis Enrique

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Preservación de la disponibilidad: Según Najmi et al. (2021) indicaron que la preservación de la disponibilidad desde el punto de vista de la ciberseguridad se consigue al garantizar obtener el acceso completo, necesario y formalmente autorizado a los sistemas y servicios contenidos en el ciberespacio.	Accesibilidad	13	¿Los mecanismos de acceso son adecuados frente a las amenazas de ciberseguridad en el teletrabajo?	Óptimo [68-90] Regular [43-67] Deficiente [18-42]
			14	¿Los mecanismos de acceso garantizan que solo el personal autorizado pueda hacer uso de los sistemas y base de datos?	
		Tiempo	15	¿Considera usted que las consultas en los sistemas de información demoran en responder?	
			16	¿Los sistemas y bases de datos demoran en restablecerse luego de un incidente informático?	
		Seguridad	17	¿Considera usted que la conexión VPN está totalmente protegida para la realización del teletrabajo?	
			18	¿Alguna vez tuvo que detener sus labores por causa de algún ataque informático?	
Teletrabajo: Según LLamosas (2015), manifiesta que el teletrabajo es la manera de realizar la labor profesional desde un lugar diferente de la institución, y está compuesta por elementos como el	**Espacio Físico:** Según Gallastegui (2016) menciona que es el espacio donde se ubica el sujeto en fuente de estudio, dicho espacio está delimitado físicamente y la percepción de esta condicionada a los sentidos humanos, cuya composición está vinculada a la relación entre el cuerpo y el espacio mediante las accesiones que el cuerpo realiza sobre esta.	Accesibilidad	19	¿Los medios de ingreso y salida a su centro de teletrabajo son adecuados?	Óptimo [68-90] Regular [43-67] Deficiente [18-42]
			20	¿Cuenta con más de un medio de ingreso o salida a su centro de teletrabajo?	
		Seguridad	21	¿Cree usted que su centro de teletrabajo es totalmente seguro para que pueda realizar sus labores?	
			22	¿Su centro de teletrabajo cuenta con mecanismos que resguarden su información y la de su empresa?	
		Controles	23	¿Cuenta con controles de acceso a su centro de teletrabajo?	
			24	¿Considera usted que los controles de acceso a su centro de teletrabajo son adecuados?	

TÍTULO: Ciberseguridad y su incidencia en el Teletrabajo en una entidad pública, Lima 2022

AUTOR: Marin Puris, Luis Enrique

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
espacio físico, el uso de las TIC y el cambio organizacional.	**Uso de las TIC:** Según Pinto-Fernández et al. (2018) manifestaron que el uso de las TIC es una parte importante de las habilidades esenciales de las personas, la cual hoy en día es una característica necesaria para formar una población más cualificada.	Conocimiento	25	¿Conoce el manejo de los sistemas utilizados en el teletrabajo?	Óptimo [68-90] Regular [43-67] Deficiente [18-42]
			26	¿Se capacita frecuentemente al personal sobre el manejo de los sistemas de la empresa?	
		Disponibilidad	27	¿Los sistemas de la empresa se encuentran operativos cuando se les requiere?	
			28	¿El servicio de internet presenta caídas frecuentemente?	
		Seguridad	29	¿Considera usted que las herramientas tecnológicas utilizadas son las más adecuadas?	
			30	¿Se cuenta con herramientas tecnológicas que protejan la realización de sus labores en teletrabajo?	
	Cambio Organizacional: Según Kühl (2013) indica que las organizaciones en la sociedad actual utilizan sus características, las cuales son establecidas por cualquier organización, ya sea empresarial o de la gestión pública, para enfocarse en metas que conlleven al bienestar de todos sus integrantes.	Metas	31	¿Las metas de la institución están enfocadas al cambio adecuado respecto al teletrabajo?	
			32	¿Se establecen objetivos a corto plazo que permitan alcanzar las metas organizacionales?	
		Controles	33	¿Existen controles que permitan asegurar el cambio de manera efectiva?	
			34	¿Se realiza un monitoreo frecuente de los controles establecidos para el cambio?	
		Documentación	35	¿Considera usted que el cambio se encuentra adecuadamente documentado en la institución?	
			36	¿Se comunica los planes y beneficios del cambio organizacional a todo el personal?	

Anexo 3: Instrumento de Recolección de Datos

Cuestionario para los trabajadores de la entidad pública

Fecha: [/ /]
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**: (1) Muy en desacuerdo, (2) En desacuerdo, (3) Ni de acuerdo, ni en desacuerdo, (4) De acuerdo, (5) Muy de acuerdo

Nº	Pregunta	Valoración				
		1	2	3	4	5
	Sobre ciberseguridad					
1	¿Considera usted que las políticas de ciberseguridad garantizan el acceso autorizado a los sistemas?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
2	¿Considera usted que los métodos para establecer contraseñas seguras son los más adecuados?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
3	¿Considera usted que solo el personal autorizado debe acceder a los sistemas, base de datos e información digital de la institución?	Muy en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Muy de acuerdo
4	¿Considera usted que los mecanismos de autorización son los adecuados frente a alguna amenaza informática?	Muy inadecuados	Algo inadecuados	Ni adecuados, ni inadecuados	Algo adecuados	Muy adecuados
5	¿Considera usted que se deben realizar copias de seguridad periódicamente?	Muy en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Muy de acuerdo
6	¿Cree usted que se ha perdido información importante debido a algún ataque informático?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
7	¿Considera usted que la información que se recibe en las bases de datos es exacta?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
8	¿Considera usted que la información contenida en los sistemas y base de datos se mantiene exacta a través del tiempo?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
9	¿Considera usted que los mecanismos para que la información permanezca completa en la base de datos son adecuados?	Muy inadecuados	Algo inadecuados	Ni adecuados, ni inadecuados	Algo adecuados	Muy adecuados
10	¿Considera usted que la información contenida en los sistemas y base de datos debe continuar completa a través del tiempo?	Muy en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Muy de acuerdo
11	¿Los mecanismos de modificación en los sistemas y base de datos son adecuados?	Muy inadecuados	Algo inadecuados	Ni adecuados, ni inadecuados	Algo adecuados	Muy adecuados
12	¿Considera usted imposible realizar una modificación de datos no autorizada en los sistemas?	Posible	Casi posible	Ni posible, ni imposible	Casi imposible	Imposible
13	¿Los mecanismos de acceso son adecuados frente a las amenazas de ciberseguridad en el teletrabajo?	Muy inadecuados	Algo inadecuados	Ni adecuados, ni inadecuados	Algo adecuados	Muy adecuados
14	¿Los mecanismos de acceso garantizan que solo el personal autorizado pueda hacer uso de los sistemas y base de datos?	Muy en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Muy de acuerdo
15	¿Considera usted que las consultas en los sistemas de información demoran en responder?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
16	¿Los sistemas y bases de datos demoran en restablecerse luego de un incidente informático?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
17	¿Considera usted que la conexión VPN está totalmente protegida para la realización del teletrabajo?	Nada	Casi nada	A veces	Parcialmente	Totalmente
18	¿Alguna vez tuvo que detener sus labores por causa de algún ataque informático?	Nunca	Casi nunca	A veces	Casi siempre	Siempre

Nº	Pregunta	Valoración				
		1	2	3	4	5
	Sobre teletrabajo					
19	¿Los medios de ingreso y salida a su centro de teletrabajo son adecuados?	Muy inadecuados	Algo inadecuados	Ni adecuados, ni inadecuados	Algo adecuados	Muy adecuados
20	¿Cuenta con más de un medio de ingreso o salida a su centro de teletrabajo?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
21	¿Cree usted que su centro de teletrabajo es totalmente seguro para que pueda realizar sus labores?	Muy inseguro	Algo inseguro	Ni seguro, ni inseguro	Algo seguro	Muy seguro
22	¿Su centro de teletrabajo cuenta con mecanismos que resguarden su información y la de su empresa?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
23	¿Cuenta con controles de acceso a su centro de teletrabajo?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
24	¿Considera usted que los controles de acceso a su centro de teletrabajo son adecuados?	Muy inadecuados	Algo inadecuados	Ni adecuados, ni inadecuados	Algo adecuados	Muy adecuados
25	¿Conoce el manejo de los sistemas utilizados en el teletrabajo?	Nada	Casi nada	A medias	Algo	Mucho
26	¿Se capacita frecuentemente al personal sobre el manejo de los sistemas de la empresa?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
27	¿Los sistemas de la empresa se encuentran operativos cuando se les requiere?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
28	¿El servicio de internet presenta caídas frecuentemente?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
29	¿Considera usted que las herramientas tecnológicas utilizadas son las más adecuadas?	Muy inadecuadas	Algo inadecuadas	Ni adecuadas, ni inadecuadas	Algo adecuadas	Muy adecuadas
30	¿Se cuenta con herramientas tecnológicas que protejan la realización de sus labores en teletrabajo?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
31	¿Las metas de la institución están enfocadas al cambio adecuado respecto al teletrabajo?	Nada	Casi nada	A medias	Algo	Totalmente
32	¿Se establecen objetivos a corto plazo que permitan alcanzar las metas organizacionales?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
33	¿Existen controles que permitan asegurar el cambio de manera efectiva?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
34	¿Se realiza un monitoreo frecuente de los controles establecidos para el cambio?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
35	¿Considera usted que el cambio se encuentra adecuadamente documentado en la institución?	Nunca	Casi nunca	A veces	Casi siempre	Siempre
36	¿Se comunica los planes y beneficios del cambio organizacional a todo el personal?	Nunca	Casi nunca	A veces	Casi siempre	Siempre

¡Gracias por su tiempo!

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

Validación del Experto N°1

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: Ciberseguridad

Nº	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Preservación de la confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera usted que las políticas de ciberseguridad garantizan el acceso autorizado a los sistemas?	x		x		x		
2	¿Considera usted que los métodos para establecer contraseñas seguras son los más adecuados?	x		x		x		
3	¿Considera usted que solo el personal autorizado debe acceder a los sistemas, base de datos e información digital de la institución?	x		x		x		
4	¿Considera usted que los mecanismos de autorización son los adecuados frente a alguna amenaza informática?	x		x		x		
5	¿Considera usted que se deben realizar copias de seguridad periódicamente?	x		x		x		
6	¿Cree usted que se ha perdido información importante debido a algún ataque informático?	x		x		x		
	Preservación de la Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Considera usted que la información que proporciona los sistemas y bases de datos es precisa?	x		x		x		
8	¿La información contenida en los sistemas y base de datos se mantiene precisa a través del tiempo?	x		x		x		
9	¿Los métodos aplicados para que la información permanezca completa en la base de datos cumplen su función?	x		x		x		
10	¿Alguna vez los sistemas han fallado al grabar información o han mostrado datos errados al ser consultados?	x		x		x		
11	¿Los procedimientos para realizar una modificación en los sistemas y base de datos son adecuados?	x		x		x		
12	¿Considera usted imposible realizar una modificación de datos no autorizada en los sistemas?	x		x		x		
	Preservación de la Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Los mecanismos de acceso son adecuados frente a las amenazas de ciberseguridad en el teletrabajo?	x		x		x		
14	¿Los mecanismos de acceso garantizan que solo el personal autorizado pueda hacer uso de los sistemas y base de datos?	x		x		x		
15	¿Considera usted que las consultas en los sistemas de información demoran en responder?	x		x		x		
16	¿Los sistemas y bases de datos demoran en restablecerse luego de un incidente informático?	x		x		x		
17	¿Considera usted que la conexión VPN está totalmente protegida para la realización del teletrabajo?	x		x		x		
18	¿Alguna vez tuvo que detener sus labores por causa de algún ataque informático?	x		x		x		

VARIABLE: Teletrabajo

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Espacio físico	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Los medios de ingreso y salida a su centro de teletrabajo son adecuados?	X		X		X		
20	¿Cuenta con más de un medio de ingreso o salida a su centro de teletrabajo?	X		X		X		
21	¿Cree usted que su centro de teletrabajo es totalmente seguro para que pueda realizar sus labores?	X		X		X		
22	¿Su centro de teletrabajo cuenta con mecanismos que resguarden su información y la de su empresa?	X		X		X		
23	¿Cuenta con controles de acceso a su centro de teletrabajo?	X		X		X		
24	¿Considera usted que los controles de acceso a su centro de teletrabajo son adecuados?	X		X		X		
	Uso de las TIC	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Conoce el manejo de los sistemas utilizados en el teletrabajo?	X		X		X		
26	¿Se capacita frecuentemente al personal sobre el manejo de los sistemas de la empresa?	X		X		X		
27	¿Los sistemas de la empresa se encuentran operativos cuando se les requiere?	X		X		X		
28	¿El servicio de internet presenta caídas frecuentemente?	X		X		X		
29	¿Considera usted que las herramientas tecnológicas utilizadas son las más adecuadas?	X		X		X		
30	¿Se cuenta con herramientas tecnológicas que protejan la realización de sus labores en teletrabajo?	X		X		X		
	Cambio organizacional	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Las metas de la institución están enfocadas al cambio adecuado respecto al teletrabajo?	X		X		X		
32	¿Se establecen objetivos a corto plazo que permitan alcanzar las metas organizacionales?	X		X		X		
33	¿Existen controles que permitan asegurar el cambio de manera efectiva?	X		X		X		
34	¿Se realiza un monitoreo frecuente de los controles establecidos para el cambio?	X		X		X		
35	¿Considera usted que el cambio se encuentra adecuadamente documentado en la institución?	X		X		X		
36	¿Se comunica los planes y beneficios del cambio organizacional a todo el personal?	X		X		X		

Observaciones (precisar si hay suficiencia):___ _____

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

11 de Octubre del 2022

Apellidos y nombres del juez evaluador: LEZAMA GONZALES PEDRO MARTIN **DNI: 09656793**

Especialista: Metodólogo [X] **Temático [X]**

Grado: Maestro [ ] **Doctor [X]**

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

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

Firma del Experto Informante

Validación del Experto N°2

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: Ciberseguridad

Nº	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Preservación de la confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera usted que las políticas de ciberseguridad garantizan el acceso autorizado a los sistemas?	x		x		x		
2	¿Considera usted que los métodos para establecer contraseñas seguras son los más adecuados?	x		x		x		
3	¿Considera usted que solo el personal autorizado debe acceder a los sistemas, base de datos e información digital de la institución?	x		x		x		
4	¿Considera usted que los mecanismos de autorización son los adecuados frente a alguna amenaza informática?	x		x		x		
5	¿Considera usted que se deben realizar copias de seguridad periódicamente?	x		x		x		
6	¿Cree usted que se ha perdido información importante debido a algún ataque informático?	x		x		x		
	Preservación de la Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Considera usted que la información que proporciona los sistemas y bases de datos es precisa?	x		x		x		
8	¿La información contenida en los sistemas y base de datos se mantiene precisa a través del tiempo?	x		x		x		
9	¿Los métodos aplicados para que la información permanezca completa en la base de datos cumplen su función?	x		x		x		
10	¿Alguna vez los sistemas han fallado al grabar información o han mostrado datos errados al ser consultados?	x		x		x		
11	¿Los procedimientos para realizar una modificación en los sistemas y base de datos son adecuados?	x		x		x		
12	¿Considera usted imposible realizar una modificación de datos no autorizada en los sistemas?	x		x		x		
	Preservación de la Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Los mecanismos de acceso son adecuados frente a las amenazas de ciberseguridad en el teletrabajo?	x		x		x		
14	¿Los mecanismos de acceso garantizan que solo el personal autorizado pueda hacer uso de los sistemas y base de datos?	x		x		x		
15	¿Considera usted que las consultas en los sistemas de información demoran en responder?	x		x		x		
16	¿Los sistemas y bases de datos demoran en restablecerse luego de un incidente informático?	x		x		x		
17	¿Considera usted que la conexión VPN está totalmente protegida para la realización del teletrabajo?	x		x		x		
18	¿Alguna vez tuvo que detener sus labores por causa de algún ataque informático?	x		x		x		

VARIABLE: Teletrabajo

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Espacio físico	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Los medios de ingreso y salida a su centro de teletrabajo son adecuados?	x		x		x		
20	¿Cuenta con más de un medio de ingreso o salida a su centro de teletrabajo?	x		x		x		
21	¿Cree usted que su centro de teletrabajo es totalmente seguro para que pueda realizar sus labores?	x		x		x		
22	¿Su centro de teletrabajo cuenta con mecanismos que resguarden su información y la de su empresa?	x		x		x		
23	¿Cuenta con controles de acceso a su centro de teletrabajo?	x		x		x		
24	¿Considera usted que los controles de acceso a su centro de teletrabajo son adecuados?	x		x		x		
	Uso de las TIC	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Conoce el manejo de los sistemas utilizados en el teletrabajo?	x		x		x		
26	¿Se capacita frecuentemente al personal sobre el manejo de los sistemas de la empresa?	x		x		x		
27	¿Los sistemas de la empresa se encuentran operativos cuando se les requiere?	x		x		x		
28	¿El servicio de internet presenta caídas frecuentemente?	x		x		x		
29	¿Considera usted que las herramientas tecnológicas utilizadas son las más adecuadas?	x		x		x		
30	¿Se cuenta con herramientas tecnológicas que protejan la realización de sus labores en teletrabajo?	x		x		x		
	Cambio organizacional	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Las metas de la institución están enfocadas al cambio adecuado respecto al teletrabajo?	x		x		x		
32	¿Se establecen objetivos a corto plazo que permitan alcanzar las metas organizacionales?	x		x		x		
33	¿Existen controles que permitan asegurar el cambio de manera efectiva?	x		x		x		
34	¿Se realiza un monitoreo frecuente de los controles establecidos para el cambio?	x		x		x		
35	¿Considera usted que el cambio se encuentra adecuadamente documentado en la institución?	x		x		x		
36	¿Se comunica los planes y beneficios del cambio organizacional a todo el personal?	x		x		x		

Observaciones (precisar si hay suficiencia):___ _____

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

13 de octubre del 2022

Apellidos y nombres del juez evaluador: **Pereyra Acosta Manuel Antonio** **DNI: 07268839**

Especialista: Metodólogo [X] **Temático [X]**

Grado: Maestro [ ] **Doctor [X]**

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

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

Firma del Experto Informante

Validación del Experto N°3

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: Ciberseguridad

Nº	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Preservación de la confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera usted que las políticas de ciberseguridad garantizan el acceso autorizado a los sistemas?	x		x		x		
2	¿Considera usted que los métodos para establecer contraseñas seguras son los más adecuados?	x		x		x		
3	¿Considera usted que solo el personal autorizado debe acceder a los sistemas, base de datos e información digital de la institución?	x		x		x		
4	¿Considera usted que los mecanismos de autorización son los adecuados frente a alguna amenaza informática?	x		x		x		
5	¿Considera usted que se deben realizar copias de seguridad periódicamente?	x		x		x		
6	¿Cree usted que se ha perdido información importante debido a algún ataque informático?	x		x		x		
	Preservación de la Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Considera usted que la información que proporciona los sistemas y bases de datos es precisa?	x		x		x		
8	¿La información contenida en los sistemas y base de datos se mantiene precisa a través del tiempo?	x		x		x		
9	¿Los métodos aplicados para que la información permanezca completa en la base de datos cumplen su función?	x		x		x		
10	¿Alguna vez los sistemas han fallado al grabar información o han mostrado datos errados al ser consultados?	x		x		x		
11	¿Los procedimientos para realizar una modificación en los sistemas y base de datos son adecuados?	x		x		x		
12	¿Considera usted imposible realizar una modificación de datos no autorizada en los sistemas?	x		x		x		
	Preservación de la Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Los mecanismos de acceso son adecuados frente a las amenazas de ciberseguridad en el teletrabajo?	x		x		x		
14	¿Los mecanismos de acceso garantizan que solo el personal autorizado pueda hacer uso de los sistemas y base de datos?	x		x		x		
15	¿Considera usted que las consultas en los sistemas de información demoran en responder?	x		x		x		
16	¿Los sistemas y bases de datos demoran en restablecerse luego de un incidente informático?	x		x		x		
17	¿Considera usted que la conexión VPN está totalmente protegida para la realización del teletrabajo?	x		x		x		
18	¿Alguna vez tuvo que detener sus labores por causa de algún ataque informático?	x		x		x		

VARIABLE: Teletrabajo

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Espacio físico	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Los medios de ingreso y salida a su centro de teletrabajo son adecuados?	x		x		x		
20	¿Cuenta con más de un medio de ingreso o salida a su centro de teletrabajo?	x		x		x		
21	¿Cree usted que su centro de teletrabajo es totalmente seguro para que pueda realizar sus labores?	x		x		x		
22	¿Su centro de teletrabajo cuenta con mecanismos que resguarden su información y la de su empresa?	x		x		x		
23	¿Cuenta con controles de acceso a su centro de teletrabajo?	x		x		x		
24	¿Considera usted que los controles de acceso a su centro de teletrabajo son adecuados?	x		x		x		
	Uso de las TIC	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Conoce el manejo de los sistemas utilizados en el teletrabajo?	x		x		x		
26	¿Se capacita frecuentemente al personal sobre el manejo de los sistemas de la empresa?	x		x		x		
27	¿Los sistemas de la empresa se encuentran operativos cuando se les requiere?	x		x		x		
28	¿El servicio de internet presenta caídas frecuentemente?	x		x		x		
29	¿Considera usted que las herramientas tecnológicas utilizadas son las más adecuadas?	x		x		x		
30	¿Se cuenta con herramientas tecnológicas que protejan la realización de sus labores en teletrabajo?	x		x		x		
	Cambio organizacional	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Las metas de la institución están enfocadas al cambio adecuado respecto al teletrabajo?	x		x		x		
32	¿Se establecen objetivos a corto plazo que permitan alcanzar las metas organizacionales?	x		x		x		
33	¿Existen controles que permitan asegurar el cambio de manera efectiva?	x		x		x		
34	¿Se realiza un monitoreo frecuente de los controles establecidos para el cambio?	x		x		x		
35	¿Considera usted que el cambio se encuentra adecuadamente documentado en la institución?	x		x		x		
36	¿Se comunica los planes y beneficios del cambio organizacional a todo el personal?	x		x		x		

Observaciones (precisar si hay suficiencia): Si tiene audiencia para su aplicación

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

15 de octubre del 2022

Apellidos y nombres del juez evaluador: Flores Zafra David DNI: 41541647

Especialista: Metodólogo [X] Temático [X]

Grado: Maestro [ ] Doctor [X]

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

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

Firma del Experto Informante

Anexo 5: Base de datos

Encuesta	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	1	5	5	4	4	5	3	5	5	5	5	5	4	5	5	3	3	5	3	3	2	4	3	3	3	5	5	4	2	4	4	3	5	4	4	4	3
2	1	4	5	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	3	5	2	3	3	3	3	5	5	4	2	3	4	3	4	4	4	5	3
3	2	4	5	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	5	4	2	3	3	3	3	4	4	4	1	3	4	3	4	4	4	5	3
4	2	4	4	5	4	4	2	4	4	4	5	4	2	3	3	2	2	4	3	4	3	5	5	5	5	5	5	5	3	5	5	4	5	5	5	4	5
5	1	3	3	2	2	3	1	3	3	2	3	2	1	2	3	1	1	1	1	5	1	5	5	5	5	5	5	5	2	5	5	5	5	5	5	5	5
6	1	5	5	5	5	4	2	5	5	4	4	4	4	5	5	3	3	5	3	5	1	4	3	3	3	5	4	5	1	4	4	3	5	4	4	4	3
7	2	5	5	5	5	4	1	5	4	4	4	4	4	5	5	2	3	5	5	3	1	3	3	3	3	4	4	4	1	3	4	3	4	5	5	3	3
8	1	5	5	5	4	3	1	4	5	3	3	3	3	4	3	2	1	3	3	5	3	4	4	4	4	5	3	5	3	4	4	4	5	5	5	4	4
9	2	5	5	5	5	5	1	5	5	5	5	5	2	5	5	3	3	5	3	5	2	3	3	3	3	5	5	4	2	3	4	3	4	4	4	5	3
10	2	4	4	5	5	3	1	4	4	3	3	3	3	4	5	3	3	5	3	5	1	5	5	5	5	5	5	5	2	5	5	5	5	4	5	5	5
11	1	5	5	5	5	5	2	5	5	5	5	5	5	5	5	3	3	5	3	5	2	5	3	3	3	4	4	4	1	3	4	3	4	4	4	5	3
12	1	5	4	5	5	4	2	5	5	4	4	4	4	5	5	3	3	5	3	5	1	4	3	3	3	5	4	5	1	4	4	3	5	4	4	4	3
13	1	5	3	5	5	5	1	5	5	5	5	5	5	5	5	3	3	5	3	3	1	3	3	3	3	4	4	4	1	3	4	3	4	3	5	4	3
14	2	4	3	4	4	4	2	5	3	3	4	4	4	5	4	2	2	4	3	5	3	4	4	4	4	5	3	5	3	4	4	4	5	5	5	4	4
15	2	5	5	4	5	5	2	5	5	4	5	4	4	5	5	3	3	5	3	5	1	4	3	3	3	5	3	5	2	3	4	3	5	5	2	3	3
16	2	5	3	3	3	4	1	4	5	4	4	3	3	5	4	1	2	4	4	5	5	4	4	4	4	5	5	4	2	5	5	4	4	5	5	4	4
17	1	5	4	3	3	3	2	5	5	3	3	3	3	4	3	1	1	3	4	5	1	5	5	5	5	5	5	5	2	5	5	5	5	4	5	5	5
18	1	5	5	4	4	4	2	4	5	4	4	5	5	5	5	3	5	5	5	3	1	3	3	3	3	4	4	4	1	3	4	3	4	4	4	5	3
19	2	1	1	1	1	1	1	1	1	2	3	2	3	5	5	3	3	5	3	4	3	4	5	5	5	5	5	4	5	5	5	3	2	2	1	3	2
20	2	5	5	5	5	5	2	5	5	4	4	4	3	5	5	3	3	5	3	3	1	3	3	3	3	4	4	4	1	3	4	3	4	3	5	4	3
21	2	5	5	4	4	4	2	5	5	4	4	4	4	5	5	3	5	5	5	3	1	4	3	3	3	4	4	4	1	3	5	2	3	3	3	3	3
22	1	5	4	4	4	4	2	4	4	4	5	3	3	5	5	3	3	3	3	5	2	3	3	3	3	5	5	4	2	3	4	3	4	4	4	5	3
23	1	3	3	3	2	2	1	3	3	2	3	2	1	3	3	3	2	3	1	3	2	5	5	5	5	5	5	5	2	5	5	5	4	5	5	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	1	5	5	4	4	4	2	5	5	4	4	4	4	5	5	3	3	5	3	5	2	5	3	3	3	4	4	4	1	3	4	4	5	3	3	5	3
25	1	4	4	4	4	4	2	4	5	4	4	3	3	5	5	3	3	3	3	5	2	3	4	4	4	5	4	5	1	4	4	4	5	3	3	5	3
26	1	5	5	3	3	5	2	4	4	4	5	3	3	4	3	2	2	2	2	5	1	5	5	5	5	5	4	4	3	5	5	5	5	5	5	5	5
27	1	5	5	3	3	5	3	4	4	5	5	5	5	5	5	2	4	5	5	5	2	5	3	3	3	4	4	4	1	3	4	3	4	4	4	5	3
28	1	5	5	3	3	5	2	3	3	4	4	4	4	4	5	2	2	2	4	5	1	5	5	5	5	5	5	4	2	5	5	5	4	5	5	5	5
29	1	5	4	5	5	5	4	5	5	5	5	5	5	4	5	2	4	5	5	5	1	4	3	3	3	5	4	5	1	4	4	3	5	4	4	4	3
30	2	5	5	5	5	5	3	5	5	5	5	5	5	5	5	2	5	5	5	3	1	3	3	3	3	4	4	4	1	3	4	3	4	4	4	5	3
31	1	5	5	3	3	5	4	5	5	5	5	5	5	5	5	2	5	5	5	3	1	4	3	3	3	4	4	4	1	3	5	3	5	5	2	3	3
32	1	4	4	4	4	4	2	4	4	4	4	3	4	4	4	3	4	3	2	5	1	5	5	5	5	5	5	5	2	5	5	5	5	4	5	5	5
33	1	4	5	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	5	3	1	3	3	3	3	4	4	4	1	3	4	3	4	4	4	5	3
34	2	5	5	3	3	4	2	4	4	4	4	3	4	4	4	2	2	3	2	4	3	5	5	5	5	5	5	5	3	5	5	4	5	5	5	4	5
35	1	4	4	4	4	4	2	5	3	3	3	3	4	4	4	2	2	2	2	5	1	5	5	5	5	5	5	5	2	5	5	5	5	5	5	5	5
36	1	5	5	5	5	4	2	5	5	4	4	4	4	5	5	3	3	5	3	4	2	3	3	3	3	4	4	4	1	3	4	3	4	4	4	5	3
37	1	5	5	5	5	5	2	4	4	5	5	4	4	5	5	3	5	5	3	5	2	5	3	3	3	4	4	4	1	3	4	3	4	4	4	5	3
38	1	5	5	5	5	3	2	4	5	5	5	4	4	5	5	3	5	5	5	2	1	2	3	1	2	2	2	3	2	2	3	3	2	2	1	3	2
39	2	5	5	4	4	4	1	4	5	3	3	3	3	4	3	1	2	3	3	5	3	5	5	5	5	5	3	5	3	4	4	4	5	5	5	4	4
40	2	3	3	3	1	3	1	3	3	2	3	1	2	2	3	1	1	1	1	5	3	5	5	5	5	5	3	5	3	4	4	4	5	5	5	4	4
41	1	5	5	4	4	5	3	5	5	5	5	5	4	5	5	3	3	5	3	5	2	5	3	3	3	4	4	4	1	3	4	3	4	4	4	5	3
42	1	4	5	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	3	3	1	3	3	3	3	4	4	4	1	3	4	3	4	4	4	5	3
43	2	4	5	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	5	1	1	2	2	1	2	1	3	2	2	2	2	3	2	2	1	3	2
44	1	5	5	3	3	3	1	5	5	3	3	3	3	5	3	1	1	3	4	5	3	5	5	5	4	5	3	5	3	4	4	4	5	5	5	4	4
45	1	5	5	3	3	3	1	5	5	3	3	3	3	5	3	1	1	3	4	4	3	4	5	5	5	5	5	5	2	5	5	5	4	5	5	5	5
46	1	3	3	3	2	2	1	3	3	2	3	1	2	2	3	1	1	1	1	5	3	5	5	5	4	5	4	5	3	4	5	4	4	5	5	4	4
47	1	4	5	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	3	5	1	4	3	3	3	5	5	4	1	3	4	3	5	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
48	2	4	5	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	5	1	1	2	2	1	2	1	3	2	2	2	2	3	2	2	1	3	2
49	2	3	3	3	2	2	1	3	3	2	3	1	2	2	3	1	1	1	1	4	3	4	5	5	5	5	5	5	2	5	5	5	4	5	5	5	5
50	2	5	5	5	5	5	2	4	4	5	5	4	4	5	5	3	3	5	3	3	1	3	3	3	3	4	4	4	1	3	4	3	4	3	5	4	3
51	1	5	5	5	5	3	2	4	5	5	5	4	4	5	5	3	5	5	3	1	1	2	2	1	2	1	3	2	2	2	2	3	2	2	1	3	2
52	1	5	5	3	3	3	1	5	5	3	3	3	3	5	3	1	1	3	4	4	3	4	5	5	5	5	5	5	2	5	5	5	4	5	5	5	5
53	1	5	5	4	3	5	2	4	5	5	5	5	5	5	5	3	3	5	3	3	1	3	3	3	3	4	4	4	1	3	4	3	4	3	5	4	3
54	1	5	4	5	5	4	2	4	5	4	4	4	4	5	5	3	5	5	3	2	1	2	3	1	2	2	2	3	2	2	3	2	2	3	2	2	3
55	1	3	3	3	2	2	1	4	4	4	5	4	4	5	5	3	3	5	3	4	3	5	4	4	4	5	5	4	1	3	4	3	4	4	4	5	3
56	2	5	4	4	4	5	4	5	5	5	5	5	5	4	5	2	4	5	5	5	1	4	3	3	3	2	2	3	2	2	3	2	2	3	2	2	3
57	1	4	4	5	4	5	1	4	4	5	4	3	3	5	5	2	4	4	3	5	5	4	4	3	3	3	3	2	3	1	2	2	2	3	2	2	3
58	2	5	5	5	4	5	3	4	5	3	3	3	3	5	5	3	3	3	3	4	2	3	3	3	3	5	5	4	1	4	5	3	4	5	5	4	3
59	2	5	5	4	4	3	3	5	4	4	3	3	3	5	4	2	4	4	2	4	3	5	4	4	4	5	5	4	1	3	4	3	4	4	4	5	3
60	2	4	4	3	4	5	3	5	5	5	5	5	5	5	5	2	5	5	5	3	3	4	5	5	5	4	4	4	1	3	4	3	4	4	4	5	2
61	1	3	3	2	2	3	1	5	4	4	3	3	5	5	4	2	4	4	5	5	5	4	4	3	3	3	3	2	3	1	2	2	2	3	2	2	3
62	1	5	5	4	4	3	3	5	4	4	3	3	3	5	4	2	4	4	2	4	1	4	4	5	5	5	5	5	2	5	5	5	5	4	5	5	5
63	1	4	4	5	4	5	1	4	4	5	4	3	3	5	5	2	4	4	3	3	1	4	3	3	3	5	5	4	1	4	5	3	5	5	5	5	3
64	1	5	5	5	5	5	4	4	3	2	2	4	3	5	4	2	4	4	2	3	1	4	3	3	3	5	5	4	1	4	5	3	5	5	5	5	3
65	1	5	5	5	4	5	4	5	5	5	5	5	5	5	5	3	3	5	5	2	1	2	3	1	2	3	2	3	2	2	3	3	3	3	2	3	2
66	1	3	3	3	4	4	2	4	4	4	4	4	4	5	4	2	4	4	5	4	3	5	5	5	5	5	5	5	3	5	5	5	5	5	5	5	5
67	1	3	3	3	1	3	1	3	3	2	3	1	2	2	3	1	1	1	1	4	3	4	5	5	5	5	5	4	2	4	4	4	4	4	4	4	4
68	2	5	5	5	5	5	4	5	5	5	5	5	5	5	5	3	3	5	3	3	2	4	3	3	3	5	5	4	1	4	4	3	5	4	4	4	3
69	1	4	4	4	3	3	1	4	5	3	3	4	5	5	5	3	3	5	3	4	3	5	5	5	5	3	3	2	3	1	2	2	2	3	2	2	3
70	2	2	2	2	2	2	1	3	3	2	3	2	2	4	4	2	2	3	1	4	3	5	5	5	5	5	5	5	3	5	5	5	5	5	5	5	5
71	2	5	5	5	5	5	4	5	5	5	5	5	5	5	5	3	3	5	3	5	2	5	3	3	3	4	4	4	1	3	4	3	5	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
72	1	5	5	4	5	5	3	5	5	5	5	5	5	5	5	2	5	5	5	2	1	2	3	1	2	2	2	3	2	2	3	2	2	3	2	2	3
73	1	1	1	1	1	1	1	1	1	2	3	2	3	5	5	3	3	5	3	5	3	5	5	5	5	5	5	5	3	4	5	3	2	2	1	3	2
74	1	5	5	5	5	5	2	5	4	4	4	5	5	2	3	2	2	3	2	3	2	4	3	3	3	5	5	4	1	3	4	3	4	5	5	4	3
75	1	4	4	5	4	3	1	5	5	3	3	3	3	5	5	3	3	5	3	4	3	5	5	5	5	5	5	5	2	5	5	3	5	4	4	4	3
76	1	1	1	1	1	1	1	1	1	2	3	2	3	5	5	3	3	5	3	4	3	5	5	5	5	5	5	5	3	5	5	2	2	3	2	2	3
77	2	5	5	4	5	5	3	5	5	5	5	5	5	4	4	2	4	4	5	3	2	4	3	3	3	4	4	4	1	3	5	3	4	5	5	4	3
78	1	5	5	4	4	4	2	4	5	4	4	4	4	5	4	1	1	4	4	2	1	2	3	1	2	2	2	3	2	2	3	3	3	3	2	3	2
79	2	1	1	1	1	1	1	1	1	2	3	2	3	5	5	3	3	5	3	4	3	4	5	5	5	5	5	4	5	5	5	3	2	2	1	3	2
80	1	5	5	4	4	4	2	4	5	4	4	4	4	4	5	2	4	5	5	3	1	3	3	3	3	4	4	4	1	3	4	3	4	4	4	4	3
81	1	5	5	4	5	3	1	5	5	3	3	3	3	5	3	1	1	3	4	4	3	5	5	5	5	5	4	5	2	4	5	3	5	5	5	5	3
82	1	3	3	3	2	2	1	3	3	2	3	1	2	2	3	1	1	1	1	4	3	4	5	5	5	5	5	5	2	5	5	5	4	5	5	5	5
83	1	5	5	4	4	5	1	4	5	5	5	5	5	4	5	2	4	5	5	3	2	4	3	3	3	5	5	3	1	4	5	3	5	4	4	4	3
84	1	5	5	5	5	4	3	5	4	4	4	4	4	5	4	2	4	4	5	1	1	2	2	1	2	1	3	2	2	2	2	3	2	2	1	3	2
85	2	3	3	3	2	2	1	3	3	1	3	2	2	2	3	1	1	1	1	4	3	5	4	4	4	5	4	5	3	4	5	4	5	5	5	5	4
86	2	5	4	4	4	5	4	5	5	5	5	5	5	4	5	2	4	5	5	3	2	4	4	4	4	5	4	4	2	4	4	2	3	3	1	3	3
87	1	5	5	5	4	3	1	4	5	3	3	3	3	4	3	1	2	3	3	5	1	5	5	5	5	5	5	4	2	5	5	5	5	5	4	5	5
88	1	5	5	5	4	5	3	4	5	5	5	5	5	5	5	3	4	5	5	5	1	5	5	5	5	5	5	4	2	5	5	5	4	5	5	5	5
89	1	5	5	4	5	3	1	4	5	3	3	3	3	4	3	1	2	3	3	3	2	4	3	3	3	5	5	3	1	4	5	3	5	4	4	4	3
90	2	5	5	4	5	5	3	5	5	5	5	5	5	5	5	2	5	5	5	1	1	2	2	1	2	1	3	2	2	2	2	3	2	2	1	3	2
91	1	1	1	1	1	1	1	1	1	2	3	2	3	5	5	3	3	5	3	4	3	4	5	5	5	5	5	4	5	5	5	3	2	2	1	3	2
92	1	4	4	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	3	5	1	4	3	3	3	5	4	5	1	4	4	3	5	4	4	4	3
93	2	4	5	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	5	3	1	3	3	3	3	4	4	4	1	3	4	3	4	4	4	4	3
94	1	5	5	5	5	5	4	5	5	5	5	5	5	4	5	2	4	5	5	3	1	4	3	3	3	4	4	4	1	3	5	2	3	3	1	3	3
95	1	5	5	5	4	5	4	5	5	5	5	5	5	5	5	3	3	5	5	2	1	2	3	1	2	2	2	3	2	2	3	3	2	2	2	3	2

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	5	5	5	4	3	1	4	5	3	3	3	3	4	3	1	2	3	3	4	3	5	5	5	5	5	4	4	3	4	4	4	5	5	4	5	4
97	2	5	5	4	5	4	1	5	4	4	4	4	4	5	5	3	3	5	3	3	2	4	4	4	4	5	4	4	2	4	4	2	3	3	1	3	3
98	1	4	4	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	3	1	1	2	2	1	2	1	3	2	2	2	2	3	2	2	1	3	2
99	2	4	4	4	4	4	2	4	4	4	4	4	3	4	4	3	4	3	2	4	3	5	5	5	5	5	5	5	2	5	5	5	4	4	5	5	5
100	1	4	4	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	3	3	1	3	3	3	3	4	4	4	1	3	4	3	5	4	4	4	3
101	1	4	5	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	5	1	1	2	2	1	2	1	3	2	2	2	2	3	2	2	1	3	2
102	2	4	4	4	4	4	2	4	4	4	4	4	3	4	4	3	4	3	2	4	3	5	5	5	5	5	5	5	3	5	5	4	5	5	5	4	5
103	1	5	5	5	4	5	4	5	5	5	5	5	5	5	5	3	3	5	5	3	2	4	4	4	4	5	4	4	2	4	4	3	4	4	4	4	3
104	1	5	5	5	4	4	2	5	5	4	4	4	4	5	5	3	3	5	3	1	1	2	2	1	2	1	3	2	2	2	2	3	2	2	1	3	2
105	1	4	5	5	4	3	1	4	4	3	3	3	3	4	3	2	2	3	3	4	3	5	5	5	5	5	4	4	3	4	4	4	4	4	4	4	4
106	1	5	5	4	5	4	1	5	4	4	4	4	4	4	5	2	4	5	5	3	2	4	3	3	3	5	5	3	1	4	5	3	5	4	4	4	3
107	1	4	4	5	5	5	4	5	5	5	5	5	5	5	5	3	5	5	3	1	1	2	2	1	2	1	3	2	2	2	2	3	2	2	1	3	2
108	1	4	5	5	4	3	1	4	4	3	3	3	3	4	3	2	2	3	3	4	3	5	5	5	5	5	5	5	2	5	5	5	4	4	5	5	5

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, VISURRAGA AGUERO JOEL MARTIN, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Ciberseguridad y su incidencia en el Teletrabajo en una entidad pública, Lima 2022", cuyo autor es MARIN PURIS LUIS ENRIQUE, constato que la investigación tiene un índice de similitud de 17.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 07 de Enero del 2023

Apellidos y Nombres del Asesor:	**Firma**
VISURRAGA AGUERO JOEL MARTIN **DNI:** 10192325 **ORCID:** 0000-0002-0024-668X	Firmado electrónicamente por: JMVISURRAGA el 11-01-2023 20:53:55

Código documento Trilce: TRI - 0513095

INVESTIGA UCV