FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

TESIS

LOS DELITOS INFORMÁTICOS Y LA VULNERACIÓN DEL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES EN LIMA METROPOLITANA

PARA OBTENER EL TÍTULO DE

ABOGADA

AUTORA

ANABELIZA URDANEGUI RANGEL

ORCID: 0000-0001-7560-9820

ASESOR

MAG. MARCOS ENRIQUE TUME CHUNGA

ORCID: 0000-0003-4484-6609

LÍNEA DE INVESTIGACIÓN

PROMOCIÓN Y DEFENSA DE LOS DERECHOS HUMANOS EN EL ÁMBITO NACIONAL E INTERNACIONAL

LIMA, PERÚ, DICIEMBRE DE 2023

CC BY

https://creativecommons.org/licenses/by/4.0/

Esta licencia permite a otros distribuir, mezclar, ajustar y construir a partir de su obra, incluso con fines comerciales, siempre que le sea reconocida la autoría de la creación original. Esta es la licencia más servicial de las ofrecidas. Recomendada para una máxima difusión y utilización de los materiales sujetos a la licencia.

Referencia bibliográfica

Urdanegui Rangel, A. (2023). *Los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana* [Tesis de pregrado, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú.

HOJA DE METADATOS

Datos del autor	
Nombres y apellidos	Anabeliza Urdanegui Rangel
Tipo de documento de identidad	DNI
Número de documento de identidad	44247111
URL de ORCID	https://orcid.org/0000-0001-7560-9820
Datos del asesor	
Nombres y apellidos	Marcos Enrique Tume Chunga
Tipo de documento de identidad	DNI
Número de documento de identidad	41058938
URL de ORCID	https://orcid.org/0000-0003-4484-6609
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Luis Ángel Espinoza Pajuelo
Tipo de documento	DNI
Número de documento de identidad	10594662
Secretario del jurado	
Nombres y apellidos	Jessica Patricia Huali Ramos Vda. De Afán
Tipo de documento	DNI
Número de documento de identidad	42686844
Vocal del jurado	
Nombres y apellidos	Marcos Enrique Tume Chunga
Tipo de documento	DNI
Número de documento de identidad	41058938
Datos de la investigación	
Título de la investigación	Los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana
Línea de investigación Institucional	Persona, Sociedad, Empresa
Línea de investigación del Programa	Enfoque interdisciplinario de la ciencia jurídica
URL de disciplinas OCDE	https://purl.org/pe-repo/ocde/ford#5.05.01

FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

ACTA DE SUSTENTACIÓN DE TESIS

En la ciudad de Lima, el jurado de sustentación de tesis conformado por: el DR. LUIS ÁNGEL ESPINOZA PAJUELO como presidente, la MAG. JESSICA PATRICIA HUALI RAMOS VDA. DE AFAN como secretaria y el MAG. MARCOS ENRIQUE TUME CHUNGA como vocal, reunidos en acto público para dictaminar la tesis titulada:

LOS DELITOS INFORMÁTICOS Y LA VULNERACIÓN DEL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES EN LIMA METROPOLITANA

Presentado por la bachiller:

ANABELIZA URDANEGUI RANGEL

Para obtener el **Título Profesional de Abogada**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado – Bueno** con una calificación de **DIECISEIS (16).**

En fe de lo cual firman los miembros del jurado, el 11 de diciembre del 2023.

PRESIDENTE DR. LUIS ÁNGEL ESPINOZA PAJUELO	**SECRETARIA** MAG. JESSICA PATRICIA HUALI RAMOS VDA. DE AFAN	**VOCAL** MAG. MARCOS ENRIQUE TUME CHUNGA

ACTA DE APROBACIÓN DE ORIGINALIDAD

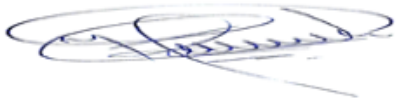
Yo Marcos Enrique Tume Chunga docente de la Facultad de Derecho de la Escuela Profesional de Derecho de la Universidad Autónoma del Perú, en mi condición de asesor de la tesis titulada:

LOS DELITOS INFORMÁTICOS Y LA VULNERACIÓN DEL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES EN LIMA METROPOLITANA

De la bachiller ANABELIZA URDANEGUI RANGEL, certifico que la tesis tiene un índice de similitud de 20% verificable en el reporte de similitud del software Turnitin que se adjunta.

El suscrito revisó y analizó dicho reporte a lo que concluyó 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 Autónoma del Perú.

Lima, 23 de Enero de 2024



_____

Marcos Enrique Tume Chunga

DNI 41072118

DEDICATORIA

La realización de este trabajo está dedicada a nuestras familias, pilares fundamentales en nuestras vidas. Sin ellos jamás hubiésemos podido conseguir lo que hasta ahora. Su tenacidad y lucha insaciable han hecho de ellos un gran ejemplo a seguir y destacar. A ellos este trabajo.

AGRADECIMIENTOS

Agradezco a Dios por permitirme concluir mi carrera con salud, a nuestro centro de estudios la Universidad Autónoma del Perú, a mi asesor MG. Marcos Enrique Tume Chunga, quien me supo inculcar sus conocimientos a lo largo de este tiempo con gran compromiso y dedicación. Indudablemente a mi familia por ser mi mayor motivación a lo largo de toda mi vida, por su apoyo y sabios consejos que orientaron mi formación, tanto personal como profesional. Asimismo, agradezco a todas las personas que me apoyaron de manera incondicional en su oportunidad.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

LOS DELITOS INFORMÁTICOS Y LA VULNERACIÓN DEL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES EN LIMA METROPOLITANA

ANABELIZA URDANEGUI RANGEL
UNIVERSIDAD AUTÓNOMA DEL PERÚ

RESUMEN

La presente investigación fue relevante porque permitió conocer la realidad referente a un tema actual en materia de delitos informáticos y su impacto frente al detrimento del derecho fundamental de protección de datos personales, pues con transcurrir del tiempo existe un avance vertiginoso en los ordenadores de la información y comunicaciones, generando con ello el incremento de la los crímenes cibernéticos, por lo que resulta relevante una protección eficaz por parte del Estado, a fin de contrarrestar esta problemática. En tal sentido, se describió la realidad problemática, teniendo en cuenta que si bien es cierto en el Perú se cuenta con la normatividad que regula y protege la vulneración de datos personales de los ciudadanos, así también tenemos normatividad en materia de delitos informáticos, los mismos que se encuentran sancionados penalmente, es importante analizar si esto ha sido suficiente frente al incremento de este tipo de delitos. Los aspectos metodológicos señalaron que se ha tenido una investigación de tipo básica, se tuvo como objetivo arribar a transformar teorías existentes, el diseño fue correlacional porque ha contado con dos variables que se relacionan entre sí, también se precisa que el enfoque fue cuantitativo. En conclusión, para lograr la solución idónea al problema de los delitos informáticos es que el Estado debe crear una Política Nacional De Ciberseguridad, puesto con ello se tendrán todas las medidas de prevenciones para evitar que más usuarios padezcan de los delitos informáticos o ciberdelincuencia.

***Palabras clave*:** delitos informáticos, protección de datos, ius puniendi, política criminal

COMPUTER CRIMES AND THE VIOLATION OF THE FUNDAMENTAL RIGHT OF PROTECTION OF PERSONAL DATA IN METROPOLITAN LIMA

ANABELIZA URDANEGUI RANGEL
UNIVERSIDAD AUTÓNOMA DEL PERÚ

ABSTRACT

The present investigation was relevant because it allowed us to know the reality regarding a current issue regarding computer crimes and its impact on the detriment of the fundamental right to protection of personal data, since with the passage of time there is a dizzying advance in information computers. and communications, thereby generating an increase in cybercrimes, which is why effective protection by the State is relevant in order to counteract this problem. In this sense, the problematic reality was described, taking into account that although it is true that Peru has regulations that regulate and protect the violation of citizens' personal data, we also have regulations regarding computer crimes, same that are criminally sanctioned, it is important to analyze whether this has been sufficient in the face of the increase in this type of crimes. The methodological aspects indicated that the research was of a basic type, the objective was to transform existing theories, the design was correlational because it had two variables that are related to each other, it is also specified that the approach was quantitative. In conclusion, to achieve the ideal solution to the problem of computer crimes, the State must create a National Cybersecurity Policy, since with this it will have all the preventive measures to prevent more users from suffering from computer crimes or cybercrime.

Keywords**:** computer crimes, data protection, ius puniendi, criminal policy

INTRODUCCIÓN

La presente investigación ha sido relevante, pues al tratarse de una problemática donde se atenta contra un derecho fundamental, estando el derecho de protección de datos personales, la cual se encuentra plenamente justificada. La acción aplicada a los datos informáticos, configuran este delito, en consecuencia, se puede precisar qué se trata de un delito común, pues se requiere el cumplimiento del tipo penal, sin considerar el resultado de dicha actividad.

En tal sentido, en el Perú se alinea al estándar sugerido por el Convenio contra la Cibercriminalidad de Budapest, si bien es cierto estas adiciones, no se ajustan a los lineamientos tecnológicos estandarizados, no afectan su interpretación, ni las acciones de cooperación internacionales, que involucren la aplicación de lucha transfronteriza contra el cibercrimen

Los delitos informáticos significan un perjuicio para los derechos humanos, debiendo el Estado innovar estrategias para combatir y prevenir la concurrencia de estos delitos.

Como respuesta al objetivo general, se ha encontrado que los delitos informáticos si se relaciona de manera directa con la vulneración al derecho de protección de datos personales en Lima Metropolitana, toda vez que se consumó el instrumento de esta pesquisa por medio de estadísticas con lo cual se logró dar respuesta al objetivo general.

La esencia de esta tesis ha abarcado 5 secuencias sistemáticas.

Capítulo I, se tuvo la redacción del problema junto con las finalidades de estudio, respecto al tema planteado.

Capítulo II, se desarrolló el esquema teórico mediante estudios previos y fundamentaciones científicas.

Capítulo III, se tuvo al esquema metodológico, estando representado principalmente por el tipo y enfoque de estudio, posteriormente se desarrolló el instrumento para rec9elctar datos.

Capítulo IV, se tuvo al análisis de datos, del cual se determinó la interpretación en base a las cifras estadísticas registradas.

Capítulo V, puso fin al estudio, ya que se plantearon discusiones según los resultados adquiridos, así mismo, de ello fue factible desarrollar conclusiones y recomendaciones.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1. Realidad problemática

Los delitos informáticos son conductas punibles ejercidas por los delincuentes por medio de programas informáticos implantándose virus, suplantación de sitios web, estafas, piratería, violación de derechos de autor, etc. En la óptica internacional, la nación de México estuvo sumamente afectada por la incidencia de los delitos informáticos, por cuanto, Alcalá y Meléndez (2023) han manifestado que:

> En México, la transformación digital mundial ha facilitado casi todas las actividades del ser humano y la pandemia originada por el virus SARS-COV-2 aumentó este fenómeno, pues las actividades comerciales, laborales, sanitarias, educativas y sociales, transitaron hacia la digitalización. En México, esto ha originado, los delitos informáticos como el robo y fraude informático, el hostigamiento digital o ciberacoso, que evolucionan aceleradamente y por tanto no se encuentran a la par en la legislación penal. De ahí que, las conductas delictivas han estado presentes y evolucionado en la historia de la humanidad; y en las sociedades del siglo XXI con la acelerada revolución tecnológica han surgido y crecido exponencialmente los ciberdelitos o delitos informáticos. Su conceptualización, características y legislación aplicable, han sido temas del debate jurídico en los últimos años, y en México es un tema pendiente, por lo que se considera importante analizarlos y determinar si su reconocimiento explícito en los ordenamientos penales contribuye a la denuncia, investigación, persecución, prevención y disminución. (pp. 1-2)

Así mismo, la nación de Colombia también estuvo afectada por la tendencia de los delitos informáticos, pues Álvarez (2023) ha manifestado que:

> En Colombia se registró un crecimiento de delitos informáticos en el último año, es decir, se registró en 2022 más de 54.000 denuncias por delitos informáticos

> o cibernéticos, superando ampliamente la cifra de 2021, cuando se documentaron 11.223. Los casos más comunes son a través de computadoras, tables y teléfonos celulares. Al respecto, Julián Buitrago, teniente de la Policía y director del centro cibernético de esta autoridad colombiana, explicó a la Voz de América las modalidades más comunes que utilizan los delincuentes para estafar en línea. Estos días se ha visto cómo las personas han denunciado temas bancarios, hurtos en el sistema financiero, y es porque los delincuentes han logrado obtener esas contraseñas. Normalmente los delincuentes envían mensajes de interés como subsidios o citaciones en la Fiscalía y ahí empiezan a entregar todos los datos para después aplicarles diferentes modalidades de estafa, apuntó. (p. 1)

En la misma situación el Perú ha tenido la incidencia de los delitos informáticos, por cuanto, el diario El Peruano (2023) ha reportado que:

> Cada mes, en Perú, se reportan más de 300 denuncias relacionadas con delitos informáticos, siendo los fraudes informáticos la categoría más frecuente, representando más de la mitad del total. Los ciberdelincuentes emplean diversas modalidades, como la clonación de sitios web de entidades bancarias, compras ilícitas en línea y el uso de teléfonos móviles robados para para ciberdelitos. Durante el año 2022 se registraron 2,382 denuncias por casos de fraude informático, convirtiéndolo en el delito informático más denunciado en el Perú a lo largo de 2022. (p. 4)

Por otra parte, la Defensoría del Pueblo (2023) ha reportado que:

> Lima Metropolitana y Lima Provincias registraron un poco más de la mitad de las denuncias por ciberdelitos formuladas ante la Policía Nacional durante el 2021, con el 53% del total. De modo que, durante el 2021 los ciberdelitos han

> representado un mayor de riesgo (alto), en donde se dieron principalmente en la región Lima, con una preocupante cifra de 53.08%. (pp. 32-33)

En base a ello, se ha determinado que en la actualidad la sociedad carece de una cultura de amparo de información personal. No podemos olvidar el amparo del ciudadano; esto hace que el procedimiento de su información personal sea un mecanismo necesario para asegurar el amparo de otros derechos humanos y libertades esenciales. Los ciudadanos de Lima Metropolitana frecuentemente exhiben su información en internet, mediante las redes sociales y correo electrónico, entre otros. Esto significa un peligro para su información ya que, a pesar de aceptar condiciones y términos de empleo de los servicios en mención, lo cierto es que muchas veces desconocen lo que están aceptando, y el uso que se le está dando a la información recopilada.

Los delitos informáticos pueden ser definidos como una acción ilícita que se desarrolla en un ambiente informático, haciendo uso de una computadora; el mismo que se encontraba regulad y sancionado en el Código Penal peruano, pero que a partir del 2013 el régimen que albergaba los delitos informáticos fue derogado por otro texto normativo.

A tal efecto, se tuvo a la Ley de Delitos Informáticos (2013) cuyo enunciado 1 ha manifestado que:

> La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. (p. 1)

Esta ley ha surgido con el propósito de resguardar los datos personales de los usuarios, pero es insuficiente ya que frecuentemente se continúan reportando casos de usuarios que han sido víctimas de delitos informáticos o ciberdelincuencia.

A medida que surgen nuevas tecnologías se da cabida a la concurrencia de más delitos informáticos, toda vez que las TIC dan una ventaja a los delincuentes para que estos puedan crear nuevas artimañas a fin de ejercer fechorías, pueden planificar bien el delito, incluso superando las barreras territoriales, pero también en borrar pistas que permitan conocer a los autores del crimen.

El Perú ha integrado un convenio supranacional para afrontar a los delitos informáticos, siendo el Convenio sobre la Ciberdelincuencia (2001) el cual ha manifestado que:

> Este convenio también es conocido como convenio de Budapest, es un tratado internacional creado en el año 2001 e impulsado por el Consejo de Europa, con el objetivo de incrementar la cooperación internacional y generar marcos legales armónicos entre las naciones con el objetivo de hacer frente a los delitos informáticos y a la actividad criminal en internet. Por ello, el régimen peruano tiene el deber de adoptar las medidas legislativas y de otro tipo que resulten necesarias para combatir la ciberdelincuencia. (pp. 2-3)

Por tanto, la solución idónea al problema de los delitos informáticos es que el Estado debe crear una Política Nacional De Ciberseguridad, puesto con ello se tendrán todas las medidas de prevenciones para evitar que más personas sean víctimas de los delitos informáticos o ciberdelincuencia.

Además, con esta medida se buscar también mantener la seguridad ciudadana, sobre todo que todo usuario tendrá la protección integra de sus datos en

todo momento y en cooperación con la Ley de Delitos Informáticos se buscará sancionar las conductas punibles de los ciberdelincuentes.

1.2. Formulación del problema

Problema general

¿Cuál es la relación entre los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana?

Problemas específicos

¿Cuál es la relación entre el sabotaje informático y el derecho a la intimidad?

¿Cuál es la relación entre el acceso a base de datos y el derecho al honor?

1.3. Objetivos de la investigación

Objetivo general

Determinan cuál es la relación entre los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana.

Objetivos específicos

Determinar cuál es la relación entre el sabotaje informático y el derecho a la intimidad.

Determina cuál es la relación entre el acceso a base de datos y el derecho al honor.

1.4. Justificación e importancia de la investigación

Se pretendió dar a conocer como los delitos informáticos afectan a los usuarios. Específicamente, el problema ha afectado a la comuna de Lima Metropolitana, de modo que ha habido diversos casos de usuarios que fueron víctimas de ciberdelitos.

Por tanto, ha resultado vital establecer medidas para confrontar los delitos informáticos con miras a proteger los datos de los usuarios.

Justificación legal

El problema de los delitos informáticos ha sido abordado por medio de las disposiciones de la Ley de Delitos Informáticos, por lo demás, se tuvo en cuenta las disposiciones de la Constitución Política donde se determina la protección de datos personales.

Justificación social

Mediante la creación una Política Nacional De Ciberseguridad se tendrá una salvaguarda de derechos de datos personales de los usuarios, pero ello será favorable no solo para Lima Metropolitana sino para toda la sociedad peruana, ya que también se buscará combatir la ola de delitos informáticos.

Justificación metodológica

El objetivo de medir las cuestiones del problema, ha conllevado a la elaboración de un cuestionario, pues este instrumento fue vital para recaudar datos de todos los integrantes de la muestra de estudio, además con ello se logró afianzar lo planteado respecto al dilema científico.

1.5. Limitaciones de la investigación

No se tuvo ninguna pausa e interrupción del desarrollo de estudio, a medida se tuvieron todas las herramientas para culminar la tesis.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de estudios

Antecedentes internacionales

Peña (2023) estableció a los delitos informáticos o cibernéticos y los perjuicios hacia el sistema financiero en Colombia. El enfoque fue cualitativo, en conclusión, el poblado colombiano se ha visto afectado ante los trayectos incrementados de los delitos informáticos ya que estos afectan los derechos de los usuarios, por otra parte, el uso del internet ha sido útil para el sistema financiero, dado que ha sido factible realizar transacciones mediante el internet o plataforma digitales. Sin embargo, a la misma vez también se ha tenido problemas a causa de los actos delictivos mediante el uso de internet, es decir los delincuentes han cometido delitos informáticos mediante estafas o fraudes cibernéticos, esto ha perjudicado el sistema financiero a medida que los delincuentes cuando llaman telefónicamente a los usuarios se hacen pasar que son agentes de entidades bancarias y financieras, ofreciendo una serie de beneficios para ellos, cuando en realidad son estafas. Entonces, junto al avance tecnológico, los ciberdelitos han estado incrementándose, convirtiéndose en una problemática de seguridad el sistema colombiano por este fenómeno, siendo el fraude el delito de mayor concurrencia. Esta situación obliga al Estado a tomar medidas para promover seguridad a los usuarios, así como también la búsqueda de contar con una eficiente política criminal para sancionar los hechos delictivos provenientes de los delitos informáticos.

Carriedo (2022) ha enfatizado a los delitos informáticos y la tutela de derechos humanos en México. Se emplearon datos cuantitativos y cualitativos, cuya conclusión de estudio ha determinado que, la regulación de delitos informáticos ha estado tipificado dentro del regímenes penales, ya que se hizo necesario contar con directrices para proteger los datos personales de los usuarios, dado que ello forma

parte de los derechos humanos, por ello, el los códigos penales de cada Estado en México expresan la sanción hacia los sujetos que concurren en delitos informáticos. Ha sido fundamental tipificar las conductas que refieren los delitos informáticos a fin de lograr una armonía con los derechos humanos dentro de todo el territorio mexicano.

Paguay (2020) ha realizado estudios sobre las compras a través de internet y los delitos informáticos en Ecuador. Se estableció el método científico, el diseño fue no experimental, se utilizó encuestas para recolectar datos y el enfoque fue cuantitativo. En conclusión, en Ecuador existen millones de personas que cuentan con el uso de internet por medio de computadores o telefonía celular, con ello pueden ejercer compras a través del internet, sin embargo, lamentablemente también están expuestas a ser víctimas de los ciberdelitos o delitos informáticos, por lo que los usuarios requieren una adecuada protección del Estado, es así que para evitar que se vulneren sus derechos constitucionales dentro de las redes, es que se tiene que regular la esencia de delitos informáticos, en internet los usuarios ya sean vendedores o compradores ambos puedan defraudar, es decir el que defrauda es el que comete delito, pero que ello no está regulado en el Código Penal ecuatoriano para sancionar a los que ofrecen productos y reciben dinero sin entregar el bien o a la inversa de que reciben el bien y no depositan el dinero, no obstante, difícilmente se ha reprimido penalmente a los compradores, de modo que esta evidenciado la necesidad de reglamentar adecuadamente los delitos informáticos para que no quede ninguna impunidad.

Antecedentes nacionales

Trucios (2023) ha manifestado a los delitos informáticos o ciberdelincuencia y la captación de menores. Cuya exploración fue de tipo básica y el enfoque

cuantitativo, se tuvo una cifra de 0,949 de fiabilidad y en la prueba de hipótesis cada premisa alternativa fue aceptada. En conclusión, los delitos informáticos son tendencias vigentes que están afectando a la sociedad, estando la captación de menores por medio de comunicaciones electrónicas, cuyo fin del sujeto infractores es captar a un menor de edad para fines de explotación laboral, sexual y otras índoles. Todo ello mediante medios electrónicos que determinan la captación de menores. Por tanto, urge la puesta en marcha inmediata de políticas públicas que puedan confrontar a los delitos informáticos y evitar que más menores de edad sean víctimas de la ciberdelincuencia.

Ocupa (2022) ha enfatizado a los delitos informáticos y la aplicación del convenio Budapest. Se empleó un método de tipo básico, se utilizaron teorías fundamentadas con miras a generar teorías inductivamente mediante datos recopilados, con ello se obtuvo un entendimiento más detallado y abundante de los fenómenos estudiados, por último, el enfoque empleado fue cualitativo. En conclusión, la aplicación del convenio Budapest dentro del sistema peruano, ha sido importantísimo para fortalecer los planeamientos sobre la lucha contra los delitos informáticos o ciberdelincuencia. De una manera que, mediante la adopción de leyes y regulaciones concretas, fue viable tipificar y sancionar los delitos cibernéticos, de tal manera que se llevó a cabo la protección de la privacidad de cada usuario junto con la seguridad de la información. Por lo demás, el uso de esta directriz supranacional ha facilitado la cooperación con otras naciones a fin de luchar contra la ciberdelincuencia, conllevando a la concreción de cambios radicales en la sanción penal contra los acusados ante dichos delitos cibernéticos. Más aún que, la esta integración del Convenio de Budapest dentro del territorio peruano ha dado pasos

significativos para combatir los delitos informáticos, garantizando la seguridad en el ámbito digital.

Sotomayor (2022) ha planteado los delitos informáticos y la calificación fiscal en el distrito fiscal de Lima Centro. El diseño de investigación fue cimentado por medio de la teoría fundamentada, se tuvo la guía de entrevista y el enfoque fue cualitativo. En conclusión, se tuvo que mediante la calificación fiscal que se realiza en los delitos informáticos, estos no fueron calificados de forma correcta para definir como tal la concurrencia del delito investigado, pero que además de ello, este se desnaturalizaba y se desarrollaba otro delito al término de las investigaciones, como ejemplo de ello se ponía en marcha la calificación de la noticia criminal como delito informático, si embargo, al finalizar dicho procedimiento se terminaba formalizando por hurto agravado. De esta formaba se determinó que no ha existido la adecuada calificación de los delitos informáticos, en consecuencia, es importante la creación de fiscalías especializadas en ciberdelincuencia, además que la Ley N° 30096 debe ser fortalecida íntegramente para poder dar batallar a los delitos informáticos o ciberdelincuencia.

2.2. Bases teóricas y científicas

Este segmentó dogmático está representado por conjeturas relacionadas a la investigación.

Teoría del delito

Villavicencio (2017) ha manifestado que:

> La teoría del delito tiene como objeto analizar y estudiar los presupuestos jurídicos de la punibilidad de un comportamiento humano ya sea a través de una acción o de una omisión, del cual se deriva la posibilidad de aplicar una consecuencia jurídico penal. Esta teoría señala además los elementos del

delito siendo la acción, tipicidad, antijuricidad y culpabilidad. Estos elementos representan la estructura del delito. (p. 55)

Teoría absoluta de la pena

Villavicencio (2017) puso de manifiesto que:

> Esta teoría afirma que la pena halla su justificación en sí misma, sin que pueda ser considerada como un medio para fines ulteriores. "Absoluta" porque en esta teoría el sentido de la pena es independiente de su efecto social, se "suelta" de él. La pena es una reacción frente al delito, se consideraba que el mal no debe quedar sin castigo y que el autor de un actuar prohibido debía encontrar en este su merecido. De modo que, la pena se basa en la restitución de valores absolutos, como lo es la justicia, es así, que consideran a este valor como el único que otorga sentido y fundamento a la pena. Así pues, con el fin de restablecer la justicia, la pena es concebida como una retribución a establecer frente al delito cometido, lo que se traduce en ocasionarle un mal a un individuo que compense el mal que ha causado libremente, equilibrándose así la culpabilidad del autor. (p. 25)

Teoría de la política criminal

Borja (2003) ha expuesto que:

> La política criminal es el conjunto de respuestas que el Estado adopta para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción. La política criminal consiste en todas aquellas estrategias, instrumentos y acciones por parte del Estado con miras a prevenir y combatir delitos para afianzar la seguridad social. (p. 130)

Triangulación teórica

Se analizaron las perspectivas de cada teoría expuesta.

Tabla 1

Teorías planteadas

Teorías planteadas	
1.- Teoría del delito	Determina la existencia de elementos que configuran la concurrencia de un delito.
2.- Teoría absoluta de la pena	Cada sanción formulada y ejecutada por la jurisdicción penal, representa a la potestad punitiva del Estado.
3.- Teoría de la política criminal	Es un conjunto de estrategias y medidas para combatir y prevenir la ola de delincuencia.

Tabla 2

Interpretación cada premisa

Interpretación	
1.- Teoría del delito	El delito es una acción punible porque va en contra de lo establecido por la ley.
2.- Teoría absoluta de la pena	Toda sanción, reprehensión o pena impuesta por el juez penal es un castigo al delincuente que cometió un delito.
3.- Teoría de la política criminal	Este postulado se orienta a la búsqueda de hacer frente a los delitos a fin de reducir y prevenir la concurrencia de ellos. Siendo necesario evaluar, planificar y fiscalizar las medidas tomadas por la gubernatura.

Tabla 3

Nexos de cada premisa

Nexos	
1.- Teoría del delito	Existe nexos de esta teoría con la presente tesis.
2.- Teoría absoluta de la pena	Existe nexos con el presente estudio.

3.- Teoría de la política criminal	Existe nexos de esta teoría con esta exploración, por ser un conjunto idóneo de medidas legislativas.

Tabla 4

Contrastación de cada premisa

Contrastación	
1.- Teoría del delito	Determina la existencia de elementos que configuran la concurrencia de un delito. A tal efecto, queda claro la inexistencia de contraste del estudio con este postulado.
2.- Teoría absoluta de la pena	Cada penalidad, reprehensión o sanción se interpreta como la respuesta del Estado ante el delito cometido por el delincuente. A tal efecto, queda claro la inexistencia de contraste del estudio con esta teoría.
3.- Teoría de la política criminal	Es un conjunto de estrategias y medidas para combatir y prevenir la ola de delincuencia. A tal efecto, queda claro la inexistencia de contraste del estudio con esta teoría.

Tabla 5

Premisa seleccionada

Premisa seleccionada	
3.- Teoría de la política criminal	No cabe duda que la política criminal buscar la armonía social de la sociedad por medio de medidas y estrategias que emplea el Estado, para prevenir y combatir la ola de delitos.

Tabla 6

Cambios planteados

Reformulación

3.- Teoría de la política criminal	Este postulado científico es esencial para que el Estado pueda crear medidas y estrategias para suprimir la delincuencia. Ahora bien, respecto al problema de los delitos informáticos, la teoría de la política criminal ha desempeñado un rol vital, ya que se ha logrado determinar que la solución idónea al problema de los delitos informáticos es que el Estado debe crear una Política Nacional De Ciberseguridad, puesto con ello se tendrán todas las medidas de prevenciones para evitar que más personas sean víctimas de los delitos informáticos o ciberdelincuencia. Además, con esta medida se buscará también mantener la seguridad ciudadana, sobre todo que todo usuario tendrá la protección integra de sus datos en todo momento y en cooperación con la Ley de Delitos Informáticos se buscará sancionar las conductas punibles de los ciberdelincuentes.

2.3. Definición conceptual de la terminología empleada

Delitos informáticos

Los delitos informáticos son conductas punibles ejercidas por los delincuentes por medio de programas informáticos.

Datos personales

Es toda información relativa hacia una persona identificada o identificable.

Persecución penal

Es la acción ejercida por el ius puniendi para buscar reprimir las conductas punibles cometidas por delincuentes.

Determinación de la pena

Toda sanción impuesta por el Estado, es determinada por el juez penal ante el delito cometido por el delincuente.

Política criminal

Es un conjunto de estrategias para combatir y prevenir la ola de delincuencia.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Tipo y diseño de investigación

Tipo de investigación

El tipo de investigación utilizada fue básica, a medida que Gallardo (2017) ha determinado que: “Este tipo de estudio tiene por objetivo arribar o transformar teorías existentes o principios, con ello se logra incrementar los conocimientos adquiridos” (p. 17).

Por lo demás, el enfoque planteado fue cuantitativo, ya que Vara (2015) expuso que: “El enfoque cuantitativo emplea una secuencia de datos para ser analizados estadísticamente, con ello se busca establecer la magnitud del problema, además de contrastar las hipótesis” (p. 241).

Diseño de investigación

El diseño de investigación utilizado es correlacional, dado que, Hernández et al. (2014) sostuvieron que: “Este diseño ha sido planteado para establecer la correlación de las variables usando datos estadísticos” (p. 158).

Adicionalmente, se tuvo un diseño no experimental, por cuanto, Hernández et al. (2014) informaron que: “Este diseño abarca que no se manipule ninguna variable de estudio” (p. 152).

3.2. Población y muestra

Población

La población estuvo conformada por 134 individuos, de los cuales 34 fueron especialistas de La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú DIVINDAP PNP y 100 abogados especialistas en derecho informático que ejercen labor en Lima Metropolitana, en total la población fue de 134 individuos.

Muestra

La muestra es solo una parte de la población con la cual se trabaja en la investigación.

Muestreo

Para establecer la muestra se empleó el muestreo probabilístico, dado que Vara (2015) informo que: “Este muestreo determina que todos los sujetos que integran la población tienen la misma posibilidad de ser parte de la muestra de estudio” (p. 264).

Por ello, se emplea la fórmula para muestras finitas.

Población: 134

Nivel de confianza: 95%

Posibilidad de Error: 5 %

Tamaño de la muestra: 100

Figura 1

Fórmula empleada

$$n = \frac{Z^2 (p*q)}{e^2 + \frac{(Z^2 (p*q))}{N}}$$

N= Tamaño de la muestra

Z= Nivel de confianza deseado

P= Proporción de la población con la característica deseada (éxito)

Q= Proporción de la población con la característica deseada (fracaso)

E= Nivel de error dispuesto a ejercer

N= Tamaño de la población

Determinación

Al haberse empleado el muestreo probabilístico junto con la fórmula para muestra finitas, se tuvo la obtención de una muestra de 100 individuos.

3.3. Hipótesis

Gallardo (2017) informo que “Las hipótesis son conjeturas y posibles repuestas a los problemas planteados en una investigación” (p. 48).

Hipótesis general

Hi: Existe relación entre los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana.

Hipótesis específica 1

Hi: Existe relación entre el sabotaje informático y el derecho a la intimidad.

Hipótesis específica 2

Hi: Existe relación entre el acceso a base de datos y el derecho al honor.

3.4. Variables – Operacionalización

Se tuvieron las siguientes variables:

Variable 1: Delitos informáticos

Variable 2: Protección de datos

Operacionalización

Tabla 7

Variable 1: Delitos informáticos

Variable	Definición conceptual	Dimensiones	Indicadores	Ítems	Escala Dicotómica
V.1 Delitos informáticos	Son conductas punibles ejercidas por los delincuentes por medio de programas informáticos.	Sabotaje informático	Espionaje informático	1.- ¿Considera usted que el espionaje informático afecta la protección de datos personales de la víctima?	Si/No
			Programas informáticos	2.- ¿Considera usted que la reproducción no autorizada de programas informáticos afecta los datos personales de la víctima?	
		Acceso a base de datos	Afecta	3.- ¿Considera usted que el acceso no autorizado a base de datos afecta los datos personales de la víctima?	
			Daño	4.- ¿Considera usted que el daño a base de datos afecta los datos personales de la víctima?	

Tabla 8

Variable 2: Protección de datos

Variable	Definición conceptual	Dimensiones	Indicadores	Ítems	Escala Dicotómica
V.2 Protección de datos	Es el conjunto de medidas que se ejerce con miras a y proteger los datos de carácter personal.	Derecho a la intimidad	Privacidad	1.- ¿Considera usted que el derecho a la privacidad personal se ve vulnerado por la comisión de delitos informáticos?	Si/No
			Confidencialidad	2.- ¿Considera usted que la confidencialidad personal se ve vulnerada por la comisión de delitos informáticos?	
		Derecho al honor	Dignidad	3.- ¿Considera usted que la dignidad personal se ve vulnerada por la comisión de delitos informáticos?	
			Reputación	4.- ¿Considera usted que la reputación personal se ve vulnerada por la comisión de delitos informáticos?	

3.5. Métodos y técnicas de investigación

Métodos

Se tuvo un método deductivo para recopilar información desde el ámbito general hacia llegar a lo particular.

Técnicas

Se tuvo a la encuesta para recabar información de la muestra.

Instrumentos

Se tuvo al cuestionario para albergar preguntas de escala dicotómica, con ello se puso dar inicio al diagnóstico u evaluación de la estrategia científica.

3.6. Procesamiento de los datos

Este trámite fue consumado teniendo en cuenta los resultados obtenidos, para ello se analizaron numéricamente en función al porcentaje obtenido en la escala dicotómica.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE DATOS

4.1. Análisis de fiabilidad de las variables

Se tuvo al Alfa de Cronbach para medir la fiabilidad, en ese sentido Vara (2015) ha definido que: “El Alfa de Cronbach forma parte un estudio cuantitativo, por ser un coeficiente que buscar establecer fiabilidad para demostrar que el procedimiento empleado es válido y consistente” (pp. 394-395).

Tabla 9

Cifras estadísticas

Alfa de Cronbach	Calificación científica
> 0.90	Se establece como un valor Excelente
> 0.80	Se establece como un valor Altamente confiable
> 0.70	Se establece como un valor Confiable
> 0. 60	Se establece como un valor Cuestionable
> 0.50	Se establece como un valor Inaceptable

Tabla 10

Cifras estadísticas de fiabilidad

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
0,950	8

Interpretación

Los datos obtenidos han mostrado que existe una rotunda fiabilidad al tenerse un rango de 0,950 de Alfa de Cronbach, lo cual determina que el procedimiento empleado es totalmente valido, calificándose como “Excelente”.

Esta secuencia se ha debido a que inicialmente la formulación de interrogantes del cuestionario, ha tenido una relevante congruencia y consistencia para que los datos obtenidos hayan salido confiables, además que con ello las secuencias estadísticas han promovido la obtención de la medición del problema para poder predecir y formular alguna solución que permita remediar los problemas expuestos y analizados.

4.2. Resultados descriptivos de las dimensiones con la variable

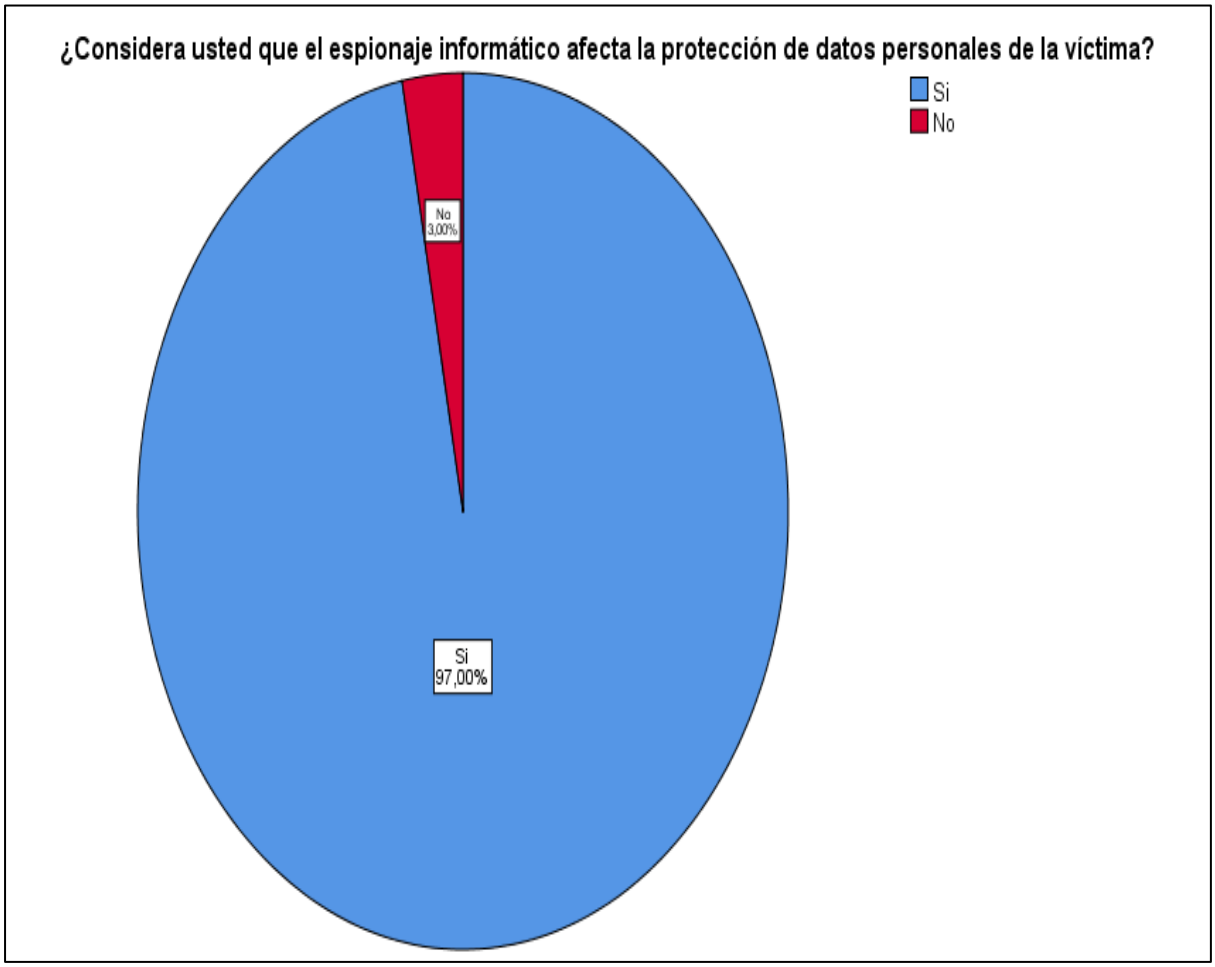
Tabla 11

Cifras estadísticas del instrumento que mide el ítem 1

		Proporción	Cifra porcentual
Válido	Si	97	97,0
	No	3	3,0
	Total	100	100,0

Figura 2

Cifras estadísticas del instrumento que mide el ítem 1



Interpretación

Los datos obtenidos han mostrado la presencia de un 97,0% de encuestados que optaron por establecer una respuesta afirmativa respecto al ítem planteado, a la inversa del mismo ítem, el 3,0% tuvo una respuesta negativa.

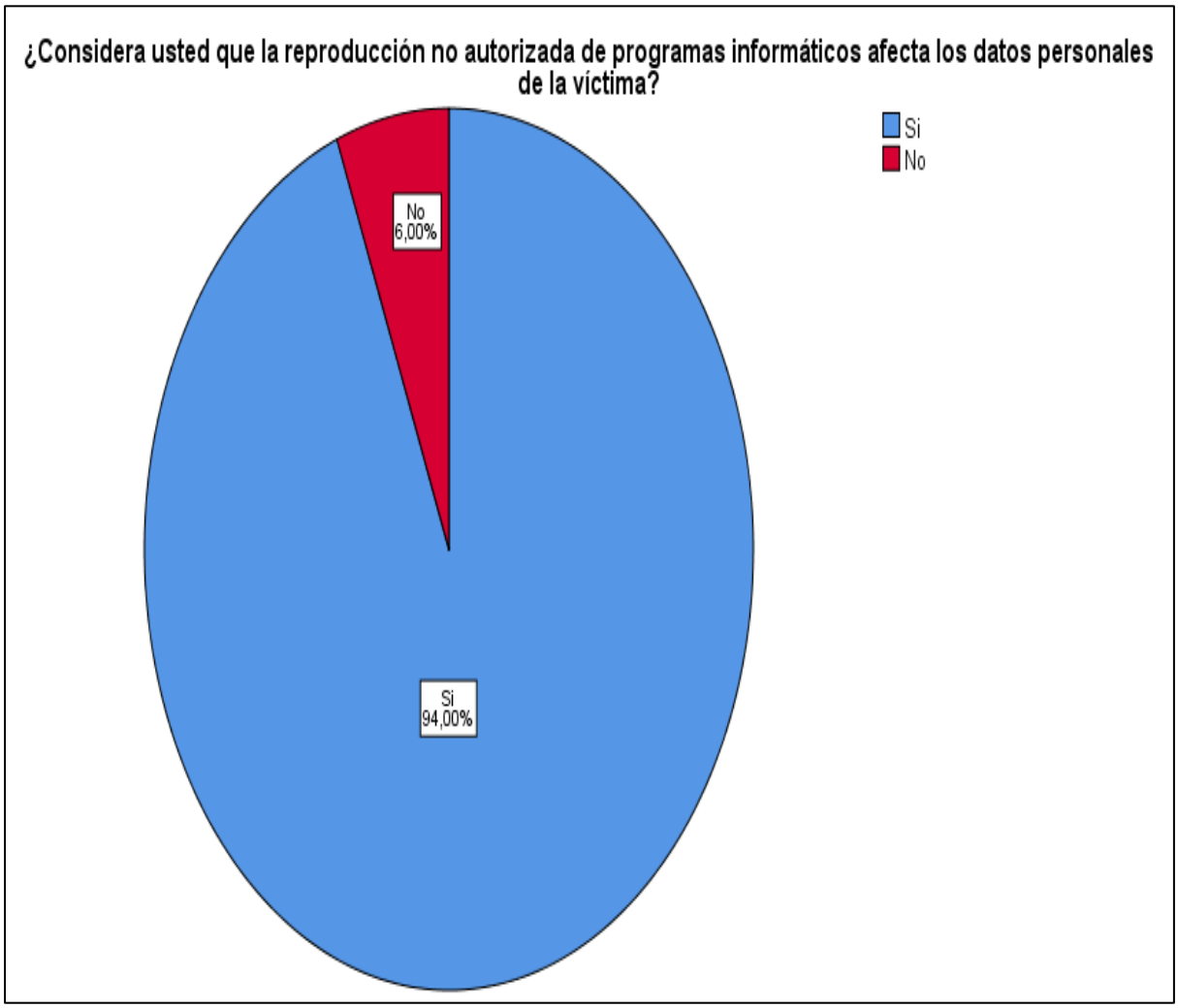
Tabla 12

Cifras estadísticas del instrumento que mide el ítem 2

		Proporción	Cifra porcentual
Válido	Si	94	94,0
	No	6	6,0
	Total	100	100,0

Figura 3

Cifras estadísticas del instrumento que mide el ítem 2



Interpretación

Los datos obtenidos han mostrado la presencia de un 94,0% de encuestados que optaron por establecer una respuesta afirmativa respecto al ítem planteado, a la inversa del mismo ítem, el 6,0% tuvo una respuesta negativa.

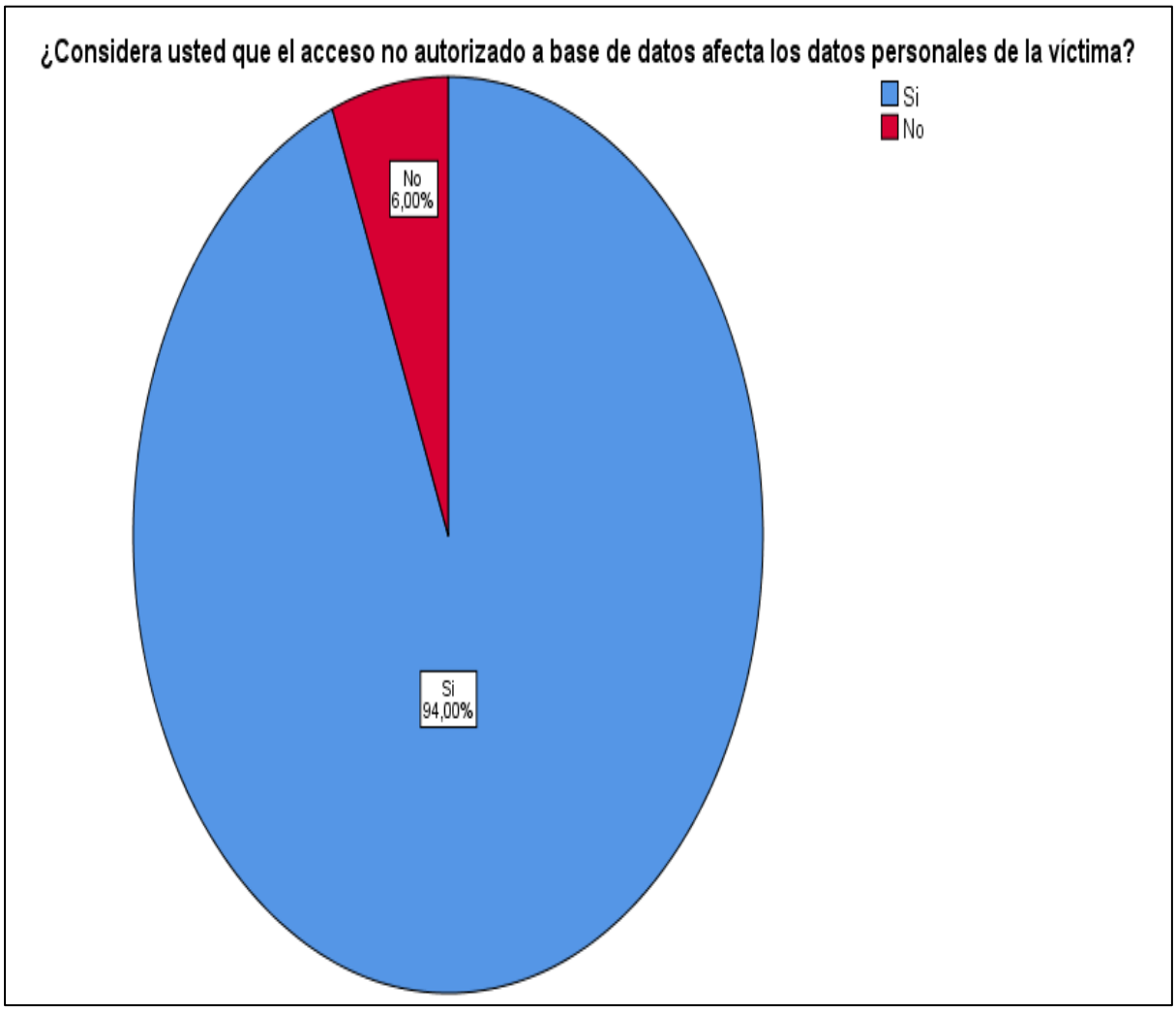
Tabla 13

Cifras estadísticas del instrumento que mide el ítem 3

		Proporción	Cifra porcentual
Válido	Si	94	94,0
	No	6	6,0
	Total	100	100,0

Figura 4

Cifras estadísticas del instrumento que mide el ítem 3



Interpretación

Los datos obtenidos han mostrado la presencia de un 94,0% de encuestados que optaron por establecer una respuesta afirmativa respecto al ítem planteado, a la inversa del mismo ítem, el 6,0% tuvo una respuesta negativa.

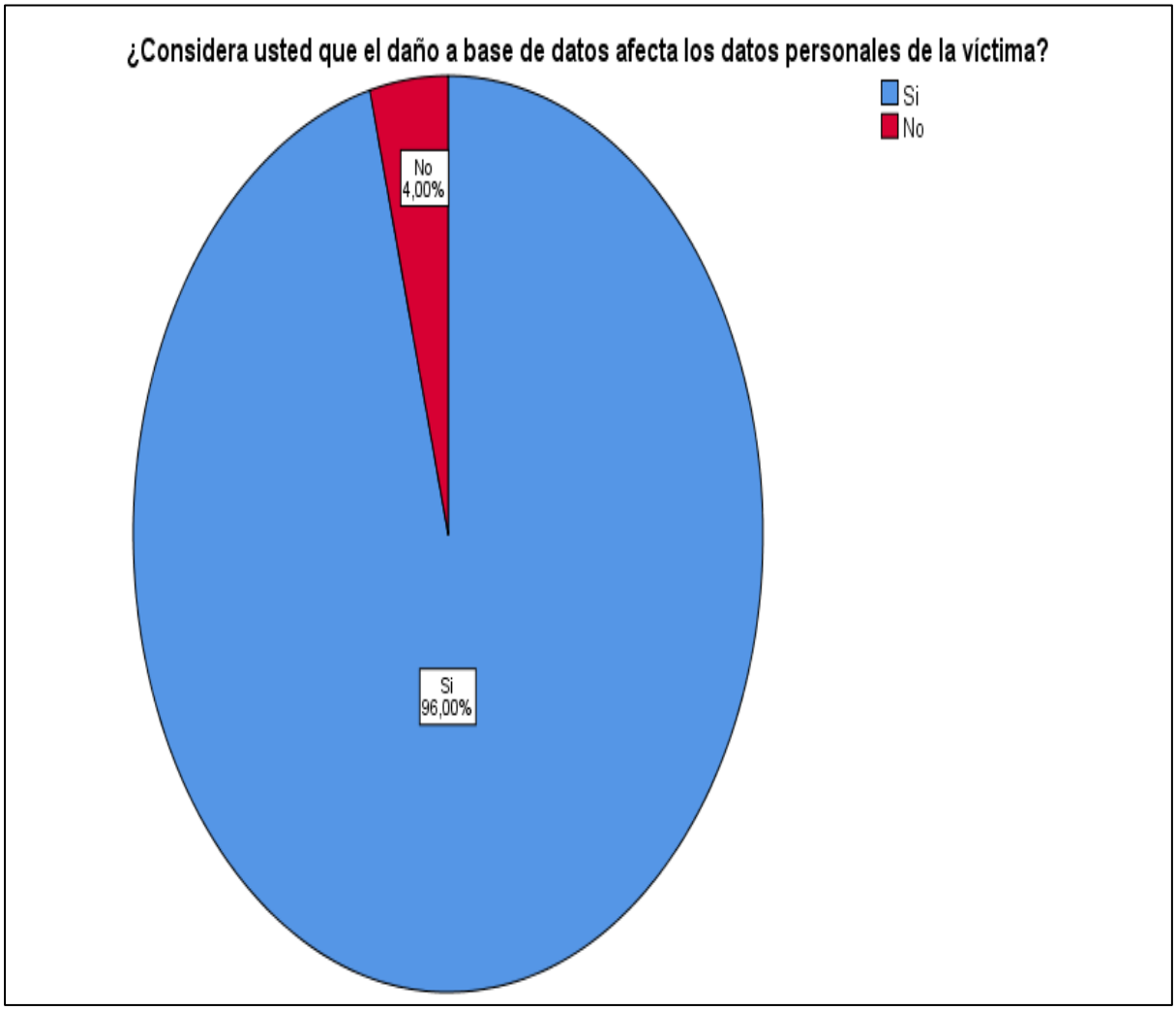
Tabla 14

Cifras estadísticas del instrumento que mide el ítem 4

		Proporción	Cifra porcentual
Válido	Si	96	96,0
	No	4	4,0
	Total	100	100,0

Figura 5

Cifras estadísticas del instrumento que mide el ítem 4



Interpretación

Los datos obtenidos han mostrado la presencia de un 96,0% de encuestados que optaron por establecer una respuesta afirmativa respecto al ítem planteado, a la inversa del mismo ítem, el 4,0% tuvo una respuesta negativa.

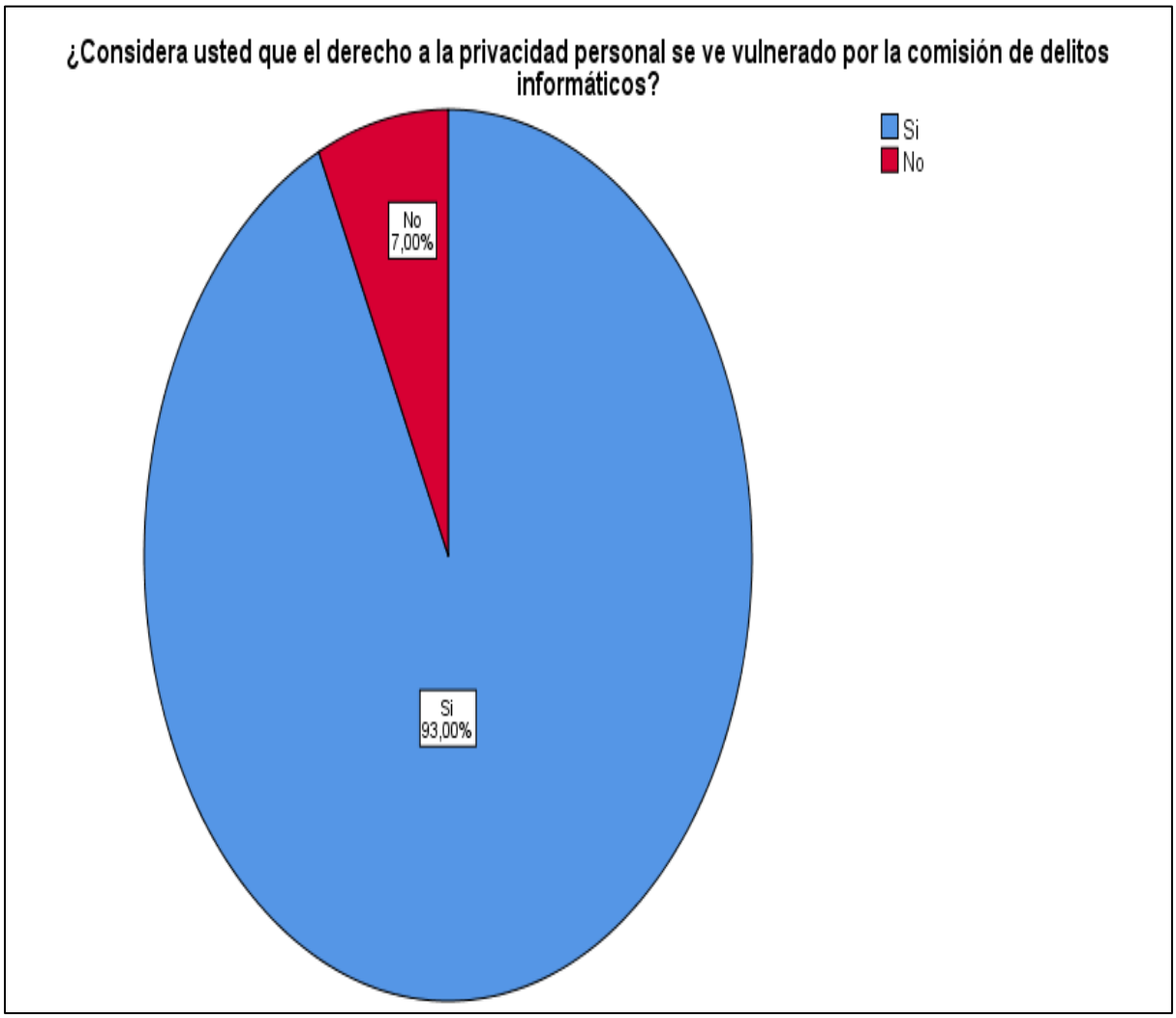
Tabla 15

Cifras estadísticas del instrumento que mide el ítem 5

		Proporción	Cifra porcentual
Válido	Si	93	93,0
	No	7	7,0
	Total	100	100,0

Figura 6

Cifras estadísticas del instrumento que mide el ítem 5



Interpretación

Los datos obtenidos han mostrado la presencia de un 93,0% de encuestados que optaron por establecer una respuesta afirmativa respecto al ítem planteado, a la inversa del mismo ítem, el 7,0% tuvo una respuesta negativa.

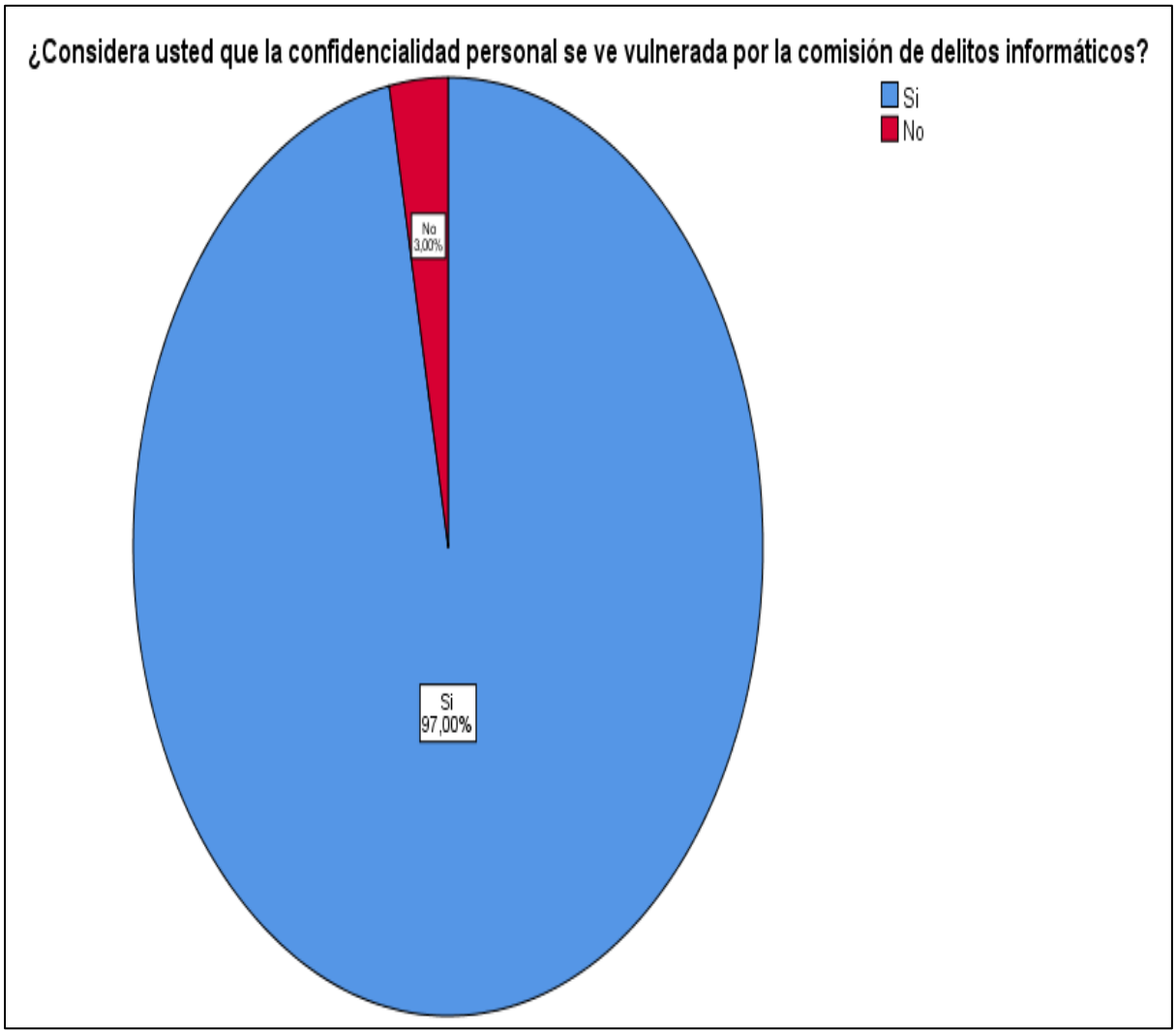
Tabla 16

Cifras estadísticas del instrumento que mide el ítem 6

		Proporción	Cifra porcentual
Válido	Si	97	97,0
	No	3	3,0
	Total	100	100,0

Figura 7

Cifras estadísticas del instrumento que mide el ítem 6



Interpretación

Los datos obtenidos han mostrado la presencia de un 97,0% de encuestados que optaron por establecer una respuesta afirmativa respecto al ítem planteado, a la inversa del mismo ítem, el 3,0% tuvo una respuesta negativa.

Tabla 17

Cifras estadísticas del instrumento que mide el ítem 7

		Proporción	Cifra porcentual
Válido	Si	99	99,0
	No	1	1,0
	Total	100	100,0

Figura 8

Cifras estadísticas del instrumento que mide el ítem 7

Interpretación

Los datos obtenidos han mostrado la presencia de un 99,0% de encuestados que optaron por establecer una respuesta afirmativa respecto al ítem planteado, a la inversa del mismo ítem, el 1,0% tuvo una respuesta negativa.

Tabla 18

Cifras estadísticas del instrumento que mide el ítem 8

		Proporción	Cifra porcentual
Válido	Si	97	97,0
	No	3	3,0
	Total	100	100,0

Figura 9

Cifras estadísticas del instrumento que mide el ítem 8

Interpretación

Los datos obtenidos han mostrado la presencia de un 97,0% de encuestados que optaron por establecer una respuesta afirmativa respecto al ítem planteado, a la inversa del mismo ítem, el 3,0% tuvo una respuesta negativa.

4.3. Contrastación de hipótesis

Se empleo el coeficiente de Spearman, toda vez que, Mondragón (2014) informo que: “El coeficiente de Spearman está identificado como un instrumento tendiente a contrastar las hipótesis mediante cifras numéricas que determinan la correlación de variables y dimensiones” (pp. 98-99).

Tabla 19

Datos numéricos de correlación

Valor de rho	Interpretación
-0.91 a -1.00	Correlación negativa perfecta
-0.76 a -0.90	Correlación negativa muy fuerte
-0.51 a -0.75	Correlación negativa considerable
-0.11 a -0.50	Correlación negativa media
-0.01 a -0.10	Correlación negativa débil
0.00	No existe correlación
+0.01 a +0.10	Correlación positiva débil
+0.11 a +0.50	Correlación positiva media
+0.51 a +0.75	Correlación positiva considerable
+0.76 a +0.90	Correlación positiva muy fuerte
+0.91 a +1.00	Correlación positiva perfecta

Nota. De Mondragón, 2014.

Hipótesis general

Hi: Existe relación entre los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana.

Ho: No existe relación entre los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana.

Tabla 20

Cifras estadísticas de la hipótesis general

Correlaciones				
			V1	V2
V1		Coeficiente de correlación	1,000	0,926**
		Sig. (bilateral)	.	0,000

Rho de Spearman	V2	N	100	100
		Coeficiente de correlación	0,926**	1,000
		Sig. (bilateral)	0,000	.
		N	100	100

**. La correlación es significativa en el nivel 0,01 (bilateral).

Interpretación

Los datos obtenidos han mostrado la presencia de una correlación positiva perfecta entre las variables a medida que los valores de Spearman previsto en la figura 10, lo aclamaron como tal pues el coeficiente de correlación obtenido fue de 0,926 y la Sig. (bilateral) de 0,000. Ante tal situación se ha determinado en rechazar la hipótesis nula.

Hipótesis específica 1

Hi: Existe relación entre el sabotaje informático y el derecho a la intimidad.

Ho: No existe relación entre el sabotaje informático y el derecho a la intimidad.

Tabla 21

Cifras estadísticas de la hipótesis específica 1

Correlaciones

			Variable 1 Dimensión 1	Variable 2 Dimensión 1
Rho de Spearman	Variable 1 Dimensión 1	Coeficiente de correlación	1,000	0,641**
		Sig. (bilateral)	.	0,000
		N	100	100
	Variable 2 Dimensión 1	Coeficiente de correlación	0,641**	1,000
		Sig. (bilateral)	0,000	.
		N	100	100

**. La correlación es significativa en el nivel 0,01 (bilateral).

Interpretación

Los datos obtenidos han mostrado la presencia de una correlación positiva considerable entre las dimensiones a medida que los valores de Spearman previsto en la figura 10, lo aclamaron como tal pues el coeficiente de correlación obtenido fue

de 0,641 y la Sig. (bilateral) de 0,000. Ante tal situación se ha determinado en rechazar la hipótesis nula.

Hipótesis específica 2

Hi: Existe relación entre el acceso a base de datos y el derecho al honor.

Ho: No existe relación entre el acceso a base de datos y el derecho al honor.

Tabla 22

Cifras estadísticas de la hipótesis específica 2

Correlaciones

			Variable 1 Dimensión 2	Variable 2 Dimensión 2
Rho de Spearman	Variable 1 Dimensión 2	Coeficiente de correlación	1,000	0,398**
		Sig. (bilateral)	.	0,000
		N	100	100
	Variable 2 Dimensión 2	Coeficiente de correlación	0,398**	1,000
		Sig. (bilateral)	0,000	.
		N	100	100

**. La correlación es significativa en el nivel 0,01 (bilateral).

Interpretación

Los datos obtenidos han mostrado la presencia de una correlación positiva media entre las dimensiones a medida que los valores de Spearman previsto en la figura 10, lo aclamaron como tal pues el coeficiente de correlación obtenido fue de 0,398 y la Sig. (bilateral) de 0,000. Ante tal situación se ha determinado en rechazar la hipótesis nula.

CAPÍTULO V

DISCUSIONES, CONCLUSIONES Y RECOMENDACIONES

5.1. Discusiones

En la hipótesis general se ha logrado hacer valer que, existe relación entre los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana. La razón de tal suceso fue porque se tuvo un rango de correlación de 0,926 y una significación bilateral de 0,000. Estos manifestados sucesos han tenido protagonismos y notoriedad con los hallazgos de Ocupa (2022) quien ha enfatizado a los delitos informático y la aplicación del convenio Budapest. Cuya determinación ha hecho mención que, la aplicación del convenio Budapest dentro del sistema peruano, ha sido de amplia magnitud y relieve con miras a fortalecer los planeamientos sobre la lucha contra los delitos informáticos o ciberdelincuencia. De una manera que, mediante la adopción de leyes y regulaciones concretas, fue viable tipificar y sancionar los delitos cibernéticos, de tal manera que se llevó a cabo la protección de la privacidad de cada usuario junto con la seguridad de la información. Por lo demás, el uso de esta directriz supranacional ha facilitado la cooperación con otras naciones a fin de luchar contra la ciberdelincuencia, conllevando a la concreción de cambios radicales en la sanción penal contra los acusados ante dichos delitos cibernéticos. Más aún que, la esta integración del Convenio de Budapest dentro del territorio peruano ha dado pasos significativos para combatir los delitos informáticos, garantizando la seguridad en el ámbito digital.

En la hipótesis específica 1 se ha logrado hacer valer que, existe relación entre el sabotaje informático y el derecho a la intimidad. La razón de tal suceso fue porque se tuvo un rango de correlación de 0,641 y una significación bilateral de 0,000. Estos manifestados sucesos han tenido protagonismos y notoriedad con los hallazgos de Carriedo (2022) quien ha enfatizado a los delitos informáticos y la tutela de derechos humanos en México. Cuya conclusión de estudio ha determinado que, la regulación

de delitos informáticos ha estado tipificado dentro del regímenes penales, ya que se hizo necesario contar con directrices para proteger los datos personales de los usuarios, dado que ello forma parte de los derechos humanos, por ello, el los códigos penales de cada Estado en México expresan la sanción hacia los sujetos que concurren en delitos informáticos. Ha sido fundamental tipificar las conductas que refieren los delitos informáticos a fin de lograr una armonía con los derechos humanos dentro de todo el territorio mexicano.

En la hipótesis específica 2 se ha logrado hacer valer que, existe relación entre el acceso a base de datos y el derecho al honor. La razón de tal suceso fue porque se tuvo un rango de correlación de 0,398 y una significación bilateral de 0,000. Estos manifestados sucesos han tenido protagonismos y notoriedad con los hallazgos de Peña (2023) quien estableció a los delitos informáticos o cibernéticos y los perjuicios hacia el sistema financiero en Colombia. Cuya conclusión ha manifestado que, existió una afectación al poblado integró ante el patrón incrementado de los delitos informáticos ya que estos afectan los derechos de los usuarios, por otra parte, el uso del internet ha sido útil para el sistema financiero, dado que ha sido factible realizar transacciones mediante el internet o plataforma digitales. Sin embargo, a la misma vez también se ha tenido problemas a causa de los actos delictivos mediante el uso de internet, es decir los delincuentes han cometido delitos informáticos mediante estafas o fraudes cibernéticos, esto ha perjudicado el sistema financiero a medida que los delincuentes cuando llaman telefónicamente a los usuarios se hacen pasar que son agentes de entidades bancarias y financieras, ofreciendo una serie de beneficios para ellos, cuando en realidad son estafas. Entonces, junto al avance tecnológico, los ciberdelitos han estado incrementándose, convirtiéndose en una problemática de seguridad el sistema colombiano por este fenómeno, siendo el fraude

el delito de mayor concurrencia. Esta situación obliga al Estado a tomar medidas para promover seguridad a los usuarios, así como también la búsqueda de contar con una eficiente política criminal para sancionar los hechos delictivos provenientes de los delitos informáticos.

5.2. Conclusiones

Primera: Los datos obtenidos en la hipótesis general, han mostrado la presencia de una correlación positiva perfecta entre las variables a medida que los valores obtenidos lo aclamaron como tal, pues la correlación obtenida fue de 0,926 y la Sig. (bilateral) de 0,000. Ante tal situación se ha determinado en rechazar la hipótesis nula.

Segunda: Los datos obtenidos en la hipótesis específica 1, han mostrado la presencia de una correlación positiva considerable entre las dimensiones a medida que los valores obtenidos lo aclamaron como tal, pues la correlación obtenida fue de 0,641 y la Sig. (bilateral) de 0,000. Ante tal situación se ha determinado en rechazar la hipótesis nula.

Tercera: Los datos obtenidos en la hipótesis específica 2, han mostrado la presencia de una correlación positiva media entre las dimensiones a medida que los valores obtenidos lo aclamaron como tal, pues la correlación obtenida fue de 0,398 y la Sig. (bilateral) de 0,000. Ante tal situación se ha determinado en rechazar la hipótesis nula. Además, con estas secuencias estadísticas se logró esclarecer la magnitud del problema.

5.3. Recomendaciones

Primera: Para lograr la solución idónea al problema de los delitos informáticos es que el Estado debe crear una Política Nacional De Ciberseguridad, puesto con ello

se tendrán todas las medidas de prevenciones para evitar que más usuarios padezcan de los delitos informáticos o ciberdelincuencia.

Segunda: Es necesario concretar el fortalecimiento de la Ley de Delitos Informáticos a fin de buscar sancionar tajantemente las conductas punibles de los ciberdelincuentes. Y sobre todo para proteger los datos personales de los usuarios.

Tercera: El legislador debe tomar medidas para promover seguridad a los usuarios, así como también la búsqueda de contar con una eficiente política criminal para sancionar los hechos delictivos provenientes de los delitos informáticos.

REFERENCIAS

Álvarez, C. (2023). *Colombia registró un crecimiento de ataques informáticos en el último año*. https://www.vozdeamerica.com/a/colombia-registro-crecimiento-ataques-informaticos-ultimo-ano-/6916577.html#:~:text=Colombia%20registr%C3%B3%20en%202022%20m%C3%A1s,computadoras%2C%20tablets%20y%20tel%C3%A9fonos%20celulares.

Alcalá, M. y Meléndez, M. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. *PAAKAT: Revista de Tecnología y Sociedad, 13*(24), 1-37. https://dialnet.unirioja.es/servlet/articulo?codigo=8956682

Borja, E. (2003). Sobre el concepto de política criminal. Una aproximación a su significado desde la obra de Claus Roxin. *Anuario de derecho penal y ciencias penales, 1*(56), 113-150. https://dialnet.unirioja.es/servlet/articulo?codigo=1217111

Carriedo, L. (2022). *Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México* [Tesis de maestría, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación]. Repositorio Institucional INFOTEC. http://infotec.repositorioinstitucional.mx/jspui/handle/1027/518

Convenio sobre la Ciberdelincuencia. (2001). *El Peruano*. https://static.legis.pe/wp-content/uploads/2019/09/Convenio-sobre-la-Ciberdelincuencia-Legis.pe_.pdf

Defensoría del Pueblo. (2023). *La ciberdelincuencia en el Perú: Estrategias y retos del estado*. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

El Peruano. (2023). *¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú.* https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru#:~:text=21%2F06%2F2023%20Cada%20mes,de%20la%20mitad%20del%20total.

Gallardo, E. (2017). *Metodología de la Investigación: manual autoformativo interactivo*. Universidad Continental.

Hernández, R., Fernández, C. y Baptista, M. (2014). *Metodología de la Investigación*. McGraw-Hill Education.

Ley de Delitos Informáticos. (2013). *Plataforma digital única del Estado Peruano*. https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096

Mondragón, M. (2014). Uso de la correlación de Spearman en un estudio de intervención en fisioterapia. *Movimiento Científico, 8*(1), 98-104. https://dialnet.unirioja.es/servlet/articulo?codigo=5156978

Ocupa, B. (2022). *Aplicación del convenio Budapest y delitos informáticos en el Perú, 2022* [Tesis de maestría, Universidad César Vallejo]. Repositorio Institucio UCV. https://hdl.handle.net/20.500.12692/119930

Paguay, V. (2020). *Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet* [Tesis de pregrado, Universidad Nacional de Chimborazo]. Repositorio Institucional UNACH. http://dspace.unach.edu.ec/handle/51000/7607

Peña, M. (2023). *Delitos Cibernéticos* [Tesis de maestría, Universidad Libre de Colombia]. Repositorio Institucional UNILIBRE. https://hdl.handle.net/10901/24774

Sotomayor, G. (2022). *La calificación fiscal en los delitos informáticos en el distrito fiscal de Lima Centro, 2019 – 2020* [Tesis de maestría, Universidad César Vallejo]. Repositorio Institucional UCV. https://hdl.handle.net/20.500.12692/95834

Trucios, A. (2023). *La ciberdelincuencia y la captación en menores de edad Lima Metropolitana, 2021* [Tesis de pregrado, Universidad Autónoma del Perú]. Repositorio Institucional AUTONOMA. https://hdl.handle.net/20.500.13067/2704

Vara, A. (2015). *7 pasos para elaborar una tesis*. Editorial Macro.

Villavicencio, F. (2017). *Derecho penal básico*. Fondo Editorial PUCP.

ANEXOS

Anexo 1. Matriz de consistencia

Problema general	Objetivo general	Hipótesis general	Variables	Metodología	Población y muestra
¿Cuál es la relación entre los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana?	Determinan cuál es la relación entre los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana.	**Hi:** Existe relación entre los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana. **Ho:** No existe relación entre los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana.	**Variable 1:** Delitos informáticos **Dimensiones:** **Dimensión 1:** Sabotaje informático **Dimensión 2:** Acceso a base de datos	**Tipo de investigación** - Básica pura **Enfoque** - Cuantitativo **Diseño de investigación** - Correlacional - No experimental - Transversal	La población estuvo conformada por 134 individuos, de los cuales 34 fueron especialistas de La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú DIVINDAP PNP y 100 abogados especialistas en derecho informático que ejercen labor en Lima Metropolitana, en total la población fue de 134 individuos. Al haberse empleado el muestreo probabilístico junto con la fórmula para muestra finitas, se tuvo la obtención de una muestra de 100 individuos.
Problemas específicos	**Objetivos específicos**	**Hipótesis específicas**	**Variable 2:** Protección de datos **Dimensiones:** **Dimensión 1:** Derecho a la intimidad **Dimensión 2:** Derecho al honor	**Técnica** - Encuesta **Instrumento** - Cuestionario	
¿Cuál es la relación entre el sabotaje informático y el derecho a la intimidad?	Determinar cuál es la relación entre el sabotaje informático y el derecho a la intimidad.	**Hipótesis específica 1** **Hi:** Existe relación entre el sabotaje informático y el derecho a la intimidad. **Ho:** No existe relación entre el sabotaje informático y el derecho a la intimidad.			
¿Cuál es la relación entre el acceso a base de datos y el derecho al honor?	Determina cuál es la relación entre el acceso a base de datos y el derecho al honor.	**Hipótesis específica 2** **Hi:** Existe relación entre el acceso a base de datos y el derecho al honor. **Ho:** No existe relación entre el acceso a base de datos y el derecho al honor.			

Anexo 2. Operacionalización de variables

Variable	Definición conceptual	Dimensiones	Indicadores	Ítems	Escala Dicotómica
V.1 Delitos informáticos	Son conductas punibles ejercidas por los delincuentes por medio de programas informáticos implantándose virus, suplantación de sitios web, estafas, piratería, violación de derechos de autor, etc.	Sabotaje informático Acceso a base de datos	Espionaje informático Programas informáticos Afecta Daño	1.- ¿Considera usted que el espionaje informático afecta la protección de datos personales de la víctima? 2.- ¿Considera usted que la reproducción no autorizada de programas informáticos afecta los datos personales de la víctima? 3.- ¿Considera usted que el acceso no autorizado a base de datos afecta los datos personales de la víctima? 4.- ¿Considera usted que el daño a base de datos afecta los datos personales de la víctima?	Si/No

Variable	Definición conceptual	Dimensiones	Indicadores	Ítems	Escala Dicotómica
V.2 Protección de datos	Es el conjunto de medidas que se ejerce con miras a y proteger los datos de carácter personal.	Derecho a la intimidad	Privacidad	1.- ¿Considera usted que el derecho a la privacidad personal se ve vulnerado por la comisión de delitos informáticos?	Si/No
			Confidencialidad	2.- ¿Considera usted que la confidencialidad personal se ve vulnerada por la comisión de delitos informáticos?	
		Derecho al honor	Dignidad	3.- ¿Considera usted que la dignidad personal se ve vulnerada por la comisión de delitos informáticos?	
			Reputación	4.- ¿Considera usted que la reputación personal se ve vulnerada por la comisión de delitos informáticos?	

DOCUMENTOS PARA VALIDAR LOS INSTRUMENTOS DE MEDICIÓN A TRAVÉS DE JUICIO DE EXPERTOS

Anexo 3. Carta de presentación

CARTA DE PRESENTACIÓN

Dr. ……..

Coordinador de Investigación de la Escuela Profesional de Derecho

Presente

Asunto: **VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.**

Es grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, en mi calidad de egresada de la Escuela Profesional de Derecho de la Facultad de Ciencias Humanas de la Universidad Autónoma del Perú, presento el instrumento para ser validado del proyecto de investigación titulada: "LOS DELITOS INFORMÁTICOS Y LA VULNERACIÓN DEL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES EN LIMA METROPOLITANA", cuyo desarrollo le permitirá a la tesista, poder optar el Título de Abogada.

En tal sentido, es imprescindible validar el(los) instrumento(s) con los cuales se recogerán los datos pertinentes, para lo cual es necesario contar con la aprobación de especialistas y llevar a cabo la aplicación del(los) instrumento(s) en mención. Conocedor(a) de su connotada experiencia en temas de investigación jurídica, se ha considerado pertinente recurrir a su persona.

El expediente de validación, que le hago llegar contiene lo siguiente:

- Carta de presentación.
- Definición conceptual(es) de la(s) variable(s) y dimensiones.
- Cuestionario.
- Matriz de operacionalización de la(s) variable(s).
- Certificado de validez de contenido de (los) instrumento(s).

Sin otro particular me despido.

Atentamente,

_____

ANABELIZA URDANEGUI RANGEL

DNI N°

DEFINICIÓN CONCEPTUAL DE LAS VARIABLES Y SUS DIMENSIONES

Variable 1: Delitos informáticos

Son conductas punibles ejercidas por los delincuentes por medio de programas informáticos implantándose virus, suplantación de sitios web, estafas, piratería, violación de derechos de autor, etc.

Dimensiones de la variable

Dimensión 1: Sabotaje informático

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Dimensión 2: Acceso a base de datos

Se refiere a la capacidad de recuperar y utilizar datos guardados en una base de datos o en otro sistema de almacenamiento. Abarca diversas actividades, que incluyen la recuperación, la gestión, el análisis y la protección de datos.

Variable 2: Protección de datos

Es el conjunto de medidas que se ejerce con miras a y proteger los datos de carácter personal.

Dimensiones de la variable

Dimensión 1: Derecho a la intimidad

Es un derecho que protege y les permite a las personas tener un espacio privado. Donde cada individuo puede desarrollar su personalidad de forma libre según sus propias convicciones.

Dimensión 2: Derecho al honor

Este derecho protege la valoración que de la persona en cuestión se tenga en su ámbito personal o social.

Operacionalización de variables

Variable	Definición conceptual	Dimensiones	Indicadores	Ítems	Escala Dicotómica
V.1 Delitos informáticos	Son conductas punibles ejercidas por los delincuentes por medio de programas informáticos implantándose virus, suplantación de sitios web, estafas, piratería, violación de derechos de autor, etc.	Sabotaje informático Acceso a base de datos	Espionaje informático Programas informáticos Afecta Daño	1.- ¿Considera usted que el espionaje informático afecta la protección de datos personales de la víctima? 2.- ¿Considera usted que la reproducción no autorizada de programas informáticos afecta los datos personales de la víctima? 3.- ¿Considera usted que el acceso no autorizado a base de datos afecta los datos personales de la víctima? 4.- ¿Considera usted que el daño a base de datos afecta los datos personales de la víctima?	Si/No

Variable	Definición	Dimensiones	Indicadores	Ítems	Escala

	conceptual				**Dicotómica**
V.2 Protección de datos	Es el conjunto de medidas que se ejerce con miras a y proteger los datos de carácter personal.	Derecho a la intimidad	Privacidad	1.- ¿Considera usted que el derecho a la privacidad personal se ve vulnerado por la comisión de delitos informáticos?	Si/No
			Confidencialidad	2.- ¿Considera usted que la confidencialidad personal se ve vulnerada por la comisión de delitos informáticos?	
		Derecho al honor	Dignidad	3.- ¿Considera usted que la dignidad personal se ve vulnerada por la comisión de delitos informáticos?	
			Reputación	4.- ¿Considera usted que la reputación personal se ve vulnerada por la comisión de delitos informáticos?	

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 1: "DELITOS INFORMÁTICOS"

N°	DIMENSIONES/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Suficiencia[4]		Sugerencias
	DIMENSIÓN 1 Sabotaje informático	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera usted que el espionaje informático afecta la protección de datos personales de la víctima?									
2	¿Considera usted que la reproducción no autorizada de programas informáticos afecta los datos personales de la víctima?									
	DIMENSIÓN 2 Acceso a base de datos	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Considera usted que el acceso no autorizado a base de datos afecta los datos personales de la víctima?									
4	¿Considera usted que el daño a base de datos afecta los datos personales de la víctima?									

Observaciones (precisar si hay suficiencia[4]): _____
Opinión de aplicabilidad: Aplicable [ ] Aplicable después de corregir [ ] No aplicable [ ]
Apellidos y nombres del juez validador: Dr. /Mg. /Abog.:…….. **DNI:** ……
Especialidad del validador: ……..

Lima sur,……de……de 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o Dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.
[4]**Suficiencia:** Los ítems son suficientes para medir la dimensión.

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 2: "PROTECCIÓN DE DATOS"

N°	DIMENSIONES/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Suficiencia[4]		Sugerencias
	DIMENSIÓN 1 Derecho a la intimidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera usted que el derecho a la privacidad personal se ve vulnerado por la comisión de delitos informáticos?									
2	¿Considera usted que la confidencialidad personal se ve vulnerada por la comisión de delitos informáticos?									
	DIMENSIÓN 2 Derecho al honor	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Considera usted que la dignidad personal se ve vulnerada por la comisión de delitos informáticos?									
4	¿Considera usted que la reputación personal se ve vulnerada por la comisión de delitos informáticos?									

Observaciones (precisar si hay suficiencia[4]): _____

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

Apellidos y nombres del juez validador: Dr. /Mg. /Abog.:……. **DNI:** ……

Especialidad del validador: ……..

Lima sur,……de……de 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o Dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.
[4]**Suficiencia:** Los ítems son suficientes para medir la dimensión.

Firma del Experto Informante.

FACULTAD DE CIENCIAS HUMANAS

ESCUELA PROFESIONAL DE DERECHO

CUESTIONARIO

Instrucciones:

- Estimado encuestado, el presente instrumento tiene como finalidad obtener el resultado variable de las variables de estudio de la Tesis titulada: “LOS DELITOS INFORMÁTICOS Y LA VULNERACIÓN DEL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES EN LIMA METROPOLITANA”, para lo cual se les hará 8 preguntas en forma de ítems con respuesta bajo una escala de tipo Dicotómica. Tómese su tiempo al responder analicé y evalué cada opción.

INSTRUCCIONES:

A continuación, se presenta 12 preguntas, sobre los cuales usted tendrá dos opciones de respuesta:

1.- SI

2.- No

VARIABLE 1. DELITOS INFORMÁTICOS

SI
NO

Lea atentamente y marque con un “X” la respuesta que usted crea conveniente.

ÍTEMS	SI	NO
1.- ¿Considera usted que el espionaje informático afecta la protección de datos personales de la víctima?		
2.- ¿Considera usted que la reproducción no autorizada de programas informáticos afecta los datos personales de la víctima?		
3.- ¿Considera usted que el acceso no autorizado a base de datos afecta los datos personales de la víctima?		
4.- ¿Considera usted que el daño a base de datos afecta los datos personales de la víctima?		

VARIABLE 2. PROTECCIÓN DE DATOS

SI
NO

Lea atentamente y marque con un “X” la respuesta que usted crea conveniente.

ÍTEMS	SI	NO
1.- ¿Considera usted que el derecho a la privacidad personal se ve vulnerado por la comisión de delitos informáticos?		
2.- ¿Considera usted que la confidencialidad personal se ve vulnerada por la comisión de delitos informáticos?		
3.- ¿Considera usted que la dignidad personal se ve vulnerada por la comisión de delitos informáticos?		
4.- ¿Considera usted que la reputación personal se ve vulnerada por la comisión de delitos informáticos?		

Anexo 4. Validación del instrumento mediante juicio de expertos

Anexo 4.1. Experto N° 1

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 1: "DELITOS INFORMÁTICOS"

N°	DIMENSIONES/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Suficiencia[4]		Sugerencias
	DIMENSIÓN 1 Sabotaje informático	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera usted que el espionaje informático afecta la protección de datos personales de la víctima?	X		X		X		X		
2	¿Considera usted que la reproducción no autorizada de programas informáticos afecta los datos personales de la víctima?	X		X		X		X		
	DIMENSIÓN 2 Acceso a base de datos	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Considera usted que el acceso no autorizado a base de datos afecta los datos personales de la víctima?	X		X		X		X		
4	¿Considera usted que el daño a base de datos afecta los datos personales de la víctima?	X		X		X		X		

Observaciones (precisar si hay suficiencia[4]): _____**Si hay suficiencia**_____

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

Apellidos y nombres del juez validador: Dr. /Mg. /Abog. DR. LUIS ÁNGEL ESPINOZA PAJUELO **DNI:** ……10594662……..

Especialidad del validador: …… MAGISTER EN GESTIÓN PÚBLICA, DOCTOR EN DERECHO……..

Lima sur,……02 de…noviembre……de 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o Dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.
[4]**Suficiencia:** Los ítems son suficientes para medir la dimensión.

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 2: "PROTECCIÓN DE DATOS"

N°	DIMENSIONES/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Suficiencia[4]		Sugerencias
	DIMENSIÓN 1 Derecho a la intimidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera usted que el derecho a la privacidad personal se ve vulnerado por la comisión de delitos informáticos?	X		X		X		X		
2	¿Considera usted que la confidencialidad personal se ve vulnerada por la comisión de delitos informáticos?	X		X		X		X		
	DIMENSIÓN 2 Derecho al honor	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Considera usted que la dignidad personal se ve vulnerada por la comisión de delitos informáticos?	X		X		X		X		
4	¿Considera usted que la reputación personal se ve vulnerada por la comisión de delitos informáticos?	X		X		X		X		

Observaciones (precisar si hay suficiencia[4]): _____**Si hay suficiencia**_____

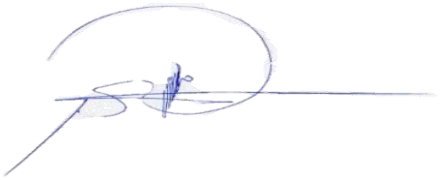
Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Dr. /Mg. /Abog. DR. LUIS ÁNGEL ESPINOZA PAJUELO **DNI:** ……10594662……..

Especialidad del validador: …… MAGISTER EN GESTIÓN PÚBLICA, DOCTOR EN DERECHO……..

Lima sur,……02 de…noviembre……de 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o Dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.
[4]**Suficiencia:** Los ítems son suficientes para medir la dimensión.



Firma del Experto Informante.

Anexo 4.2. Experto N° 2

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 1: "DELITOS INFORMÁTICOS"

N°	DIMENSIONES/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Suficiencia[4]		Sugerencias
	DIMENSIÓN 1 Sabotaje informático	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera usted que el espionaje informático afecta la protección de datos personales de la víctima?	X		X		X		X		
2	¿Considera usted que la reproducción no autorizada de programas informáticos afecta los datos personales de la víctima?	X		X		X		X		
	DIMENSIÓN 2 Acceso a base de datos	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Considera usted que el acceso no autorizado a base de datos afecta los datos personales de la víctima?	X		X		X		X		
4	¿Considera usted que el daño a base de datos afecta los datos personales de la víctima?	X		X		X		X		

Observaciones (precisar si hay suficiencia[4]): _____**Si hay suficiencia** _____
Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]
Apellidos y nombres del juez validador: Dr. /Mg. /Abog.:…MARCOS ENRIQUE TUME CHUNGA **DNI:** …… 41058938
Especialidad del validador:… Maestro en Derecho Penal y Procesal Penal……..

Lima sur,……06…de……11……de 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o Dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.
[4]**Suficiencia:** Los ítems son suficientes para medir la dimensión.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 2: "PROTECCIÓN DE DATOS"

N°	DIMENSIONES/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Suficiencia[4]		Sugerencias
	DIMENSIÓN 1 Derecho a la intimidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera usted que el derecho a la privacidad personal se ve vulnerado por la comisión de delitos informáticos?	X		X		X		X		
2	¿Considera usted que la confidencialidad personal se ve vulnerada por la comisión de delitos informáticos?	X		X		X		X		
	DIMENSIÓN 2 Derecho al honor	**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Considera usted que la dignidad personal se ve vulnerada por la comisión de delitos informáticos?	X		X		X		X		
4	¿Considera usted que la reputación personal se ve vulnerada por la comisión de delitos informáticos?	X		X		X		X		

Observaciones (precisar si hay suficiencia[4]): _____**Si hay suficiencia** _____

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

Apellidos y nombres del juez validador: Dr. /Mg. /Abog.:…MARCOS ENRIQUE TUME CHUNGA **DNI:** …… 41058938

Especialidad del validador:… Maestro en Derecho Penal y Procesal Penal……..

Lima sur,……06…de……11……de 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o Dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.
[4]**Suficiencia:** Los ítems son suficientes para medir la dimensión.

Anexo 5. Consentimiento informado

CONSENTIMIENTO INFORMADO

Institución: Facultad de Ciencias Humanas y de La Salud, Escuela Profesional de Derecho, Universidad autónoma del Perú

Nombre del Investigador(a): ANABELIZA URDANEGUI RANGEL

Título del Proyecto: "LOS DELITOS INFORMÁTICOS Y LA VULNERACIÓN DEL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES EN LIMA METROPOLITANA"

La presente investigación abarca un enfoque cuantitativo y un diseño correlacional no experimental y transversal, y conduce a la exploración de las experiencias vividas, reconociendo el significado y trascendencia de los delitos informáticos y el derecho fundamental de protección de datos personales.

Hola, mi nombre es ANABELIZA URDANEGUI RANGEL, soy estudiante de la Escuela profesional de derecho, de la Universidad Autónoma del Perú, actualmente estoy realizando un estudio acerca de **"LOS DELITOS INFORMÁTICOS Y LA VULNERACIÓN DEL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES EN LIMA METROPOLITANA",** para ello ante su connotada experiencia en la temática de estudio se ha considerado pertinente recurrir a su persona.

Tu participación en el estudio consistiría en informante.

1. La técnica a utilizar es la encuesta que es de gran utilidad en los estudios cuantitativos por ser un procedimiento en el que el investigador recopila información mediante el cuestionario previamente diseñado. Será utilizada como un dialogo, conversación, ya sea personal, grabada o mediante video.
2. El instrumento a utilizar es el cuestionario, que tendrá una duración de 30 minutos aproximadamente, el cual está conformado mediante 12 ítems mediante una escala dicotómica.
3. La encuesta se realizará fuera de su horario de trabajo, en espacios coordinados con el informante.

Tu participación en el estudio es voluntaria, si usted no puede hacerlo, comunicar con un no; ya que no es obligatoria. Asimismo, se deja constancia, si en un momento dado no quieres continuar con la entrevista, no habrá ningún problema, o si no quieres responder alguna pregunta en particular de la guía no habrá problemas

Toda información que proporciones ser fundamental para medir las variables de estudio y contrastar las hipótesis.

Esta información será confidencial, esto quiere decir que no diremos a nadie sobre tus respuestas, solo sabrán las personas que forman parte del equipo de estudio.

Por la participación en esta actividad, no involucra pago, beneficio en dinero u objetos materiales.

Si aceptas participar, te pido que marques con (✓) en el cuadro de abajo, y coloca tu nombre, caso contrario no colocar nada.

☐ Si quiero participar.

Nombres y Apellidos:

Especialidad del participante:

---------- Fecha: ….de…….de 2023

Firma del participante

Anexo 6. Fiabilidad del instrumento empleado

Resumen de procesamiento de casos

		N	%
Casos	Válido	100	100,0
	Excluido[a]	0	,0
	Total	100	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

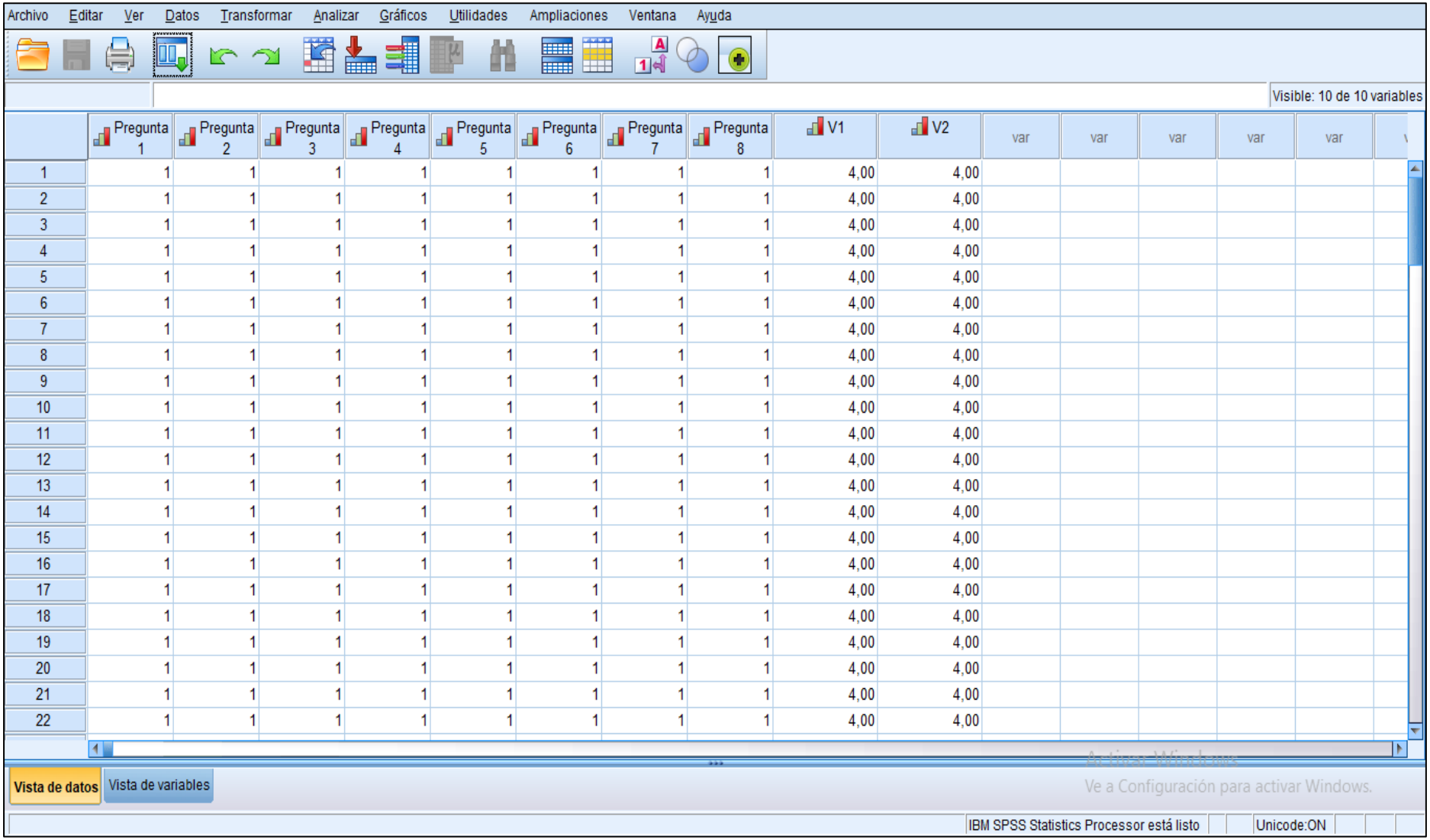
Alfa de Cronbach	N de elementos
0,950	8

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
¿Considera usted que el espionaje informático afecta la protección de datos personales de la víctima?	7,30	1,485	,875	,941
¿Considera usted que la reproducción no autorizada de programas informáticos afecta los datos personales de la víctima?	7,27	1,330	,895	,939

¿Considera usted que el acceso no autorizado a base de datos afecta los datos personales de la víctima?	7,27	1,330	,895	,939
¿Considera usted que el daño a base de datos afecta los datos personales de la víctima?	7,29	1,420	,897	,938
¿Considera usted que el derecho a la privacidad personal se ve vulnerado por la comisión de delitos informáticos?	7,26	1,326	,827	,946
¿Considera usted que la confidencialidad personal se ve vulnerada por la comisión de delitos informáticos?	7,30	1,485	,875	,941
¿Considera usted que la dignidad personal se ve vulnerada por la comisión de delitos informáticos?	7,32	1,735	,512	,960
¿Considera usted que la reputación personal se ve vulnerada por la comisión de delitos informáticos?	7,30	1,485	,875	,941

Anexo 7. Base de datos



Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

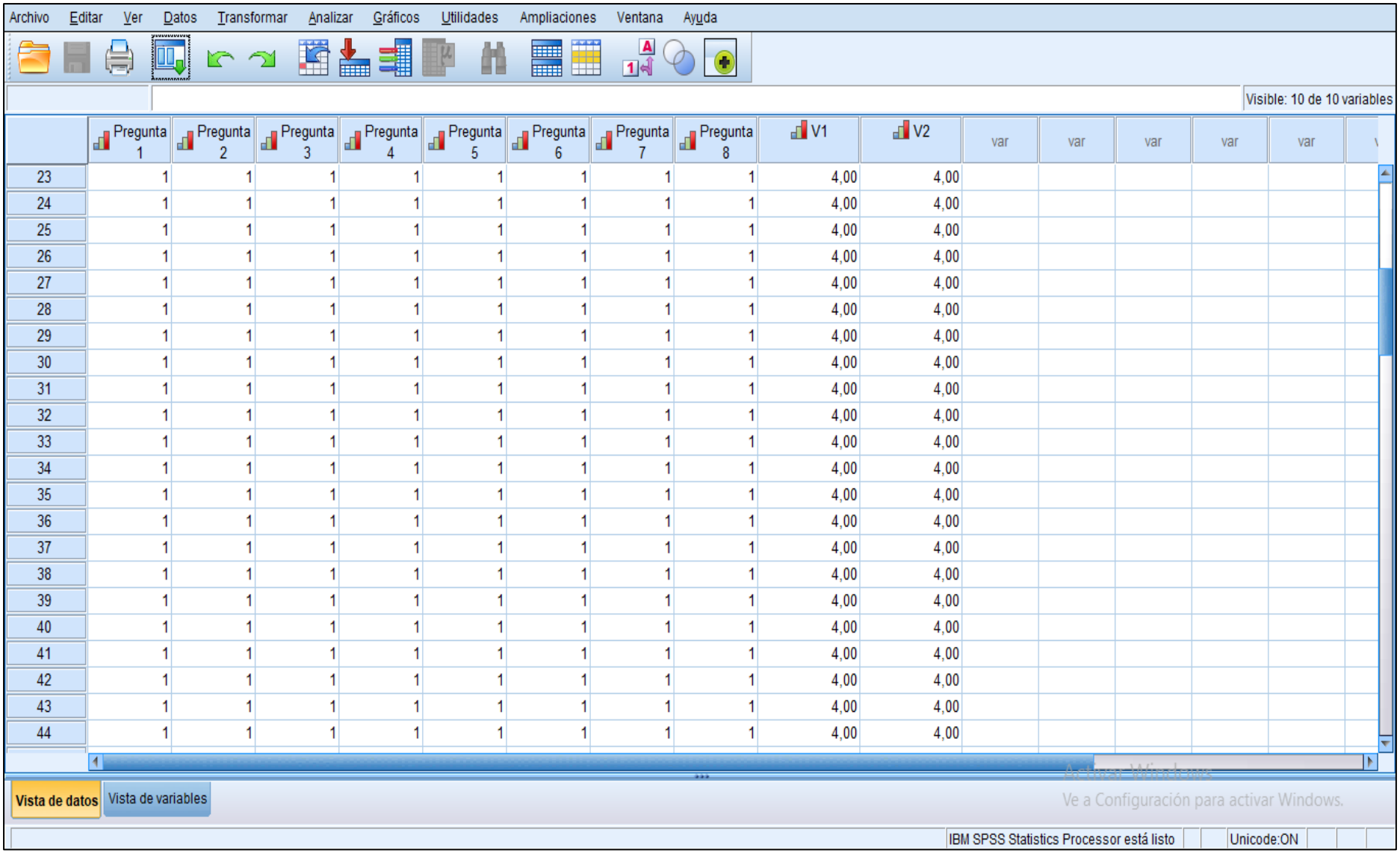
Visible: 10 de 10 variables

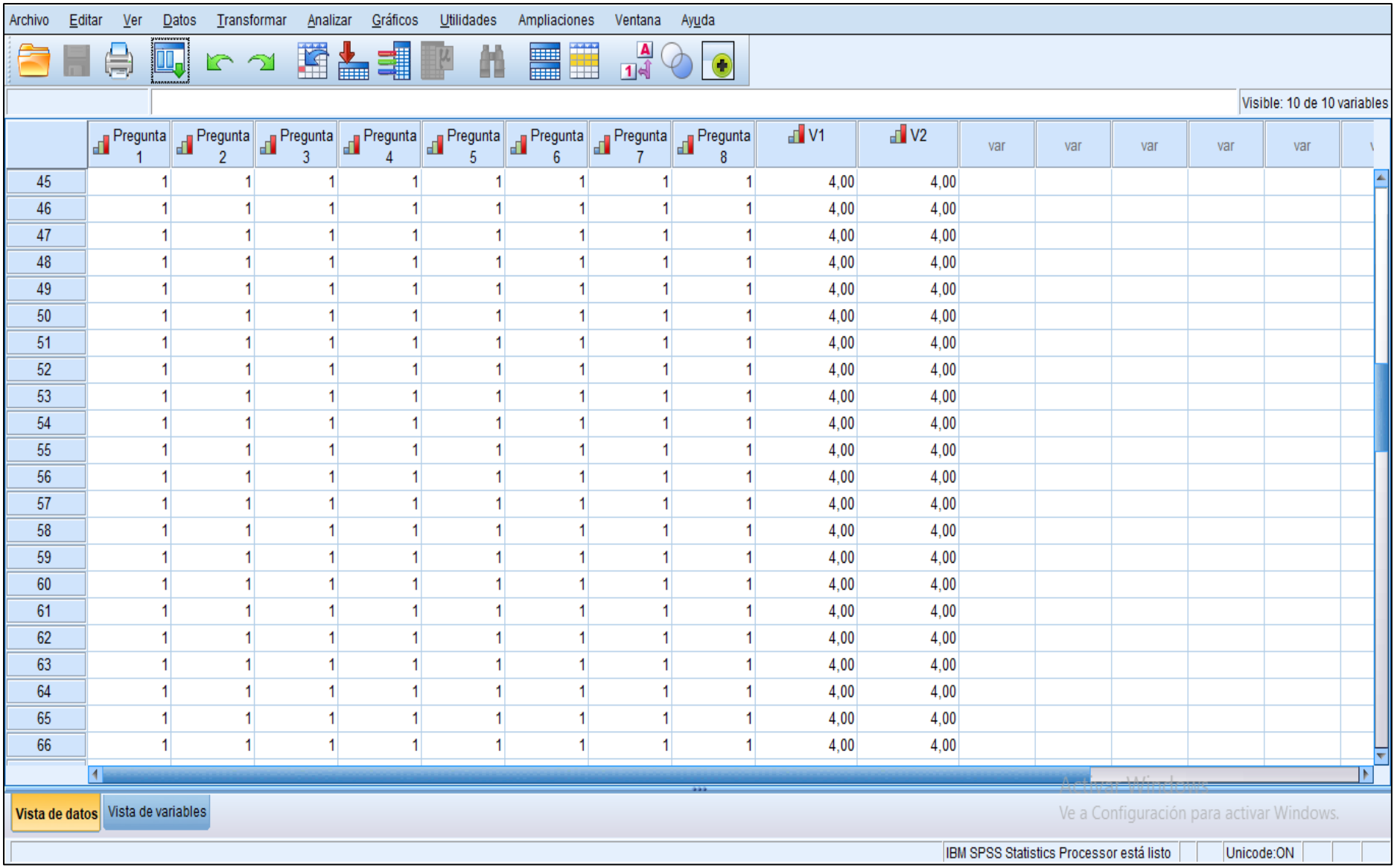
	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8	V1	V2	var	var	var	var	var
1	1	1	1	1	1	1	1	1	4,00	4,00					
2	1	1	1	1	1	1	1	1	4,00	4,00					
3	1	1	1	1	1	1	1	1	4,00	4,00					
4	1	1	1	1	1	1	1	1	4,00	4,00					
5	1	1	1	1	1	1	1	1	4,00	4,00					
6	1	1	1	1	1	1	1	1	4,00	4,00					
7	1	1	1	1	1	1	1	1	4,00	4,00					
8	1	1	1	1	1	1	1	1	4,00	4,00					
9	1	1	1	1	1	1	1	1	4,00	4,00					
10	1	1	1	1	1	1	1	1	4,00	4,00					
11	1	1	1	1	1	1	1	1	4,00	4,00					
12	1	1	1	1	1	1	1	1	4,00	4,00					
13	1	1	1	1	1	1	1	1	4,00	4,00					
14	1	1	1	1	1	1	1	1	4,00	4,00					
15	1	1	1	1	1	1	1	1	4,00	4,00					
16	1	1	1	1	1	1	1	1	4,00	4,00					
17	1	1	1	1	1	1	1	1	4,00	4,00					
18	1	1	1	1	1	1	1	1	4,00	4,00					
19	1	1	1	1	1	1	1	1	4,00	4,00					
20	1	1	1	1	1	1	1	1	4,00	4,00					
21	1	1	1	1	1	1	1	1	4,00	4,00					
22	1	1	1	1	1	1	1	1	4,00	4,00					

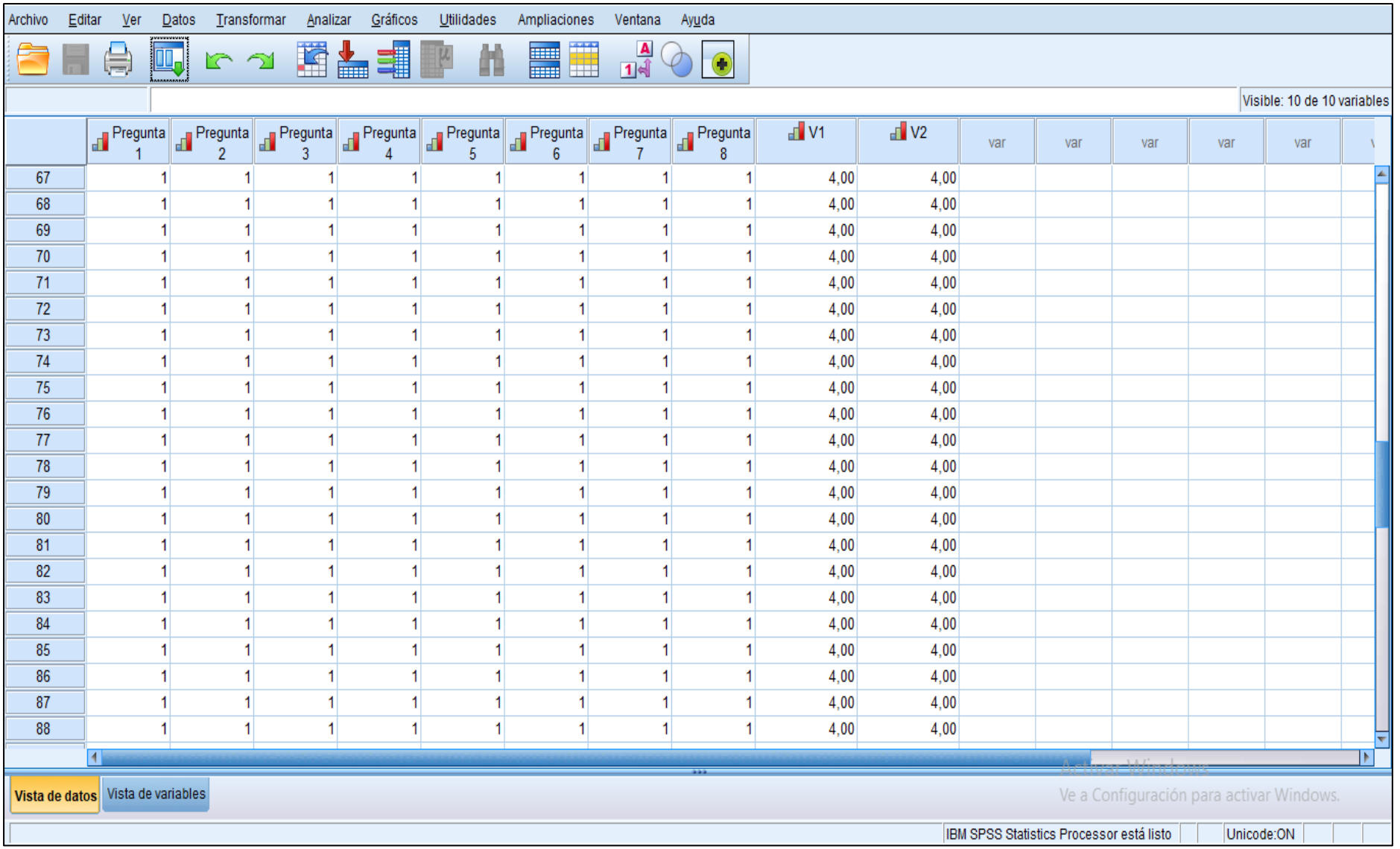
Vista de datos Vista de variables

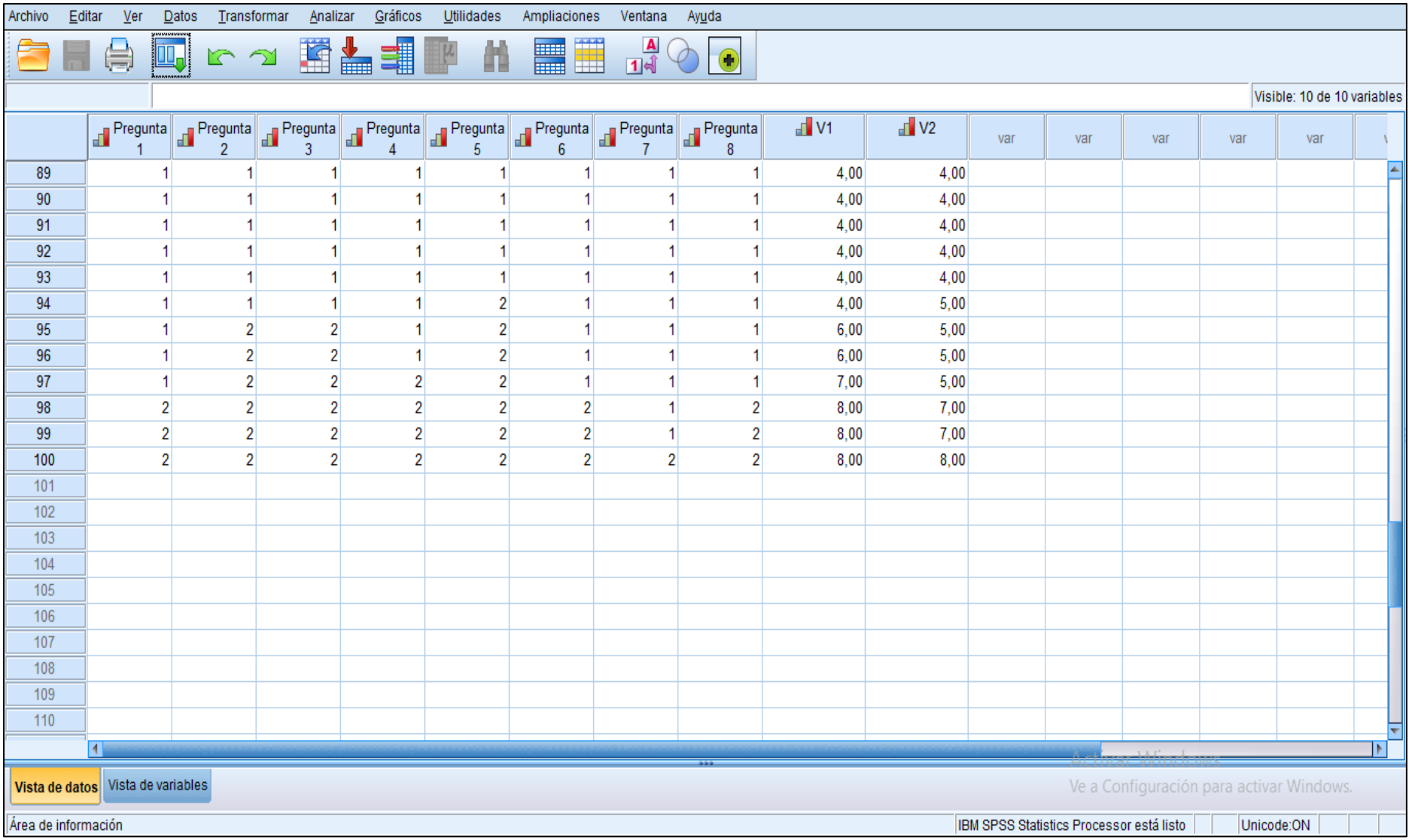
Activar Windows
Ve a Configuración para activar Windows.

IBM SPSS Statistics Processor está listo Unicode:ON


Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda
Visible: 10 de 10 variables
Pregunta 1 Pregunta 2 Pregunta 3 Pregunta 4 Pregunta 5 Pregunta 6 Pregunta 7 Pregunta 8 V1 V2 var var var var var
23 1 1 1 1 1 1 1 1 4,00 4,00
24 1 1 1 1 1 1 1 1 4,00 4,00
25 1 1 1 1 1 1 1 1 4,00 4,00
26 1 1 1 1 1 1 1 1 4,00 4,00
27 1 1 1 1 1 1 1 1 4,00 4,00
28 1 1 1 1 1 1 1 1 4,00 4,00
29 1 1 1 1 1 1 1 1 4,00 4,00
30 1 1 1 1 1 1 1 1 4,00 4,00
31 1 1 1 1 1 1 1 1 4,00 4,00
32 1 1 1 1 1 1 1 1 4,00 4,00
33 1 1 1 1 1 1 1 1 4,00 4,00
34 1 1 1 1 1 1 1 1 4,00 4,00
35 1 1 1 1 1 1 1 1 4,00 4,00
36 1 1 1 1 1 1 1 1 4,00 4,00
37 1 1 1 1 1 1 1 1 4,00 4,00
38 1 1 1 1 1 1 1 1 4,00 4,00
39 1 1 1 1 1 1 1 1 4,00 4,00
40 1 1 1 1 1 1 1 1 4,00 4,00
41 1 1 1 1 1 1 1 1 4,00 4,00
42 1 1 1 1 1 1 1 1 4,00 4,00
43 1 1 1 1 1 1 1 1 4,00 4,00
44 1 1 1 1 1 1 1 1 4,00 4,00
Vista de datos
Vista de variables
Ve a Configuración para activar Windows.
IBM SPSS Statistics Processor está listo
Unicode:ON


Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda
Visible: 10 de 10 variables
Pregunta 1 Pregunta 2 Pregunta 3 Pregunta 4 Pregunta 5 Pregunta 6 Pregunta 7 Pregunta 8 V1 V2 var var var var var
45 1 1 1 1 1 1 1 1 4,00 4,00
46 1 1 1 1 1 1 1 1 4,00 4,00
47 1 1 1 1 1 1 1 1 4,00 4,00
48 1 1 1 1 1 1 1 1 4,00 4,00
49 1 1 1 1 1 1 1 1 4,00 4,00
50 1 1 1 1 1 1 1 1 4,00 4,00
51 1 1 1 1 1 1 1 1 4,00 4,00
52 1 1 1 1 1 1 1 1 4,00 4,00
53 1 1 1 1 1 1 1 1 4,00 4,00
54 1 1 1 1 1 1 1 1 4,00 4,00
55 1 1 1 1 1 1 1 1 4,00 4,00
56 1 1 1 1 1 1 1 1 4,00 4,00
57 1 1 1 1 1 1 1 1 4,00 4,00
58 1 1 1 1 1 1 1 1 4,00 4,00
59 1 1 1 1 1 1 1 1 4,00 4,00
60 1 1 1 1 1 1 1 1 4,00 4,00
61 1 1 1 1 1 1 1 1 4,00 4,00
62 1 1 1 1 1 1 1 1 4,00 4,00
63 1 1 1 1 1 1 1 1 4,00 4,00
64 1 1 1 1 1 1 1 1 4,00 4,00
65 1 1 1 1 1 1 1 1 4,00 4,00
66 1 1 1 1 1 1 1 1 4,00 4,00
Vista de datos
Vista de variables
Ve a Configuración para activar Windows.
IBM SPSS Statistics Processor está listo
Unicode:ON


Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda
Visible: 10 de 10 variables
Pregunta 1
Pregunta 2
Pregunta 3
Pregunta 4
Pregunta 5
Pregunta 6
Pregunta 7
Pregunta 8
V1
V2
var
67 1 1 1 1 1 1 1 1 4,00 4,00
68 1 1 1 1 1 1 1 1 4,00 4,00
69 1 1 1 1 1 1 1 1 4,00 4,00
70 1 1 1 1 1 1 1 1 4,00 4,00
71 1 1 1 1 1 1 1 1 4,00 4,00
72 1 1 1 1 1 1 1 1 4,00 4,00
73 1 1 1 1 1 1 1 1 4,00 4,00
74 1 1 1 1 1 1 1 1 4,00 4,00
75 1 1 1 1 1 1 1 1 4,00 4,00
76 1 1 1 1 1 1 1 1 4,00 4,00
77 1 1 1 1 1 1 1 1 4,00 4,00
78 1 1 1 1 1 1 1 1 4,00 4,00
79 1 1 1 1 1 1 1 1 4,00 4,00
80 1 1 1 1 1 1 1 1 4,00 4,00
81 1 1 1 1 1 1 1 1 4,00 4,00
82 1 1 1 1 1 1 1 1 4,00 4,00
83 1 1 1 1 1 1 1 1 4,00 4,00
84 1 1 1 1 1 1 1 1 4,00 4,00
85 1 1 1 1 1 1 1 1 4,00 4,00
86 1 1 1 1 1 1 1 1 4,00 4,00
87 1 1 1 1 1 1 1 1 4,00 4,00
88 1 1 1 1 1 1 1 1 4,00 4,00
Vista de datos
Vista de variables
Ve a Configuración para activar Windows.
IBM SPSS Statistics Processor está listo
Unicode:ON



	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8	V1	V2	var	var	var	var	var
89	1	1	1	1	1	1	1	1	4,00	4,00					
90	1	1	1	1	1	1	1	1	4,00	4,00					
91	1	1	1	1	1	1	1	1	4,00	4,00					
92	1	1	1	1	1	1	1	1	4,00	4,00					
93	1	1	1	1	1	1	1	1	4,00	4,00					
94	1	1	1	1	2	1	1	1	4,00	5,00					
95	1	2	2	1	2	1	1	1	6,00	5,00					
96	1	2	2	1	2	1	1	1	6,00	5,00					
97	1	2	2	2	2	1	1	1	7,00	5,00					
98	2	2	2	2	2	2	1	2	8,00	7,00					
99	2	2	2	2	2	2	1	2	8,00	7,00					
100	2	2	2	2	2	2	2	2	8,00	8,00					
101															
102															
103															
104															
105															
106															
107															
108															
109															
110															