Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

UTILIDAD DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL DE LA POLICÍA NACIONAL DEL PERÚ, 2023

Línea de investigación:

Sistemas de información y optimización

Tesis para optar el grado académico de Maestro en Ingeniería de Sistemas con mención en Gestión de Tecnologías de la Información

Autor

Román Meneses, Cesar Arístides

Asesor

Bazán Briceño, José Luis

ORCID: 0000-0001-8604-3260

Jurado

Flores Masías, Edward José

Peña Carrillo, César Serapio

Flores Eulogio, Ramiro Amador

Lima - Perú

2024

UTILIDAD DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL DE LA POLICÍA NACIONAL DEL PERÚ, 2023

INFORME DE ORIGINALIDAD

29%	28%	4%	11%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.ucv.edu.pe Fuente de Internet	4%
2	repositorio.unfv.edu.pe Fuente de Internet	2%
3	latam.redilat.org Fuente de Internet	1%
4	bibliotecadigital.econ.uba.ar Fuente de Internet	1%
5	repositorio.iaen.edu.ec Fuente de Internet	1%
6	www.coursehero.com Fuente de Internet	1%
7	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	1%
8	www.ibm.com Fuente de Internet	1%

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

UTILIDAD DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL DE LA POLICÍA NACIONAL DEL PERÚ, 2023

Línea de Investigación:

Sistemas de Información y Optimización

Tesis para optar el grado académico de Maestro en Ingeniería de Sistemas con mención en Gestión de Tecnologías de la Información

Autor

Román Meneses, Cesar Arístides

Asesor
Bazán Briceño, José Luis
ORCID: 0000-0001-8604-3260

Jurado
Flores Masías, Edward José
Peña Carrillo, César Serapio
Flores Eulogio, Ramiro Amador

Lima – Perú

2024

Dedicatoria

A mis queridos padres, por este logro que es un testimonio de su dedicación, por las lecciones de vida que me han brindado y por el cariño de siempre. Mi gratitud hacia ustedes es imposible de expresar completamente. Esta tesis es un tributo a su legado y a la eterna admiración que siento y sentiré por ustedes. Gracias por el honor y la bendición de tener los mejores padres del mundo.

Agradecimiento

En primer lugar, les agradezco a mis padres que siempre me han brindado su apoyo incondicional para poder cumplir todos mis objetivos personales y académicos, frente a las adversidades, a mis asesores por su dedicación y paciencia, sin sus palabras y correcciones precisas no hubiese podido lograr llegar a esta instancia tan anhelada. Asimismo, son muchos los docentes que han sido parte de mi camino académico, y a todos ellos les quiero agradecer por transmitirme los conocimientos necesarios para hoy poder estar aquí. Por último, agradecer a mi Casa de Estudios, que me ha exigido tanto, que me ha permitido obtener mi tan ansiado título.

ÍNDICE

Índice de Tablas

Índice de Figuras

Resumen

Objetivo: Determinar la relación que existe entre la utilidad de la ciberseguridad en la protección de la información digital de la Policía Nacional del Perú, 2023. **Método:** Es de enfoque cuantitativo, de tipo básica. El diseño es no experimental. El nivel de la investigación es correlacional. La población designada son los especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP, pertenecientes a la ciudad de Lima, personal que cuenta con amplia experiencia teórica y técnica de la problemática, lo que permitirá generar conclusiones y recomendaciones a la Alta Dirección de la PNP acerca de la seguridad en la protección de la información digital. **Resultados:** El 58,9% de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la implantación de marcos de protección de información digital dentro del área de informática es óptima, mientras que el 41% indica que es alto. **Conclusiones**: Se concluye que sí existe una relación directa entre la utilidad de la ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023 dado que el coeficiente de la correlación fue de 0,753 y es una correlación positiva. En ese sentido, es preciso resaltar que la ciberseguridad es fundamental en el ecosistema digital que emplea la institución policial ya que funciona como el factor determinante para la protección del sistema contra posibles ataques y amenazas digitales.

Palabras claves: ciberseguridad, protección de la información digital, gestión de activos, propiedades de la información.

Abstract

Objective: Determine the relationship that exists between cybersecurity and the protection of digital information of the National Police of Peru, 2023. **Method:** It is a quantitative, basic type approach. The design is non-experimental. The level of the investigation. The population consists of specialist collaborators who work in the Technology, Information Technology and Communications Offices (OFITIC) of the PNP, belonging to the city of Lima, personnel who have extensive theoretical and technical experience of the problem, which will allow generating conclusions. and recommendations to the Senior Management of the PNP regarding security in the protection of digital information. **Results:** 58.9% of specialists who work in the Technology, Information Technology and Communications Offices (OFITIC) of the PNP maintain that the implementation of digital information protection frameworks within the IT area is optimal, while 41% indicates that it is high. **Conclusions:** It is concluded that there is a direct relationship between cybersecurity and the protection of digital information of the National Police of Peru, 2023. Given that; the correlation coefficient was 0.753 and it is a considerable positive correlation. In this sense, it is necessary to highlight that cybersecurity is fundamental in the digital ecosystem used by the police institution since it functions as the determining factor for the protection of the system against possible attacks and digital threats.

Keywords: cybersecurity, digital information protection, asset management, information properties.

I. INTRODUCCIÓN

1.1. Planteamiento del problema

La ciberseguridad en la información digital es un tema de creciente importancia en una sociedad altamente conectada y digitalizada. En un mundo en el que la información se transmite y almacena en forma digital, la protección de datos confidenciales y la prevención de amenazas cibernéticas se han convertido en aspectos críticos para individuos e instituciones públicas y privadas.

A nivel internacional, los ciberataques están en constante aumento tanto en frecuencia como en sofisticación, según el informe de IBM Security X-Force Threat Intelligence Index 2021. A su vez, el número de registros expuestos en violaciones de datos aumentó en un 369% en 2020 en comparación con el año anterior (IBM Security, 2021). El Informe de Amenazas de Ciberseguridad de Cyber Threat Report, 2021 reveló que se registraron más de 304.7 millones de intentos de ransomware en todo el mundo en 2020, lo que representa un aumento del 62% con respecto al año anterior (SonicWall, 2021).

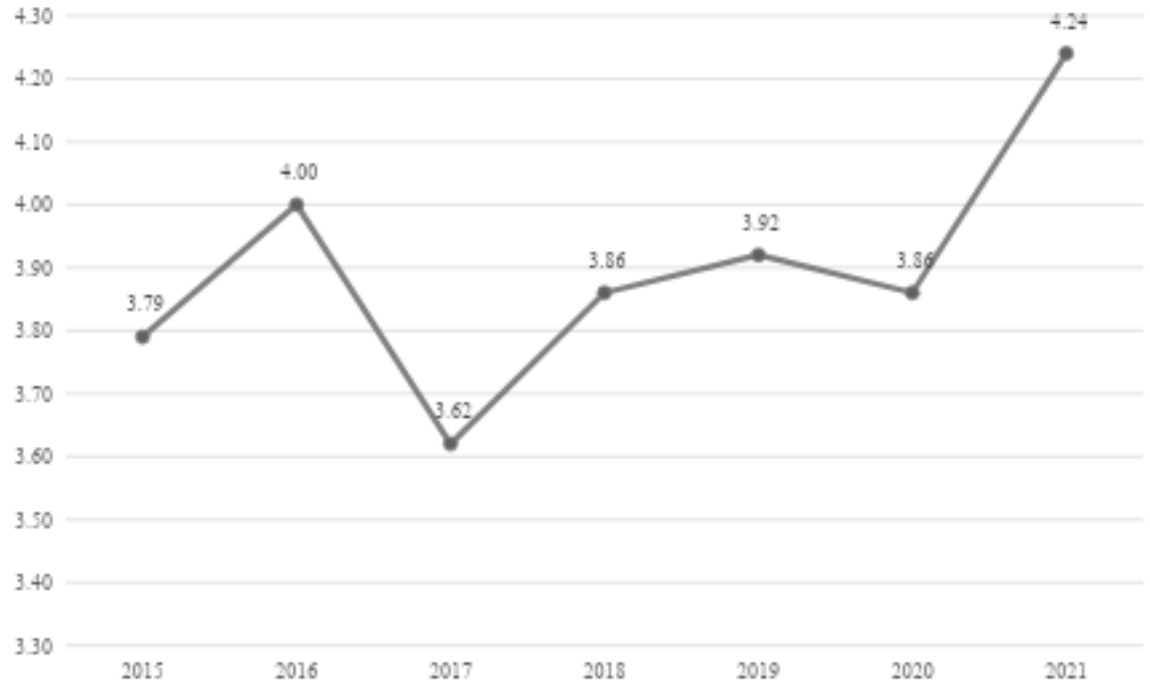
En este contexto, varios países son acusados de llevar a cabo actividades cibernéticas maliciosas con fines políticos o económicos. El informe Cybersecurity of the Nation del 2020 reveló que China, Rusia, Irán y Corea del Norte son los principales actores estatales en ciber espionaje y ciberataques (Centro de Estudios Estratégicos e Internacionales [CSIS], 2020). Según el informe Global Threat Report, el 81% de las intrusiones en 2020 fueron atribuidas a actores respaldados por el estado (Crowdstrike, 2021).

En esta línea, las brechas de alto resguardo en seguridad en datos representan una preocupación importante en el ámbito de la ciberseguridad. El Informe Cost of a Data Breach Report (2021), revela que los costes han aumentado de 3,86 a 4,24 millones de dólares lo que

representa un aumento de casi 10 % del coste total promedio respecto al año anterior; lo que significa el mayor aumento de coste de los últimos siete años. En el sector público, los costes han incrementado su valor ya que al tener un aumento del 78,7 % este se elevó de 1,08 a 1,93 millones de dólares el 2021. El ransomware y los ataques destructivos fueron más costosos que otras brechas de datos llegando a costar en promedio 4,69 millones de dólares. El porcentaje de empresas en las que el ransomware fue un factor de la brecha de datos fue del 7,8 % (IBM Security, 2021). Las brechas de datos en el sector sanitario han aumentado de un coste total medio de 7,13 millones de dólares en 2020 a 9,23 millones en 2021, es decir 29,5 % más. Este análisis es relevante ya que permite evaluar la magnitud de inversión direccionada a preservar la alta seguridad que deben tener los datos más aun en un contexto de incertidumbre política y de inseguridad ciudadano.

Figura 1

Coste medio de una brecha de datos (medido en millones de dólares)



Fuente: IBM Security (2021). Cost of a Data Breach Report.

Tabla 1

Coste total medio de una brecha de datos por país o región (medido en millones de dólares)

País o Región	Año	
	2020	2021
EE. UU	USD 8.64	USD 9.05
Canadá	USD 4.50	USD 5.40
Reino Unido	USD 3.90	USD 4.67
Alemania	USD 4.45	USD 4.89
Escandinavia	USD 2.51	USD 2.67
Turquía	USD 1.77	USD 1.91
Corea del Sur	USD 3.12	USD 3.68
Japón	USD 4.19	USD 4.69
Brasil	USD 1.12	USD 1.08
Latinoamérica	USD 1.68	USD 2.56
Francia	USD 4.01	USD 4.57
Italia	USD 3.19	USD 3.61
Sudáfrica	USD 2.14	USD 3.21
Medio Oriente	USD 6.52	USD 6.93
India	USD 2.00	USD 2.21
ASEAN	USD 2.71	USD 2.71
Australia	USD 2.15	USD 2.82

Fuente: IBM Security (2021). Cost of a Data Breach Report.

En esta línea, el informe Data Breach Investigations Report del 2023 analizó más de 16,312 incidentes de seguridad de acorde al tipo de industria y tamaño de empresa. De los incidentes analizados 5,199 fueron brechas confirmadas (Verizon, 2023), según indica la tabla 2.

Tabla 2

Número de incidentes de seguridad e infracciones por industria víctima y tamaño de la organización

Industria	Incidente				Brecha			
	Total	Pequeño (1-1,000)	Grande (1,000+)	Desconocido	Total	Pequeño (1-1,000)	Grande (1,000+)	Desconocido
Total	16312	694	489	15129	5199	376	223	4600
Alojamiento	254	4	2	248	68	4	1	63
Administrativo	38	8	14	16	32	8	11	13

Agricultura	66	1	5	60	33	0	3	30
Construcción	87	7	1	79	66	4	1	61
Educación	496	63	15	418	238	28	8	202
Entretenimiento	432	13	3	416	93	10	1	82
Finanzas	1829	70	30	1729	477	38	18	421
Salud	522	28	15	479	433	23	15	395
Información	2105	45	110	1950	380	23	19	338
Gestión	9	1	0	8	9	1	0	8
Manufactura	1814	37	24	1753	259	18	15	226
Minería	25	2	0	23	13	2	0	11
Otros Servicios	143	7	2	134	100	6	1	93
Profesional	1396	176	54	1166	421	85	32	304
Administración Pública	3270	87	110	3073	582	48	39	495
Inmobiliaria	83	15	5	63	59	10	2	47
Minorista	404	62	44	298	191	33	28	130
Transporte	349	13	25	311	106	8	13	85
Utilidades	117	12	6	99	33	3	3	27
Mayoristas	96	42	22	32	53	23	11	19
Desconocido	2777	1	2	2774	1553	1	2	1550
Total	16312	694	489	15129	5199	376	223	4600

Fuente: Verizon (2023). Data Breach Investigations Report.

El Perú fue uno de los países más afectados por ataques de malware en América Latina en 2020 al tener la mayor filtración de datos personales, dado que ocupa el tercer lugar en la región, según el informe La Fuga de Datos en América Latina, elaborado por Kaspersky (2021). Según el Reporte Anual de Ciberseguridad del 2020, en el Perú se registraron más de 33 millones de detecciones de malware durante ese año, lo que indica un alto nivel de actividad de ciberdelincuencia (ESET, 2020). Ese mismo año el Informe anual CERT-PE, estimó que se detectaron más de 32,000 casos de ataques de phishing en el país (Centro de Respuesta a Incidentes Cibernéticos del Perú [CERT-PERU], 2020). Asimismo, el artículo informativo del Diario El Peruano del 2022, menciona que el Ministerio Público, durante el 2021 recibió 18

mil 596 denuncias de casos de cibercrimen, lo que representa un incremento porcentual de 92,9% en comparación con el 2020, a ello se suma los casos reportados por la Policía Nacional del Perú (PNP) que registró 14 mil 671 denuncias por delitos informáticos durante el 2021. Ello representa un aumento de 65% de casos más que el año anterior (8 897 denuncias en 2020), considerando en primer lugar el fraude informático que es el tipo más frecuente de cibercrimen con 10 mil 924 casos y, en el segundo lugar de la lista, está la modalidad de suplantación con 2 mil 666 casos denunciados para el 2021. La falta de conciencia y educación en ciberseguridad también es un desafío en Perú. De acuerdo al estudio realizado por la empresa ESET en 2020, el 58% de los peruanos encuestados afirmaron que no recibieron ningún tipo de capacitación o educación en ciberseguridad, mientras que, en el estudio sobre ciberseguridad realizado por Ipsos Perú en 2021, el 40% de los peruanos no saben qué es un ataque cibernético y el 38% no está familiarizado con el concepto de ciberseguridad. Las brechas de datos y filtraciones de información confidencial también son un problema en Perú. En 2019, se reportó una importante brecha de datos en el Registro Nacional de Identificación y Estado Civil (RENIEC), exponiendo la información personal de millones de peruanos (Diario El Comercio); a ello se suma los ataques de malware, incluyendo ransomware, phishing y virus, que también son una preocupante realidad.

A nivel local, expertos en seguridad informática advierten el gran peligro que significa el uso de ordenadores e internet si es que no se ejecutan las normas básicas en el tema de seguridad digital lo que perjudicaría la cantidad de información dentro de un contexto de proteger los datos de alguna institución en específico (Dermutas, 2020, p.34). En este contexto, la Policía Nacional del Perú realizó la inclusión de los recursos digitales en cada actividad que realiza la institución en relación a los criterios de telecomunicaciones, y la potencia para fines bélicos en el contexto han obligado a que la ciberseguridad se encuentre abordada desde un enfoque de esfuerzo conjunto entre las áreas técnicas administrativas y políticas dentro de la

institución. De esta manera, la innovación e interdependencia tecnológica como el acceso digital, la conectividad, entre otros, han generado que la institución policial desarrolle múltiples estrategias en relación a la ciberseguridad para la protección de sus datos.

1.2. Descripción del problema

En la Policía Nacional del Perú, la protección de la información digital se vuelve crucial debido a la cantidad de datos sensibles y confidenciales que manejan. Estos datos incluyen investigaciones en curso, información de víctimas y testigos, así como datos personales de los propios agentes de la policía. Un incidente de seguridad en la red puede comprometer gravemente la integridad de la información, poner en riesgo operaciones en curso y afectar la confianza de la ciudadanía en la institución policial. Durante el 2011, un grupo de hackers publicaron los datos de 2.800 agentes de Águilas Negras, la Policía de Perú que se encarga, entre otras misiones, de custodiar las entidades bancarias en Lima.

La lista de efectivos policiales, de acceso público en internet, incluye información que identifica a los agentes con su nombre, número de Carnet de Identidad Policial (CIP), turnos de labor policial y estado de las entidades bancarias en la que hacían custodia (Areitio, 2018).

El grupo de hackers conocido como "LulzSecPeru" en el 2020 atacó los servidores de la Policía Nacional del Perú, logrando acceder y filtrar información confidencial de la institución. Este incidente puso en evidencia las vulnerabilidades de seguridad existentes en los sistemas de la policía y generó preocupación en cuanto a la protección de la información sensible. Otra institución pública afectada en el 2022 fue el Comando Conjunto de las Fuerzas Armadas y del Ejército peruano, el grupo de hackers Guacamaya accedieron a 283 mil correos electrónicos con 175 gigabytes que tienen documentos militares.

En el 2023 un reportero de televisión, comprobó la facilidad que tienen algunos

inescrupulosos cibernéticos para asentar una denuncia sin justificación a través de los servidores de la Policía Nacional del Perú. Incluso, se puede brindar información privada y financiera de cualquier persona a precios accesibles.

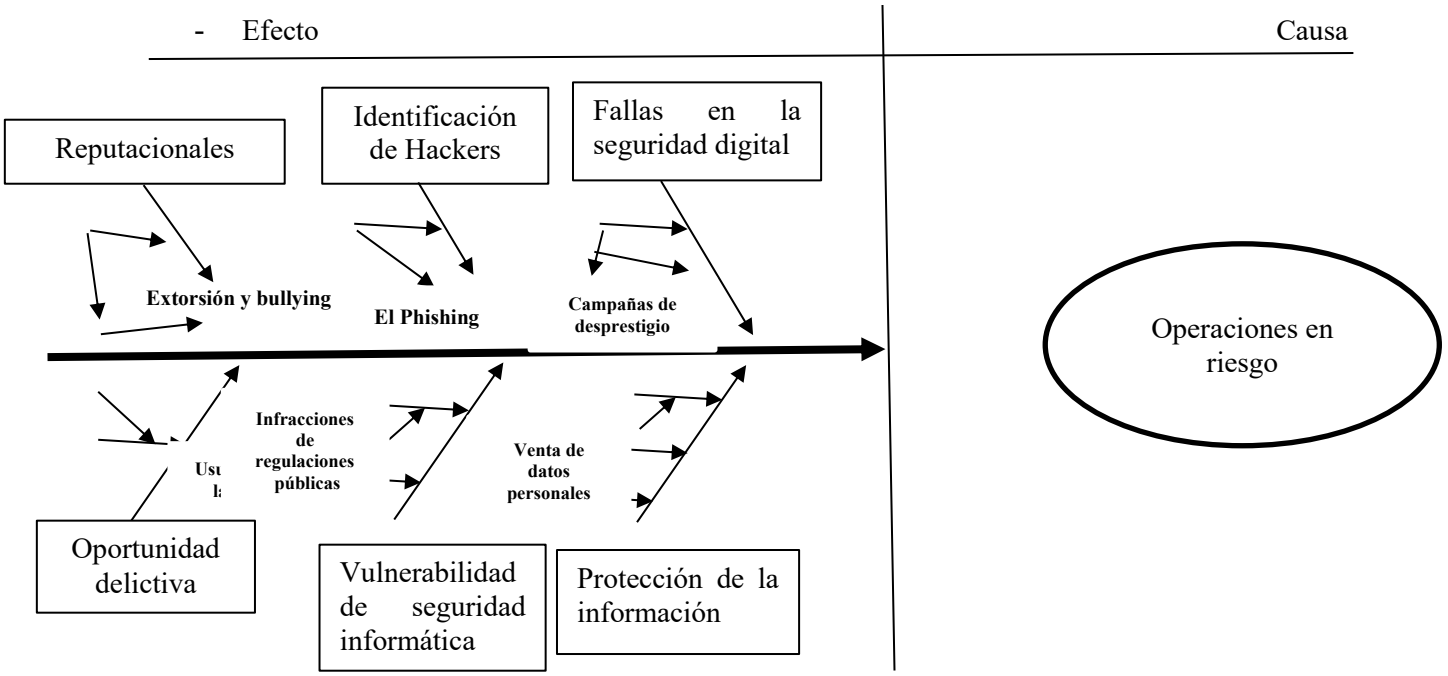
Por lo expuesto, un problema específico a nivel de propiedades de la información es el escaso compromiso de los colaboradores en preservar la confidencialidad, integridad y autenticidad de los datos de los cuales tienen acceso un grupo cerrado de usuarios autorizados y autenticados por la confianza que se les otorga.

Otro problema es la débil gestión de activos críticos que son recursos y sistemas de una nación para desarrollar sus trece capacidades nacionales; en este caso, un activo crítico sujeto a protección son las tecnologías de la información. Si bien la Dirección Nacional de Inteligencia (DINI) es el responsable de supervisar la identificación y evaluación de riesgo de cada sector (Decreto Supremo Nº 106-2017-PCM que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgo de los Activos Críticos Nacionales) en las oficinas de seguridad digital de la PNP, no se destina capacitación constante en prevención de datos como puede ser la capacitación a los directivos en conocimiento de tendencias de seguridad digital. Otro aspecto es el presupuesto para seguir resguardando la información mediante software y hardware de alta gama que cada año van saliendo en el mercado.

En el siguiente esquema se analiza los distintos factores que hacen vulnerable la seguridad y protección de la información y que ponen en riesgo constante los activos críticos como la información de la PNP. Ver figura 2. elementos

Figura 2

Diagrama de Ishikawa



1.3. Formulación del problema

1.3.1 Problema general

¿Qué relación existe entre la utilidad de la ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023?

1.3.2. Problemas específicos

¿Qué relación existe entre las propiedades de la información y la protección de la información digital de la Policía Nacional del Perú, 2023?

¿Qué relación existe entre la gestión de activos críticos y la protección de la información digital de la Policía Nacional del Perú, 2023?

1.4. Antecedentes

1.4.1. Antecedentes internacionales

Pérez y Ramos (2020) en su investigación a nivel de maestría tuvo como objetivo general determinar la formulación de una política de seguridad digital. Para dicho fin realizó un análisis de estándares internacionales que permite promover la coordinación interinstitucional en la gestión de los riesgos del ciberespacio. Como resultado planteó lineamientos para una política de ciberseguridad para proteger la información digital de Fuerza Armadas ecuatorianas, mediante la colaboración y coordinación con las instituciones especializadas en la seguridad informática en ese país. El estudio concluye que la matriz de políticas de seguridad informática fomenta un ambiente estable, que involucra las destrezas para el manejo de desafíos que incluyen la integración a nuevas tecnologías.

Pozo (2022) en su estudio de posgrado relacionado a Ciberseguridad tuvo por objetivo el planteamiento de estrategias cibernéticas para el cuidado y protección de los sistemas de datos. Se utilizó como metodología estudios de medidas de protección en las instituciones privadas, encontrando amenazas de los ciberataques que acontecen a nivel mundial, específicamente en países caracterizados por un alto grado de ciberataques. Se consideró, además, fuentes secundarias donde se aborda temas como las estrategias de defensa de varios países europeos y de América del Sur. Se concluye que el estudio de la defensa cibernética tiene una dimensión poco pragmática. Se señala que el Estado Ecuatoriano propone la configuración de un modelo local de gobernanza en ciberdefensa en el ciberespacio inscrito en su normativa vigente que tiene como finalidad prevenir y mitigar toda actividad cibernética de intrusiones maliciosa que ponga en riesgo la seguridad integral de los activos críticos del estado ecuatoriano.

Cáceres (2021) en su investigación tuvo como objetivo determinar medidas de seguridad para el desarrollo de sistemas críticos que contemple el concepto de privacidad por defecto, el método de corrección por construcción y los conceptos de seguridad por diseño y por defecto. Para ello, el estudio optó por la integración de distintas normativas y metodologías asociadas al desarrollo de software seguro. Se obtuvo como resultado la implementación de un marco metodológico de trabajo para la ciberdefensa y gestión segura del ciclo de vida de los sistemas críticos. La investigación concluye que al existir múltiples organismos que emiten recomendaciones, normas y buenas prácticas relacionadas con la programación de sistemas y elementos informáticos, también los Estados desarrollan sus propias prácticas, leyes y recomendaciones, lo cual evidencia la heterogeneidad de criterios a la hora de decidir qué estrategia abordar para iniciar proyectos de desarrollo de aplicaciones y sistemas críticos.

1.4.2. Antecedentes nacionales

Villarrubia (2019) en su estudio planteó como objetivo medidas de protección de información digital de las Fuerzas Armadas en la defensa nacional en Lima. Para dicho fin, a nivel metodológico se trabajó con el enfoque cualitativo formulado holísticamente con entrevistas semiestructuradas aplicadas a personal técnico especialista e ingenieros que laboran en los centros de informática de las instituciones armadas. Se concluye que existe limitada protección de la información digital, así como también una relativa vulnerabilidad frente a las ciber amenazas de los centros de informática del Ejercito de la Marina y de la Fuerza Aérea en el marco de ciberseguridad de la Política de Seguridad y Defensa Nacional.

Davis (2020) con su tesis de Maestría relacionado a la ciberseguridad de la Marina de Guerra del Perú, tuvo como objetivo determinar el nivel de conocimiento del personal de la Fuerzas Navales en aspectos vinculados a ciberseguridad específicamente al personal usuario de las redes informáticas. La metodología comprendió la validación de una encuesta tipo test

dirigido al personal superior, personal subalterno y personal de marinería de las Fuerzas Navales con la que se evaluó el nivel de conocimiento en ciberseguridad. El estudio concluyó que el nivel de conocimiento de personal de las Fuerzas Navales es bajo, lo que refleja la vulnerabilidad y exposición a ataques de tipo Phishing, ya que a los especialistas les costaría trabajo enfrentar y decidir cómo actuar frente a un ataque de este tipo.

Correa (2022) en la investigación propuso como objetivo determinar la incidencia de la ciberseguridad en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur. La metodología empleada fue de tipo aplicada con diseño no experimental, de tipo transversal y nivel correlacional – causal. El cuestionario utilizado fue aplicado a 1046 colaboradores, dando como resultados que el tratamiento de datos personales se relacionó en un 45.0% con el nivel medio de ciberseguridad. Asimismo, se constató que un 39.4% obtuvo el nivel óptimo de ciberseguridad y en un 13.5% el nivel no óptimo de ciberseguridad. El estudio concluye que la ciberseguridad incide significativamente en el tratamiento de datos institucionales en una Municipalidad distrital de Lima Sur.

1.5. Justificación de la investigación

1.5.1. Justificación temática

La investigación está contemplada en la Resolución Ministerial Nº 411-2017-IN sobre el Plan de Modernización del Ministerio del Interior 2017 - 2021, que permite el desarrollo de plataformas tecnológicas que favorezcan la modernización tecnológica institucional de la PNP, según la Resolución Ministerial Nº 410-2017–IN que permite adecuar instrumentos de gestión respecto a la simplificación administrativa, direccionando la estandarización de procesos.

1.5.2. Justificación geográfica

Geográficamente, se implementó en todas las oficinas de tecnología de la información de las diferentes unidades PNP a nivel nacional, homogenizando los procesos en ciberseguridad a nivel nacional, protegiendo la información e infraestructura de comunicación digital.

1.5.3. Justificación social

Socialmente promueve el uso correcto tecnologías de información en el personal que labora en las unidades de la PNP, optimizando el tiempo para el desarrollo de las actividades del personal, atenuando los factores de riesgo ante posibles ataques cibernéticos.

1.5.4. Justificación medioambiental

El aumento de las amenazas cibernéticas ha llevado a un incremento en las medidas de seguridad, lo que implica un mayor uso de recursos y energía en infraestructuras digitales. La implementación de soluciones de ciberseguridad eficientes puede reducir el consumo de energía y contribuir a la sostenibilidad energética.

1.5.5. Justificación metodológica

Esta investigación al tener un diseño no experimental donde no se modifican las variables analizadas en el contexto natural, es importante porque permite conocer información validada científicamente respetando el proceso de rigor de la investigación científica.

1.5.6. Justificación tecnológica

Radica en la protección de datos sensibles, la adaptación a las amenazas en constante evolución, el respaldo de los avances tecnológicos, la garantía de la continuidad del servicio, el cumplimiento con la normatividad vigente y la promoción de la confianza en la tecnología.

1.6. Limitaciones de la investigación

La investigación está limitada porque no se cuenta con presupuesto. Asimismo, el estudio se desarrolla con la escasa bibliografía relacionada a la protección de información en

entidades pública como la Policía Nacional del Perú debido a su dinamismo e influencia coyuntural política.

La investigación es fundamental porque permitió contribuir a evitar que la confidencialidad, integridad, disponibilidad y autenticación de la información sean vulneradas y tenga consecuencias graves para la Policía Nacional del Perú. Para ello, es importante la continuidad del servicio ante ciberataques dado que mitigará el impacto de dichos ataques ante la gran variedad de actividades maliciosas de intrusión o accesos no autorizados.

La relevancia del presente estudio permite, además, estudiar la relación entre la ciberseguridad y la protección de la información digital de los registros que se encuentran almacenados en los Centros de Datos de la Policía Nacional del Perú.

El presente estudio fue viable ya que se realizó en un entorno conocido laboralmente por el investigador, como es el Área de Tecnologías de la Información de la Policía Nacional del Perú, mediante la implementación de un enfoque integral, el uso de herramientas y tecnologías adecuadas, la adhesión a marcos regulatorios, la concientización de los usuarios y la colaboración entre actores, frente a las amenazas cibernéticas.

La trascendencia de esta línea de estudio es la homogenización y estandarización de los procesos de gestión de tecnologías de la información en las diferentes unidades pertenecientes a la Policía Nacional del Perú.

La originalidad se debe al enfoque específico en una institución particular, el contexto nacional, la aplicación práctica y el impacto real de las medidas de ciberseguridad en la seguridad y eficiencia operativa.

1.7. Objetivos

1.7.1. Objetivo General

Determinar la relación que existe entre la ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023.

1.7.2. Objetivos Específicos

Determinar la relación que existe entre las propiedades de la información y la protección de la información digital de la Policía Nacional del Perú, 2023.

Determinar la relación que existe entre la gestión de activos críticos y la protección de la información digital de la Policía Nacional del Perú, 2023.

1.8. Hipótesis

1.8.1. Hipótesis General

Existe una relación directa entre la utilidad de la ciberseguridad en la protección de la información digital de la Policía Nacional del Perú, 2023.

1.8.2. Hipótesis Específicos

a) Existe una relación directa entre las propiedades de la información y la protección de la Información digital de la Policía Nacional del Perú, 2023.

b) Existe una relación directa entre la gestión de activos críticos y la protección de la Información digital de la Policía Nacional del Perú, 2023.

II. MARCO TEÓRICO

2.1. Estado del Arte

El informe publicado en el 2019 por la Organización de Estados Americanos (OEA) y Amazon Web Services (AWS) sobre el abordaje integral de la Ciberseguridad, propone el empleo del Cibesecurity Framework (CSF) el cual es un marco de trabajo para reducir los riesgos para infraestructura crítica desarrollado por National Institute of Standards and Technology (NIST) que consta de tres componentes como el Framework Core, los Niveles de implementación (Tiers) y los Perfiles. Por su parte, ISO (2018) sostiene que el Framework Core son resultados de ciberseguridad deseados organizados en Categorías alineados a estándares internacionales. Los niveles de implementación describen el grado de implementación de las prácticas de gestión de riesgos de ciberseguridad de una organización. Finalmente, los perfiles son los roles y permisos de una organización que van alineados a los requisitos y objetivos institucionales, la tolerancia al riesgo y los recursos según los resultados deseados del Framework Core (NIST, 2019).

Respecto a la clasificación de datos, la Organización de Estados Americanos [OEA, 2019] señala principios comunes entre los gobiernos, las organizaciones no gubernamentales y las organizaciones comerciales donde se destaca la apertura, transparencia y valores sociales cuya clasificación debe usarse con precaución y de acuerdo con la sensibilidad, el valor y la criticidad de los datos. También reitera dar importancia al enfoque basado en el contenido clasificado en función de sus riesgos asociados, compromisos y contenido, independientemente de su formato de archivamiento, medios u origen. El Enfoque de gestión de riesgos proporciona protección a la información de acuerdo al nivel de sensibilidad, valor y criticidad de esta. Otro principio elemental es la Proporcionalidad de la información. Otro principio es las responsabilidades claras con respecto a los permisos a causa de la clasificación de datos, la

política y los procesos deben asignarse para optimizar la seguridad de la información dentro de la organización. Finalmente, el principio del Enfoque del ciclo de vida como parte de un sistema de gestión de la información debe tener en cuenta la información durante todo el ciclo de vida (Pérez y Ramos, 2020, p.12).

El Informe de la Revisión de Capacidades de Ciberseguridad de la República Federativa del Brasil, realizado por el Departamento de Seguridad de la Información (DSI) de la Oficina de Seguridad Institucional de la Presidencia de la República señala que este país no tiene un marco regulatorio que proteja la seguridad cibernética, es por ello que han adoptado varias directrices oficiales o "leyes blandas" que se refieren a cuestiones de seguridad cibernética como La Ley de Delitos Cibernéticos (Ley Nº 12.737/2012), también conocida como la Ley Carolina Dieckmann, y el Marco Civil de Internet de Brasil (Ley Nº 12.965/2014), ambas son consideradas instrumentos legislativos vigentes pertinentes. Se precisa además que en diciembre de 2019, Brasil inició su adhesión al Convenio de Budapest, en calidad de observador (Polo, 2020, p.45).

Por otro lado, el estudio sobre Estado de la Ciberseguridad en el Sistema Financiero Mexicano del 2019, proviene de una base de datos de 240 entidades e instituciones financieras participantes del Sistema Financiero Mexicano. Se resalta que un 73% del total de las entidades bancarias del país impulsan planes de seguridad de la información y un 55% fomentan la concientización, educación y capacitación y asignando mayor presupuesto (Organización de los Estados Americanos [OEA], 2018).

En lo referente al recurso humano en ciberseguridad, existe una falta de profesionales calificados a nivel mundial. Al respecto, el informe sobre ISC $^{(2)}$, Cybersecurity Workforce Study (2020) estima que existe un déficit global de 3.12 millones de profesionales en ciberseguridad (ISC $^{(2)}$, 2020), en este contexto, el estudio The State of Industrial Cybersecurity

del 2019, reveló que el 65% de las empresas señalaron una falta de personal con habilidades y capacidades suficientes para administrar problemas como ataques de ciberseguridad (Kaspersky, 2021).

2.2. Bases Teóricas

2.2.1. Ciberseguridad

Es el conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, seguros y tecnologías para proteger los activos de la organización y los usuarios (Unión Internacional de Telecomunicaciones [ITU], 2008).

De acuerdo a los expertos de Information Systems Audit and Control Association (ISACA, 2018) la ciberseguridad se define como "una capa de protección para los archivos de información" (Vásquez, 2019).

En este sentido, la ciberseguridad es el ejercicio de proteger sistemas, redes y programas de ataques digitales que buscan el acceso, modificación o destrucción de información crítica a fin de extorsionar a los usuarios o interrumpir la continuidad del negocio (Carlini, 2016).

En el presente estudio se define ciberseguridad como el conjunto de herramientas normativas y prácticas que permiten generar niveles de protección de los activos críticos y continuidad del servicio de una entidad frente a ciberataques.

2.2.1. Características de la Ciberseguridad.

La Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations del NIST, refiere que la ciberseguridad se basa en tres pilares fundamentales: confidencialidad, integridad y disponibilidad (ISO, 2018).

El Center for Internet Security (CIS) considera que las características principales de la ciberseguridad incluyen la autenticación, que verifica la identidad de los usuarios y sistemas; la autorización, que otorga privilegios y permisos adecuados; y la disponibilidad, que garantiza que los sistemas y datos estén accesibles y funcionando correctamente (ISO, 2018).

El informe Cybersecurity Culture in Organizations, la European Union Agency for Cybersecurity (ENISA) menciona que la confidencialidad se refiere a que la información solo sea accesible para personas autorizadas. Por su parte, la integridad busca proteger la información de variaciones no autorizadas. La disponibilidad garantiza que los sistemas y datos estén accesibles en cualquier momento (ISO, 2018).

Al respecto, para Aguilar (2014) la conservación de la confidencialidad de la información digital se debe entender como la no divulgación de información hacia terceras instituciones o personal no autorizado. El autor añade que la confidencialidad tiene como eje principal la capacidad de control de la entidad en el resguardo de la información como activos críticos de alta sensibilidad, para que no sea materia de acceso o sea difundida sin la autorización debida; impactando negativamente en los procesos de funcionamiento de la institución pública. Al respecto, Escalante (2018) indica que la confidencialidad también está ligada a la protección de datos vinculados a maquinas industriales de producción. Refiere además que la integridad de la información se define como la protección y mantenimiento de la información sin alteración obtenida a través de la comunicación que fluye en el ciberespacio. Así también, la International Organization for Standardization (ISO, 2018) en su numeral 6.4.2 señala que la pérdida de integridad se produce al dañar un activo crítico (considerando a la información sensible como tal) por medio de una modificación sin autorización.

La disponibilidad en términos de ciberseguridad consiste en el acceso pleno, necesario y debidamente autorizado a las aplicaciones, recursos y servicios alojados en el ciberespacio.

Para Cuartas (2007), la disponibilidad es uno de los tres pilares de la ciberseguridad junto a la confiabilidad e integridad, que garantiza acceso a la información cada vez que se requiera acceder a ella. Por otro lado, Dermutas (2020) afirma que la disponibilidad es una propiedad de acceso acreditado a ordenadores, datos y redes informáticas que son atacadas por los ciberdelincuentes y generan condiciones para la denegación de los servicios. Se infiere que la disponibilidad es el acceso debidamente autorizado a recursos informáticos pertenecientes a los activos de la entidad, con la finalidad de acceder en el momento que sea requerido (Arias et al., 2015, p.89).

Asimismo, la Autenticación de la Información, según Open Web Application Security Project (OWASP) es el proceso de verificar que los datos transmitidos o almacenados son genuinos y provienen de una fuente autorizada. Esto se logra mediante el uso de métodos criptográficos y protocolos de seguridad, como el cifrado de datos, el uso de claves de autenticación y la verificación de la integridad de los datos. La autenticación de la información es esencial para proteger la confidencialidad, la integridad y la disponibilidad de la información en entornos digitales. (Alfaro, 2008). En el ámbito de la seguridad informática, El National Institute of Standards and Technology (NIST) define a la autenticación de la información como el proceso de verificar la identidad de un usuario o entidad que accede a un sistema o recurso. Esto implica la validación de las credenciales proporcionadas por el usuario, como un nombre de usuario y una contraseña, un certificado digital o una huella dactilar. La autenticación de la información ayuda a garantizar que solo los usuarios autorizados puedan acceder a la información o recursos protegidos, por lo que se evita el acceso no autorizado y los posibles ataques. Dentro de este marco, la línea de estudio Oracle Corporation (ORACLE) refiere a la autenticación como el proceso de confirmar que la información transmitida o almacenada no ha sido modificada y proviene de una fuente legítima. Se utilizan diversos métodos para lograr la autenticación de la información, como el uso de algoritmos de resumen (hash), la

encriptación de datos y la verificación de la integridad de los mensajes. La autenticación de la información es esencial en ámbitos como la seguridad de la información, la protección de datos y la prevención del fraude. (SBS, 2019). Por lo anteriormente analizado se define Autenticación de la Información como el proceso de verificación por el cual los datos transmitidos sean genuinos, auténticos y de fuente confiable, usando diversos métodos de autenticación como algoritmos y encriptamientos.

Es así, que estos pilares son muy relevantes en términos de la ciberseguridad los cuales permiten una orientación correcta al tratamiento de la información. Según los aportes de los autores citados esta relación entre las propiedades y la utilidad de la ciberseguridad asegura la propuesta de un criterio objetivo en el tratamiento de la protección de la información como bien intangible que amerita resguardo.

2.2.3. Factores positivos en la construcción de la Ciberseguridad

La construcción de la ciberseguridad implica una serie de factores positivos que contribuyen a fortalecer la protección de los sistemas y datos digitales. Se destaca al respecto, la Conciencia y educación, que según Aquino et al. (2009), una mayor conciencia sobre los riesgos y las mejores prácticas de ciberseguridad es fundamental. La educación en ciberseguridad ayuda a los individuos a comprender las amenazas y adoptar comportamientos seguros en línea. Otro elemento relevante es la Colaboración y cooperación, que según el Center for Strategic and International Studies (CSIS) la ciberseguridad es un esfuerzo colectivo donde los roles de los gobiernos, empresas, instituciones académicas y organizaciones internacionales, son esenciales para compartir información sobre amenazas, desarrollar estándares comunes y responder de manera coordinada a los incidentes.

Otro aspecto son los avances tecnológicos. Para el Instituto Internacional de Seguridad Cibernética (IICS), el avance constante de la tecnología también aporta beneficios a la ciberseguridad. Por ejemplo, el desarrollo de herramientas de seguridad más sofisticadas, como soluciones de detección de intrusiones, análisis de comportamiento y cifrado, ayuda a proteger los sistemas y datos contra amenazas cada vez más complejas.

El Marco legal y las regulaciones son claves también. Al respecto, La Comisión Europea (EC) propone que los marcos legales y las regulaciones relacionadas con la ciberseguridad juegan un papel crucial en la protección de los sistemas y datos. Estas normativas establecen requisitos y estándares de seguridad que las organizaciones deben seguir, lo que contribuye a una mayor protección de la información y proporciona un marco de responsabilidad.

La Inversión en seguridad, es un factor importante. Para Gartner Inc. (GARTNER) la asignación de recursos adecuados para la ciberseguridad es esencial. Las organizaciones y los gobiernos que invierten en la implementación de medidas de seguridad sólidas, como sistemas de prevención de intrusiones, firewalls, autenticación multifactorial y capacitación del personal, están mejor preparados para defenderse contra las amenazas cibernéticas.

Asimismo, la evaluación y mejora continua. Según el Institute (SANS) señala que la ciberseguridad como un proceso en constante evolución. La evaluación constante de los sistemas, las políticas y los procedimientos de seguridad, junto con la mejora sostenible de las medidas de protección, permite adaptarse a las nuevas amenazas y mantener un nivel óptimo de seguridad.

García (2017) agrega que la ciberseguridad desempeña un papel fundamental en la estrategia de seguridad nacional de muchos países, incluida la Policía Nacional del Perú (PNP),

esta se integra en las estrategias de seguridad nacional en general, las cuales están contempladas dentro del marco legal, además de la protección de la información digital y la protección de infraestructuras.

2.2.4. La protección de la información digital

Este aspecto está enmarcado en la definición de la seguridad de la información, relacionado con la seguridad informática por lo que la descripción teórica es importante en los objetivos de la presente investigación. La protección de la información digital en las entidades públicas, se tiene sobre la seguridad de los activos críticos registrados en la base de datos, servidores o unidades de almacenamiento externo. En esta línea, se afirma que las actividades cotidianas de las empresas y del sector público requieren del correcto funcionamiento de los sistemas y redes informáticas y de su seguridad (Gómez, 2011, p.38). Este aporte busca garantizar la seguridad y protección de los activos digitales registrados; al respecto, Gómez (2011) sugiere dar énfasis a medidas que impidan la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos resultados pueden generar peligro o daños a la información (p. 38). Sugiere el especialista que estas medidas de seguridad digital o electrónica, deben implementarse en las redes informáticas, con la finalidad de administrar y controlar los accesos de usuarios no autorizadas a las redes de servicio informático.

2.2.5. Gestión de incidentes de la seguridad de la información

Se encuentra relacionada con la administración en la seguridad de la información, refiriéndose a la protección de activos críticos de la entidad. Gómez (2011, p. 52) sostiene que parte del sistema general de gestión comprende la política instaurada, la estructura organizativa, los recursos necesarios, los procedimientos y procesos necesarios para poner en marcha la gestión de la seguridad de la información en una entidad.

Los resultados de la evaluación y análisis de riesgos conducen a la elaboración de la política de seguridad, en la cual el documento que indica el compromiso y apoyo de la dirección, así como la definición del papel que debe jugar en la consecución de la misión y visión de la organización. En esencia se documenta para que se explique la necesidad de seguridad de la información (y sus principios) a todos los usuarios de los recursos de información.

2.3. Marco Conceptual

La ciberseguridad es un ámbito estratégico y operativo que implica un conjunto integral de herramientas, políticas, estándares y prácticas diseñadas para salvaguardar y fortalecer la protección de los activos críticos y la continuidad de los servicios de una entidad frente a una variedad de ciberataques Abarca aspectos técnicos y organizativos. El ámbito técnico, se refiere a la implementación de soluciones tecnológicas avanzadas, como firewalls, sistemas de detección de intrusiones, encriptación y autenticación multifactorial. Aquí el objetivo de mitigar y prevenir amenazas cibernéticas. Además, incluye la gestión proactiva de parches y actualizaciones de software para cerrar posibles brechas de seguridad (Seminario, 2020). Desde una perspectiva organizativa, la ciberseguridad permite la formulación y aplicación de políticas y procedimientos internos coherentes. Abarca, además, la formación y concientización de los empleados sobre las mejores prácticas de seguridad cibernética, la creación de una cultura de seguridad en la que la protección de la información sea una prioridad, y la planificación de respuestas efectivas ante incidentes en caso de que ocurran ciberataques (Amish y Velázquez, 2014).

La confidencialidad se enfoca en garantizar que la información sensible y crítica de una entidad sea accesible a personas autorizadas. La falta de confidencialidad perjudica gravemente los procesos normales de la institución (Alfaro, 2008).

La integridad busca que la información no sea alterada de manera no autorizada o malintencionada. Mantener la integridad de los datos es esencial para garantizar que la información sobre la cual se toman decisiones importantes sea precisa y confiable.

La disponibilidad garantiza que los recursos y la información estén accesibles cuando sean necesarios. Esto implica que los sistemas y servicios críticos no sufran interrupciones inesperadas y que los usuarios autorizados puedan acceder a ellos de manera oportuna. La falta de disponibilidad podría afectar negativamente la productividad y la capacidad de operación de la entidad.

La autenticación se refiere al proceso de verificar la identidad de un usuario o entidad que intenta acceder a los sistemas o recursos. Dicho elemento se obtiene a través de diversos métodos, como contraseñas, autenticación de dos factores y biometría. La autenticación garantiza que solo aquellos con los permisos adecuados puedan acceder a la información y los servicios, reduciendo así el riesgo de accesos no autorizados.

En línea con la mencionado por la National Cybersecurity Alliance (NCA), es importante que se destaque la promoción de la conciencia y la educación en ciberseguridad. Una mayor conciencia sobre los riesgos asociados con el entorno cibernético y la adopción de las mejores prácticas de seguridad son consideradas de vital importancia.

La educación en ciberseguridad desempeña un papel esencial al capacitar a las personas para que comprendan las diversas amenazas que acechan en el mundo en línea. A través de la educación, los individuos adquieren un conocimiento profundo sobre las tácticas utilizadas por los ciberdelincuentes y las potenciales vulnerabilidades en sus propios dispositivos y sistemas. Esto, a su vez, capacita a las personas para reconocer y enfrentar los riesgos de manera proactiva, no solo se trata de conocer las amenazas, sino también de adoptar comportamientos

seguros en línea. Esta formación empodera a los individuos para tomar decisiones informadas al utilizar tecnologías digitales, identificar posibles intentos de estafa o phishing, y aplicar medidas de protección adecuadas. Además, al entender cómo se producen las violaciones de seguridad y cómo prevenirlas, los individuos pueden contribuir activamente a la construcción de un entorno cibernético más seguro y resistente.

Según la perspectiva del Center for Strategic and International Studies (CSIS), se subraya la importancia de la colaboración y la cooperación en el ámbito de la ciberseguridad. Según esta visión, la ciberseguridad se concibe como un esfuerzo colectivo que demanda la participación activa y coordinada de diversos actores en la comunidad global.

La colaboración entre distintos protagonistas, que incluyen gobiernos, empresas, instituciones académicas y organizaciones internacionales, emerge como un pilar esencial en la construcción de un entorno cibernético más seguro. El intercambio de información sobre amenazas cibernéticas se convierte en un elemento clave para anticipar y mitigar posibles ataques. A través de la colaboración, estos actores pueden compartir inteligencia sobre tácticas de ciberdelincuentes, vulnerabilidades descubiertas y estrategias de prevención, contribuyendo así a la creación de un conocimiento más amplio y efectivo en la lucha contra las amenazas digitales.

Otro aspecto crucial de la colaboración es el desarrollo de estándares comunes en ciberseguridad. Al establecer pautas y normativas compartidas, se facilita la creación de un marco global para abordar los desafíos de seguridad en línea. Estos estándares no solo mejoran la interoperabilidad entre sistemas y plataformas, sino que también proporcionan un enfoque unificado para evaluar y gestionar los riesgos cibernéticos.

La cooperación se extiende aún más en la respuesta a incidentes cibernéticos. La capacidad de responder de manera coordinada y eficiente a ataques cibernéticos requiere una estrecha cooperación entre los actores involucrados. Esto implica la compartición oportuna de información sobre incidentes, la identificación de medidas de contención y la permanente coordinación para minimizar el impacto y mitigar las amenazas.

De acuerdo al Instituto Internacional de Seguridad Cibernética (IICS), los avances tecnológicos desempeñan un papel crucial en la mejora de la ciberseguridad. La evolución constante de la tecnología no solo introduce nuevas oportunidades, sino que también aporta beneficios al campo de la ciberseguridad la cual permite una mayor protección y resiliencia contra amenazas digitales en constante evolución. Una prueba de ello son las soluciones de detección de intrusiones que aprovechan técnicas de monitoreo y análisis en tiempo real para identificar patrones de comportamiento anómalos que detectan ataques. Por otra parte, el análisis de comportamiento basado en algoritmos evalúa el comportamiento típico de los usuarios y sistemas para detectar desviaciones que podrían ser indicativas de actividad maliciosa. A su vez, el cifrado, otro avance tecnológico, protege la confidencialidad de los datos al convertir la información en un formato ilegible para cualquier persona que no tenga la clave de descifrado adecuada. De esta forma se salvaguardar la privacidad y la integridad de los datos transmitidos y almacenados.

Según la propuesta de la Comisión Europea (EC), el marco legal y las regulaciones desempeñan una función fundamental en la salvaguardia de los sistemas y datos en el contexto de la ciberseguridad. La importancia de estos marcos radica en la necesidad de establecer lineamientos claros y requisitos concretos para garantizar la seguridad digital en un entorno cada vez más conectado. Además de definir los estándares técnicos, las regulaciones también desempeñan un rol en la creación de un marco de responsabilidad. Es decir, al establecer

responsabilidades claras para las organizaciones y las partes involucradas en la gestión de datos y sistemas digitales, las regulaciones fomentan una mayor rendición de cuentas en caso de incidentes cibernéticos que no solo genera una mayor transparencia, sino que también proporciona incentivos para que las organizaciones adopten medidas preventivas y de mitigación (Areitio, 2008).

El marco legal y las regulaciones también pueden tener un alcance transfronterizo. En un mundo cada vez más interconectado, donde las amenazas digitales pueden trascender fronteras, las regulaciones a nivel regional o internacional pueden ser cruciales para establecer un enfoque unificado en la lucha contra el cibercrimen y la protección de la información sensible.

Según Gartner Inc., las organizaciones y los gobiernos que optan por invertir en ciberseguridad reconocen la necesidad de implementar medidas de seguridad sólidas y eficaces. Estas medidas pueden abarcar una variedad de enfoques, incluyendo la implementación de sistemas de prevención de intrusiones, la adopción de firewalls avanzados, la implementación de autenticación multifactorial y la formación continua del personal. (Borrero, 2015).

La inversión en sistemas de prevención de intrusiones permite la detección temprana y la respuesta rápida ante posibles amenazas cibernéticas. Estos sistemas monitorean continuamente la actividad en línea y alertan sobre actividades sospechosas o no autorizadas.

Los firewalls, por su parte, actúan como una barrera de protección fundamental al bloquear el acceso no autorizado a sistemas y redes. Estos elementos son esenciales para reducir la superficie de ataque y prevenir intrusiones no deseadas.

La autenticación multifactorial es un método de seguridad que exige múltiples formas de verificación para acceder a sistemas o datos sensibles. Esta técnica añade una capa adicional de protección al requerir no solo contraseñas, sino también otros factores como códigos temporales o reconocimiento biométrico. Además de las soluciones técnicas, la inversión en capacitación y formación del personal es clave para fomentar una cultura de seguridad sólida. Al educar a los empleados sobre las mejores prácticas de ciberseguridad y el reconocimiento de amenazas potenciales, las organizaciones pueden fortalecer su primera línea de defensa contra ataques cibernéticos.

El enfoque del SANS Institute, señala que la ciberseguridad se caracteriza como un proceso en continua evolución. Este enfoque reconoce la naturaleza dinámica y en constante cambio de las amenazas cibernéticas y la necesidad de mantener una postura de seguridad adaptable y efectiva. La evaluación y mejora continua son pilares esenciales en este enfoque. La evaluación periódica de los sistemas, políticas y procedimientos de seguridad puede abarcar pruebas de penetración, auditorías de seguridad y análisis de riesgos, entre otros métodos.

La mejora continua, en consecuencia, según Carlini (2016) se basa en los resultados de estas evaluaciones. Consiste en la implementación de medidas correctivas y preventivas para abordar las debilidades identificadas. Esta etapa también involucra la adaptación a nuevas amenazas y la incorporación de las lecciones aprendidas de incidentes anteriores. La mejora continua no solo se trata de corregir problemas, sino de mantener una postura de seguridad proactiva y en constante actualización.

Este enfoque dinámico de la ciberseguridad es fundamental para enfrentar los desafíos cambiantes del panorama cibernético. Las amenazas y las tácticas de los ciberdelincuentes evolucionan con rapidez, lo que hace necesario mantenerse ágil y receptivo a las nuevas circunstancias. La evaluación y mejora continua garantizan que las medidas de protección se

mantengan efectivas y que la organización esté preparada para contrarrestar las amenazas emergentes.

En el contexto de la investigación, se enfatiza la importancia de la protección de la información digital, un componente intrínseco de la seguridad de la información y su relación estrecha con la seguridad informática. La comprensión teórica de este concepto se revela como esencial para los objetivos que se persiguen en el estudio.

La protección de la información digital, como parte de la seguridad de la información, abarca un conjunto de medidas y prácticas diseñadas para salvaguardar la integridad, confidencialidad y disponibilidad de los datos en entornos digitales.

Estos datos, albergados en bases de datos, servidores y unidades de almacenamiento externo, pueden ser considerados activos críticos debido a su valor y relevancia para el funcionamiento de las entidades públicas.

En el contexto de las entidades públicas, la protección de la información digital asume un rol crucial en la preservación de la confidencialidad de los activos críticos. La seguridad de estos activos es vital para asegurar que la información sensible y estratégica no se vea comprometida por accesos no autorizados o manipulación malintencionada.

Además, la protección de la información digital se extiende a garantizar la integridad de los datos, evitando su alteración o corrupción, y a asegurar la disponibilidad de la información cuando sea necesaria para el funcionamiento continuo de la entidad.

Haro (2019) sostiene que la información digital es un componente fundamental en las operaciones y la toma de decisiones en las entidades públicas, su protección se convierte en un objetivo primordial. La adopción de políticas, procedimientos y tecnologías de seguridad

adecuados aporta a la mitigación de riesgos cibernéticos y al fortalecimiento de la resiliencia frente a amenazas digitales (p.34).

Por otra parte, la gestión de incidentes de seguridad de la información se refiere al conjunto de políticas, procesos, procedimientos y recursos destinados a identificar, evaluar, mitigar y resolver incidentes relacionados con la seguridad de los activos digitales. Esto incluye elementos como la formulación de políticas claras, la estructura organizativa dedicada a la seguridad de la información, la asignación de los recursos necesarios y la implementación de procedimientos y procesos que permitan la gestión efectiva de los incidentes (Hernandez, 2018).

La gestión de incidentes de seguridad de la información se basa en un enfoque proactivo y reactivo. Por un lado, busca prevenir y minimizar los riesgos a través de la identificación temprana de vulnerabilidades, la implementación de controles de seguridad y la educación continua del personal. Por otro lado, se prepara para responder de manera adecuada y eficiente a los incidentes cuando se producen, lo que incluye la contención del incidente, la recuperación de los sistemas afectados y la posterior investigación forense para comprender su alcance y origen (Cuartas, 2017).

2.4. Marco Legal

Política Nacional de Ciberseguridad tiene como objetivo la protección de la infraestructura de información, datos e información de las entidades públicas y de la tecnología utilizada en su procesamiento a fin de asegurar las propiedades de la información (Galindo, 2005).

Directiva No 004-2009-IN-0801. Uso correcto de Equipos de cómputo, servicios de red, internet y correo electrónico, mediante el cual se optimiza el uso de los equipos

informáticos, internet, intranet y correos electrónicos institucionales en el que se garantiza la eficiencia de los mismos.

Directiva No 006-2013-IN Normas para el acceso y uso de los Servicios de Red e Internet, establece mecanismos que garantizan la integridad de la red, mediante el correcto uso y control de la intranet e internet para así contribuir al mejor uso de los servicios tecnológicos.

Directiva No 012-2013-IN Normas para el Acceso y Uso del Servicio de Correo Electrónico Institucional, mediante criterio técnicos permite el uso correcto, control y administración de los correos institucionales. De esta forma se asegura la calidad de comunicación para ejecutar los servicios informáticos.

Políticas de Seguridad de la Información de la Policía Nacional del Perú, tiene como finalidad mantener altos niveles en las propiedades de la información respecto a los activos críticos, capacidades reactivas frente a las amenazas o accesos no autorizados.

Directiva N° 003-2014-IN-DGTIC Normas para la Administración y Legalidad del Software permite normar la administración y legalidad del software adquirido y utilizado en el Ministerio del Interior.

Resolución Ministerial Nº 004-2016-PCM, aprueba el uso de la **Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI**. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática.

III. MÉTODO

3.1. Tipo de investigación

Es de enfoque cuantitativo, de tipo básica; puesto que se logró acrecentar el conocimiento teórico en el que se promueve nuevos conocimientos y está orientada a conocer a profundidad cómo se desarrolla el problema. Al respecto, según Hernández *et al.* (2014), señala que este tipo de investigación persigue las generalizaciones ya que se basa en principios y leyes acerca del fenómeno estudiado.

3.1.1. Diseño de investigación

El diseño utilizado es el no experimental puesto que las variables al ser analizadas y observadas en el contexto natural no son manipuladas ni sometidas a ningún experimento (Hernández *et al.*, 2014, p. 56).

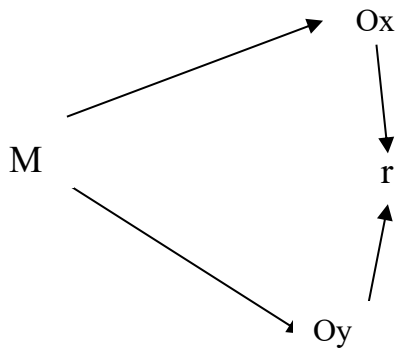
3.1.2. Nivel de Investigación

El nivel de la investigación es correlacional, dado que permite medir el nivel de asociación estadística entre las variables sin influencia de ninguna variable extraña (Arias, 2020).

3.1.3. Según el periodo de tiempo

Según el periodo temporal, la investigación es transversal ya que los datos del estudio muestral serán recolectados en base a un determinado rango de tiempo concreto sobre una muestra predefinida (Hernández *et al.*, 2014, p.34).

Por lo tanto, el esquema del diseño correlacional es:



Dónde:

M= muestra

OX = Observación de la variable X

OY= Observación de la variable Y

R= Indica la relación entre las variables X e Y

3.2 Población y muestra

3.2.1. Población

Según Hernández et al. (2014) una población o universo es un conjunto de elementos homogéneos de los cuales se pretende indagar y conocer sus características. La población consiste en los colaboradores especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP, pertenecientes a la ciudad de Lima, personal que cuenta con amplia experiencia teórica y técnica de la problemática, lo que permitirá generar conclusiones y recomendaciones a la Alta Dirección de la PNP acerca de la seguridad en la protección de la información digital.

3.2.2. Muestra

La muestra tomada son los colaboradores especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP, que se encuentran en actividad. Se determinó un nivel de confianza del 95% (con el cual **α** = 0.05 y, por tanto, se sabe que Z = Z 0.25 = 1.96) y un error del 5% (con lo que = 0.05).

Se aplica la fórmula de la muestra:

$$n = (Z^2pqN) / (Ne^2 + Z^2pq)$$

Nivel de confianza (Z) = 1.96

Grado de error (e) = 0.05

Universo (N) = 300 especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP.

Probabilidad de ocurrencia (p) = 0.5

Probabilidad de no ocurrencia (q) = 0.5

Se llegó a obtener un tamaño de muestra de:

n = 168 personas para encuestar en dos semanas.

3.3 Operacionalización de variables

3.3.1. Variables e indicadores

Los factores que tienen influencia en el problema de estudio reciben el nombre de variables. A una variable se les define como un término que puede tomar valores diferenciados o variantes (Sabino,1992).

3.3.2. Variable de supervisión

La Protección de la Información de la Policía Nacional del Perú, se define como las actividades que garantizan la estabilidad de las propiedades de la información registrada y almacenada en los centros de informática de la PNP.

3.3.3. Variable de asociación

La utilidad de la Ciberseguridad son los marcos teóricos y legales que influyen en la

infraestructura de hardware y software, con la finalidad de gestionar los procesos relacionados a la protección de la información.

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno (García, 2017).

3.3.4. Cuadro de operacionalización de variables

Tabla 3

Matriz de operacionalización de variables

Variables	Definición conceptual	Dimensiones	Sub Dimensiones	Indicadores	Tipo de variable
VARIABLE ASOCIADA: UTILIDAD CIBERSEGURIDAD	La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. (ITU, 2008)	PROPIEDADES DE LA INFORMACIÓN	Conservación de la Confidencialidad	Cantidad de ataques de intrusión detectados	Numérica
			Estado de la Integridad	Capacidad de resolución de incidentes	Categórica
			Disponibilidad de la información	Tiempo de acceso a la información	Numérica
		GESTIÓN DE ACTIVOS CRÍTICOS	Cumplimiento de los activos	Establecer políticas de gestión de activos	Categórica
			Reducir la vulnerabilidad	Prevención de ataques y seguridad en la nube	Categórica
			Mejora de la ciberseguridad	Desarrollar servicios antifraude	Categórica
VARIABLE DE SUPERVISIÓN: PROTECCIÓN DE LA INFORMACIÓN DIGITAL	Administrar y controlar los accesos de usuarios no autorizadas a las redes de servicio informático. (Gómez, 2011).	TRATAMIENTO DE LA INFORMACIÓN DIGITAL	Proceso de accesibilidad	Percepción de vulnerabilidad	Categórica
			Proceso normativo	Percepción de calidad	Categórica
			Proceso de seguridad	Percepción de incidencias	Categórica

3.4 Instrumentos

En la presente investigación para la recolección de datos según Hernández et al (2014) se utilizó la técnica primaria del cuestionario en la modalidad de encuesta con la finalidad de recopilar información directa de las personas. Fue dirigida a los especialistas que laboran en los diversos centros de informática que tiene la Policía Nacional el Perú.

Por otro lado, los datos se recolectaron mediante el instrumento cuestionario, que tiene como objetivo registrar las preguntas y respuestas, cuyos resultados permitirán recolectar información necesaria y deseada para la investigación. Adicionalmente, se utilizó la técnica de indagación documental que permitirá el acceso a registros de documentos y rutas estratégicas almacenados en los archivos de la PNP al cual se tiene acceso.

3.4.1 Validación y confiabilidad.

Para la realización de la validez de los instrumentos, Hernández *et al.* (2014) refiere que son cinco las estrategias para obtener un elevado grado de validez interna o adecuación de los resultados: selección de personas, saturación del campo, permanencia prolongada en el campo, análisis de casos negativos, contraste con los actores sociales. (p. 67).

Para determinar el Alfa de Cronbach se realizó una encuesta piloto con 20 encuestados, obteniéndose los siguientes resultados:

Tabla 4

Validación del instrumento - Alfa de Cronbach

	ITEMS													
ENCUESTADOS	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
E1	5	4	5	5	4	5	5	4	4	3	5	3	5	3
E2	5	4	4	5	4	5	5	4	4	4	5	3	4	5

E3	2	5	2	3	2	3	2	3	3	5	3	3	2	5
E4	2	3	3	3	3	3	3	3	2	4	3	3	2	5
E5	2	4	2	3	2	3	2	3	3	4	3	4	3	5
E6	2	5	2	4	2	4	2	4	3	5	3	5	2	5
E7	2	4	3	4	3	4	3	4	2	4	2	4	2	4
E8	2	5	2	4	2	5	2	4	3	4	2	3	2	4
E9	2	5	3	5	3	5	3	4	3	4	2	4	1	5
E10	2	5	2	5	2	4	2	4	3	4	2	4	1	5
E11	3	3	2	4	3	4	2	4	3	4	3	4	2	4
E12	2	4	3	5	3	5	3	5	3	5	2	4	2	4
E13	2	4	3	4	3	4	2	4	3	4	3	4	2	4
E14	3	5	2	4	2	4	3	4	3	5	3	5	2	4
E15	2	4	3	4	3	4	2	4	3	4	3	4	2	4
E16	3	5	2	4	3	3	3	3	3	3	3	3	2	3
E17	2	5	2	3	3	4	3	3	3	5	3	4	2	4
E18	2	5	3	4	3	4	3	4	3	4	3	4	2	4
E19	3	4	2	4	2	4	3	4	3	5	3	5	2	3
E20	2	5	3	4	3	4	3	4	3	5	3	5	2	3
Varianza	**0.850**	**0.440**	**0.628**	**0.448**	**0.388**	**0.448**	**0.760**	**0.260**	**0.200**	**0.388**	**0.648**	**0.490**	**0.760**	**0.528**

Tabla 5

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum {S_i}^2}{{S_T}^2}\right]$$

Coeficiente de confiabilidad

α:	Coeficiente de confiabilidad del cuestionario	0.75
k:	Número de ítems del instrumento	14
$\sum_{i=1}^{k} S_i^2$:	Sumatoria de las varianzas de los ítems.	7.233
S_t^2:	Varianza total del instrumento.	24.048

Tabla 6

Rangos de alfa de Cronbach

RANGO	CONFIABILIDAD
0.53 a menos	Confiabilidad nula
0.54 a 0.59	Confiabilidad baja
0.60 a 0.65	Confiable
0.66 a 0.71	Muy confiable
0.72 a 0.99	Excelente confiabilidad
1	Confiabilidad perfecta

El alfa de Cronbach calculada es de valor de 0.75, lo cual indica que es un instrumento de excelente confiabilidad.

3.5. Procedimientos

En la presente investigación se utilizó como instrumento el cuestionario para recopilar la información permitente para el análisis e interpretación de resultados.

Así mismo, se realizó la encuesta a la muestra establecida previamente, para posteriormente realizar el análisis y procedimiento de datos a través de gráficos y tablas para conocer los niveles y grados de relación entre las variables de estudio a través del Rho de Spearman. Por último, se realizó la discusión del estudio, las conclusiones y recomendaciones respectivas de la presente investigación.

3.6 Análisis de datos

En la presente investigación el análisis de datos consistió en el alcance descriptivo y correlacional utilizando el software IBM SPSS 25 Statistics.

Por otro lado, la base de datos se concretó con las encuestas que se realizó a los

especialistas que laboran en los centros informáticos de la PNP. Finalmente, se procedió a generar histogramas y tablas de contingencia producto del análisis descriptivo que permitirá contrastar la hipótesis planteada, de acuerdo a los resultados estadísticos.

3. 7 Consideraciones éticas

Se cumple con las disposiciones del Código de Ética de la Universidad Nacional Federico Villarreal, según Resolución No 251-2011-R-COG-UNFV. Así también, se ha considerado el Decreto Legislativo N.º 822 del 24 de abril de 1996 acerca de los derechos de Autor, se incluye, la Ley de Protección de Datos Personales, Ley N. º29733 en respeto de la reserva de sensibilidad de datos y anonimato, y el Decreto Legislativo N.º 1267, Ley de la Policía Nacional del Perú que regula el régimen disciplinario de la PNP.

IV. RESULTADOS

4.1 Resultados inferenciales

4.1.1 Alfa de Cronbach: Análisis e interpretación de la información

Se realizó el análisis del instrumento para determinar la confiabilidad de la realización del instrumento, empleando el coeficiente alfa de Cronbach.

Tabla 7

Alfa de Cronbach del instrumento

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,919	14

Resumen de procesamiento de casos

		N	%
Casos	Válido	168	100,0
	Excluido[a]	0	,0
	Total	168	100,0

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

Se aplicó el alfa de Cronbach para determinar confiabilidad de los instrumentos es confiable. Por lo que el instrumento de la presente investigación tiene una confiabilidad de 0,919, lo cual indica que es un instrumento de alta confiabilidad.

4.1.2 Prueba de hipótesis – análisis inferencial

4.1.2.1 Contrastación de hipótesis

Dentro de este marco, se aplicó la correlación de variables a través del estadístico no paramétrico: El Rho Spearman para identificar el grado de relación e influencia de ambas variables.

Hipótesis general:

Existe una relación directa entre la utilidad de la ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023.

Nivel de Significación

El nivel confiabilidad consiste en el 95%

Función de Prueba

Análisis con el Rho de Spearman.

Cálculos

Tabla 8

Hipótesis general

Correlaciones

			CIBERSEGURIDAD	PROTECCIÓN DE LA INFORMACIÓN DIGITAL
Rho de Spearman	UTILIDAD CIBERSEGURIDAD	Coeficiente de correlación	1,000	,753**
		Sig. (bilateral)	.	,000
		N	168	168
	PROTECCIÓN DE LA INFORMACIÓN DIGITAL	Coeficiente de correlación	,753**	1,000
		Sig. (bilateral)	,000	.
		N	168	168

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

Interpretación:

Según los resultados del análisis a través del Rho de Spearman, se concluye que si existe una relación directa entre la utilidad de la ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023 puesto que el coeficiente de la correlación fue de 0,753 y es una correlación positiva considerable.

Hipótesis específica 1:

Existe una relación directa entre las propiedades de la información y la protección de la información digital de la Policía Nacional del Perú, 2023.

Nivel de Significación

El nivel confiabilidad consiste en el 95%

Función de Prueba

Análisis con el Rho de Spearman.

Cálculos

Tabla 9

Hipótesis específica 1

Correlaciones

			PROPIEDADESDELAINFORMACION	PROPIEDADESDELAINFORMACIONDIGITAL
Rho de Spearman	PROPIEDADESDELAINFORMACION	Coeficiente de correlación	1,000	,684**
		Sig. (bilateral)	.	,000
		N	168	168
	PROPIEDADESDELAINFORMACIONDIGITAL	Coeficiente de correlación	,684**	1,000
		Sig. (bilateral)	,000	.
		N	168	168

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

Interpretación:

Según los resultados del análisis a través del Rho de Spearman: Se concluyó que, si existe una relación directa entre las propiedades de la información y la protección de la Información digital de la Policía Nacional del Perú, 2023. Puesto que; el coeficiente de la correlación fue de 0,684 y es una correlación positiva considerable.

Hipótesis específica 2:

Existe una relación directa entre la gestión de activos críticos y la protección de la información digital de la Policía Nacional del Perú, 2023.

Nivel de Significación

El nivel confiabilidad consiste en el 95%

Función de Prueba

Análisis con el Rho de Spearman.

Cálculos

Tabla 10

Hipótesis específica 2

Correlaciones

			GESTIONDEACTIVOSCRITICOS	PROPIEDADESDELAINFORMACIONDIGITAL
Rho de Spearman	GESTION DE ACTIVOS CRITICOS	Coeficiente de correlación	1,000	,990*
		Sig. (bilateral)	.	.
		N	168	168
	PROPIEDADES DE LA INFORMACION DIGITAL	Coeficiente de correlación	,990*	1,000
		Sig. (bilateral)	.	.
		N	168	168

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

Interpretación:

Según los resultados del análisis a través del Rho de Spearman: Se concluyó que, si existe una relación directa entre la gestión de los activos críticos y la protección de la información digital de la Policía Nacional del Perú, 2023. Puesto que; el coeficiente de la correlación fue de 0,990 y es una correlación positiva perfecta.

4.1.3 Análisis descriptivos

Tabla 11

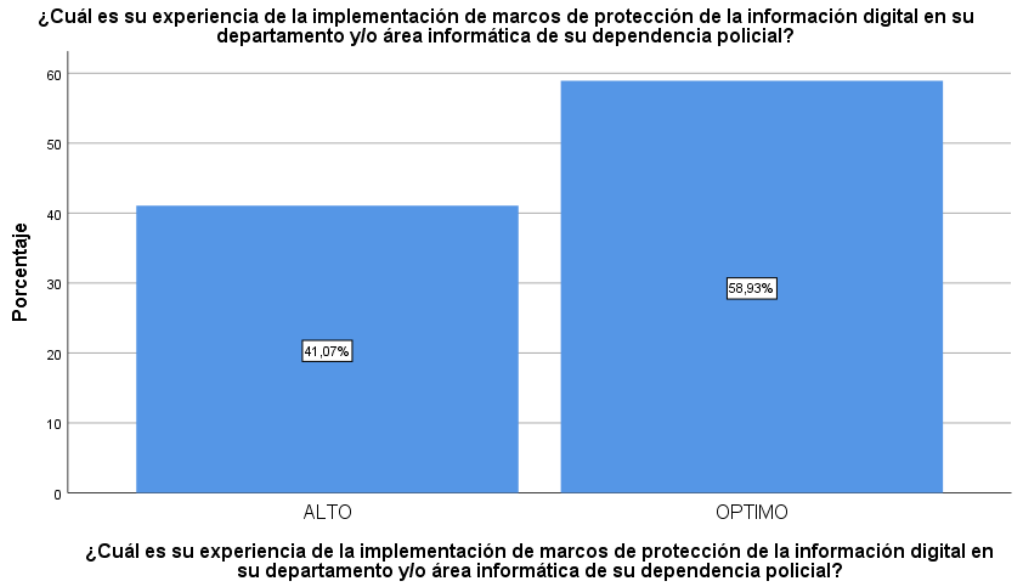
Items 1

¿Cuál es su experiencia de la implementación de marcos de protección de la información digital en su departamento y/o área informática de su dependencia policial?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALTO	69	41,1	41,1	41,1
	OPTIMO	99	58,9	58,9	100,0
	Total	168	100,0	100,0	

Figura 3

Items 1



Interpretación: De la tabla 11 y figura 1, el 58,9% de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la implantación de marcos de protección de información digital dentro del área de informática es óptima, mientras que el 41% indica que es alto.

Tabla 12

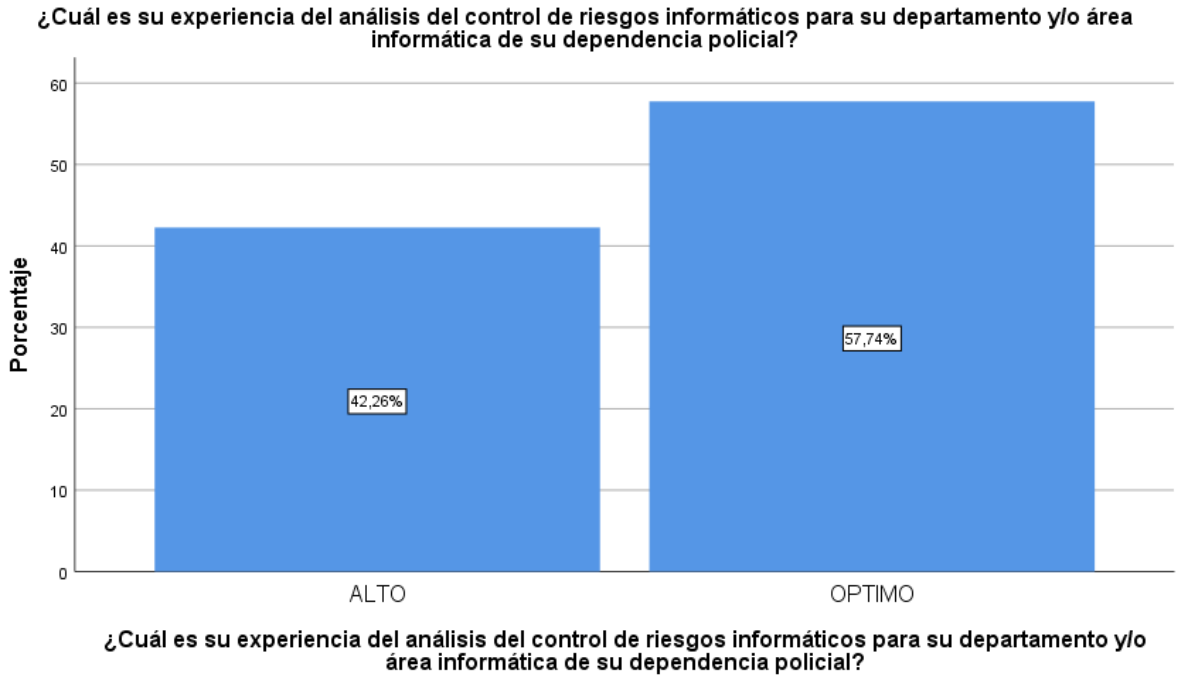
Items 2

¿Cuál es su experiencia del análisis del control de riesgos informáticos para su departamento y/o área informática de su dependencia policial?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALTO	71	42,3	42,3	42,3
	OPTIMO	97	57,7	57,7	100,0
	Total	168	100,0	100,0	

Figura 4

Items 2



Interpretación: De la tabla 12 y figura 2, el 57,7% de especialistas que laboran en las Oficinas

de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la experiencia del análisis del control de riesgos informáticos dentro de su dependencia policial es óptima, mientras un 42,3% indica que es alto.

Tabla 13

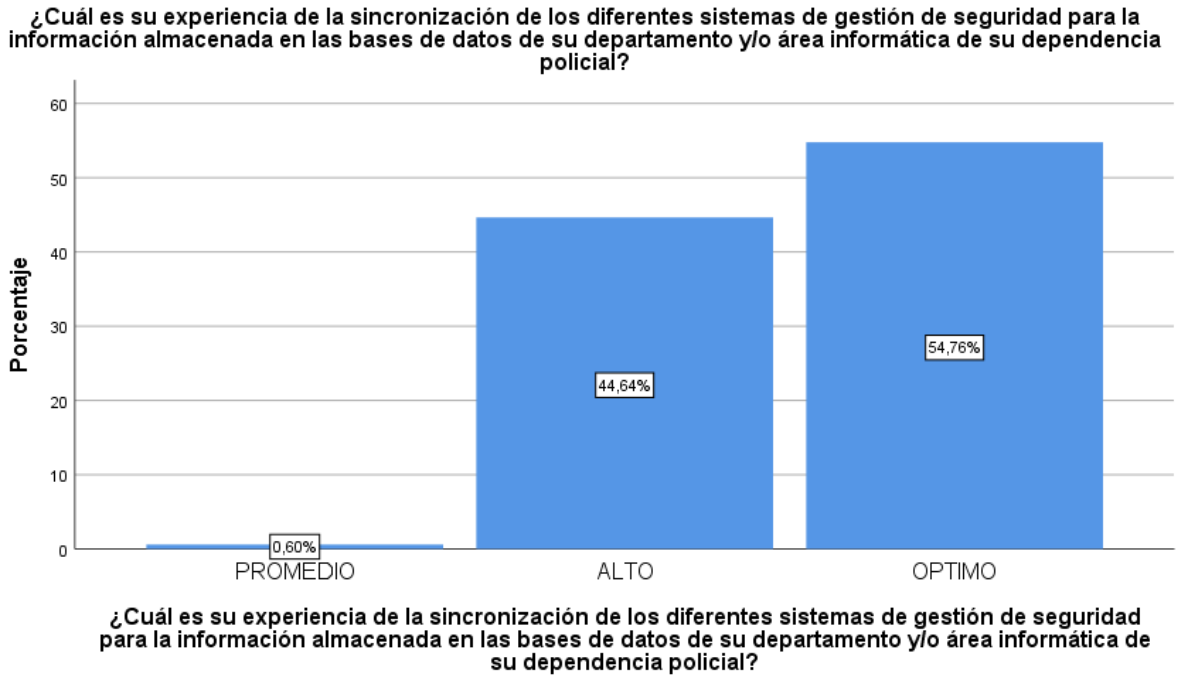
Items 3

¿Cuál es su experiencia de la sincronización de los diferentes sistemas de gestión de seguridad para la información almacenada en las bases de datos de su departamento y/o área informática de su dependencia policial?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	PROMEDIO	1	,6	,6	,6
	ALTO	75	44,6	44,6	45,2
	OPTIMO	92	54,8	54,8	100,0
	Total	168	100,0	100,0	

Figura 5

Items 3



Interpretación: De la tabla 13 y figura 3, el 54,8 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la experiencia de la sincronización de los sistemas de gestión de seguridad en la información

almacenada en la base de datos es óptima. Un 44.6% indica que es alto y un 6% un nivel promedio.

Tabla 14

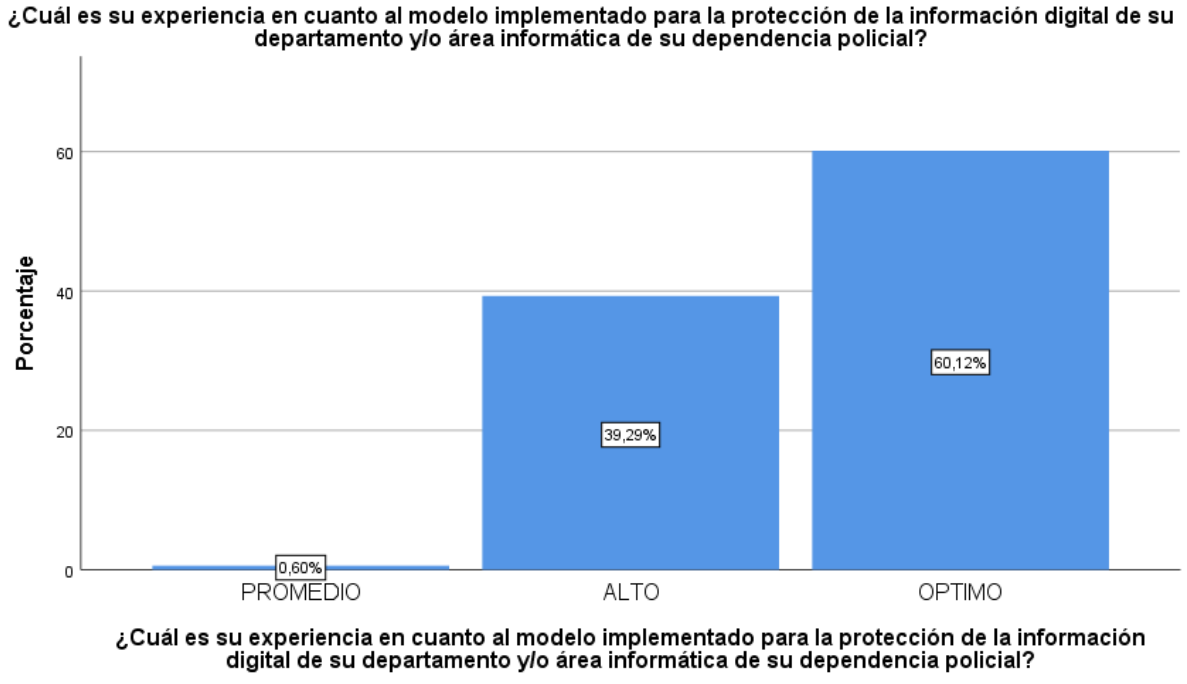
Items 4

¿Cuál es su experiencia en cuanto al modelo implementado para la protección de la información digital de su departamento y/o área informática de su dependencia policial?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	PROMEDIO	1	,6	,6	,6
	ALTO	66	39,3	39,3	39,9
	OPTIMO	101	60,1	60,1	100,0
	Total	168	100,0	100,0	

Figura 6

Items 4



Interpretación: De la tabla 14 y figura 4, el 60,1 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la experiencia del modelo implementa sobre la protección de la información digital en la

dependencia que laboran es óptima. Un 39,3% indica un nivel alto y un 6% un nivel promedio.

Tabla 15

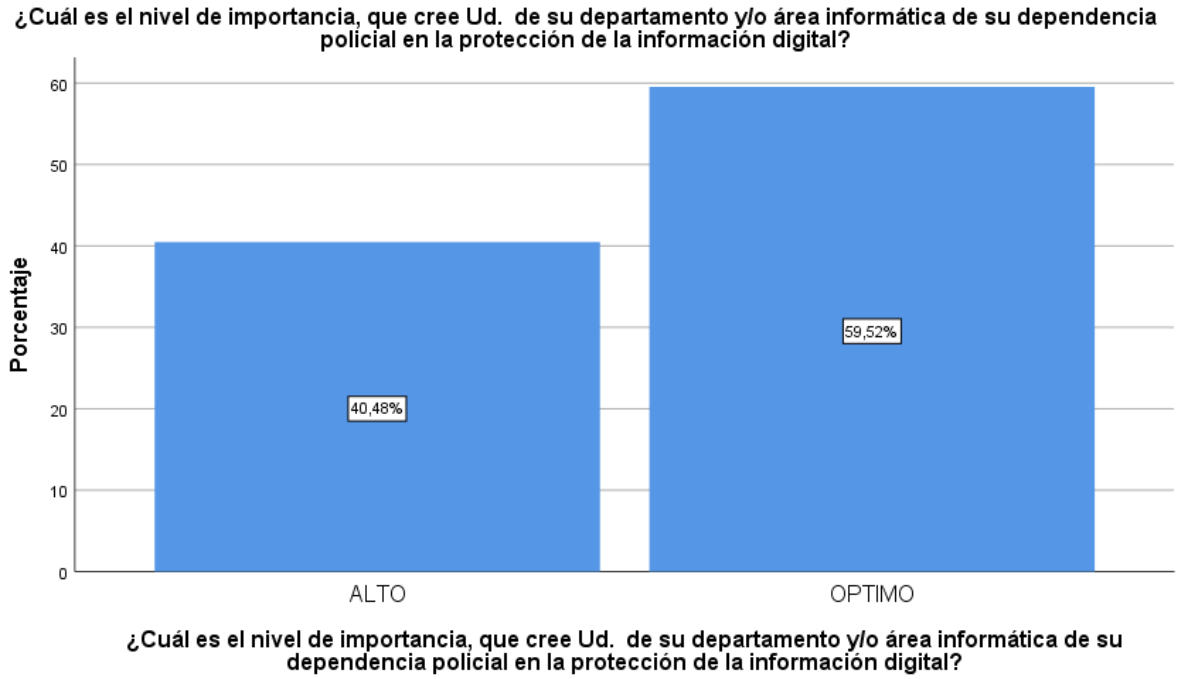
Items 5

¿Cuál es el nivel de importancia, que cree Ud. de su departamento y/o área informática de su dependencia policial en la protección de la información digital?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALTO	68	40,5	40,5	40,5
	OPTIMO	100	59,5	59,5	100,0
	Total	168	100,0	100,0	

Figura 7

Items 5



Interpretación: De la tabla 15 y figura 5, el 59,5 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que el nivel de importancia dentro de la protección de los datos digitales es óptimo. Un 40,5% indica un nivel alto.

Tabla 16

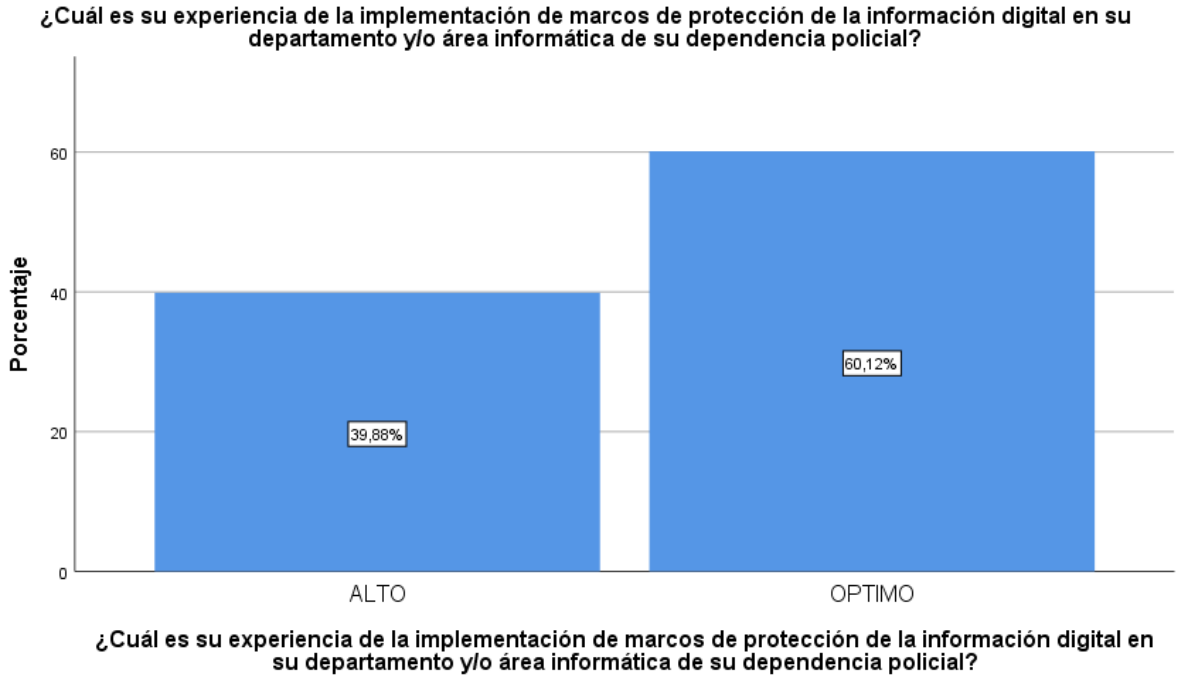
Items 6

¿Cuál es su experiencia de la implementación de marcos de protección de la información digital en su departamento y/o área informática de su dependencia policial?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALTO	67	39,9	39,9	39,9
	OPTIMO	101	60,1	60,1	100,0
	Total	168	100,0	100,0	

Figura 8

Items 6



Interpretación: De la tabla 16 y figura 6, el 60,1 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la implantación de marcos de protección de información digital dentro del área de informática es óptima, mientras que el 30,9 % indica que es alto.

Tabla 17

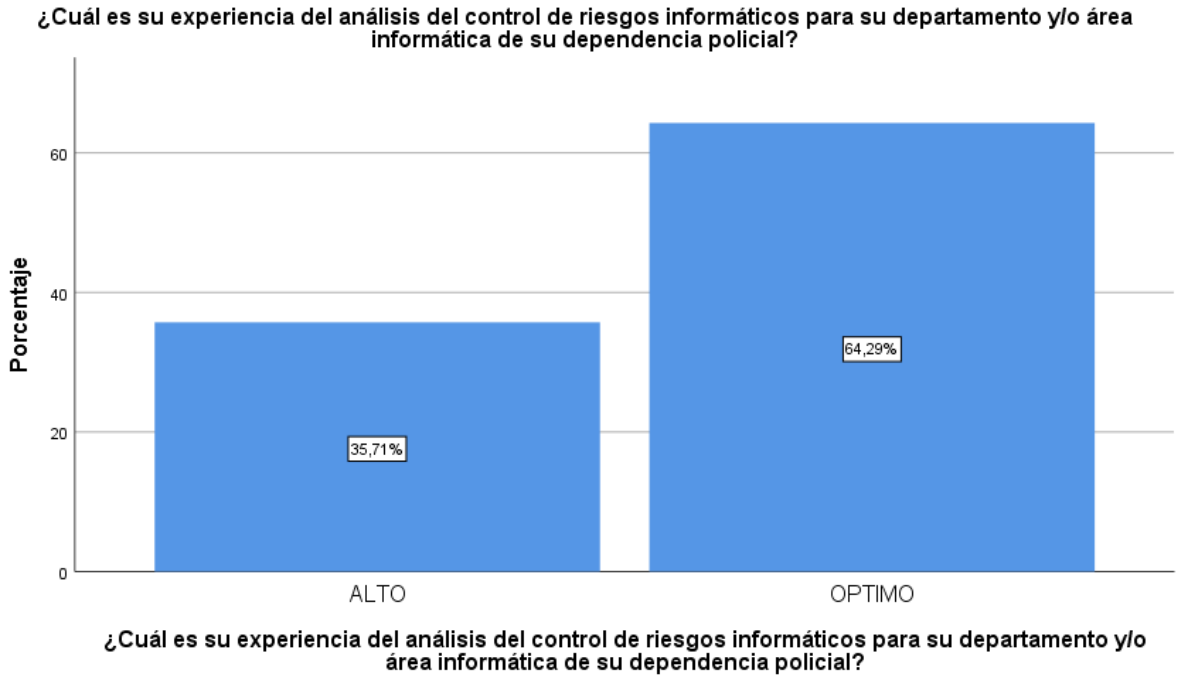
Items 7

¿Cuál es su experiencia del análisis del control de riesgos informáticos para su departamento y/o área informática de su dependencia policial?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALTO	60	35,7	35,7	35,7
	OPTIMO	108	64,3	64,3	100,0
	Total	168	100,0	100,0	

Figura 9

Items 7



Interpretación: De la tabla 17 y figura 7 el 64,3% de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la experiencia del análisis del control de riesgos informáticos dentro de su dependencia policial es óptima, mientras un 35,7% indica que es alto.

Tabla 18

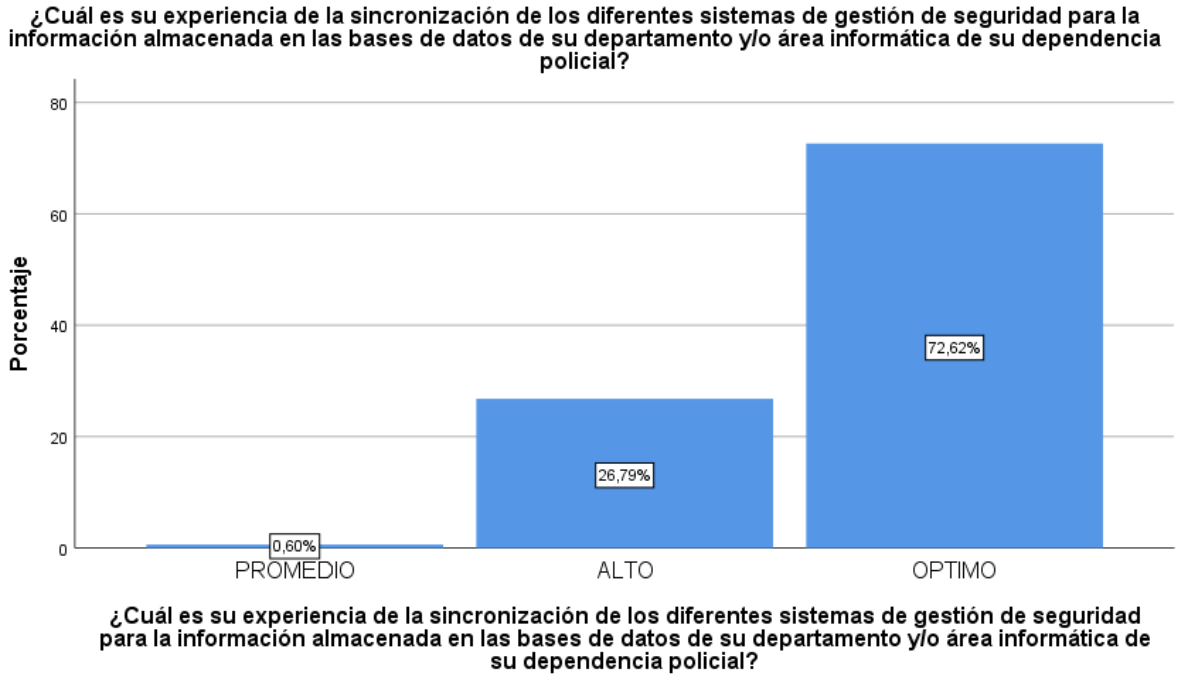
Items 8

¿Cuál es su experiencia de la sincronización de los diferentes sistemas de gestión de seguridad para la información almacenada en las bases de datos de su departamento y/o área informática de su dependencia policial?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	PROMEDIO	1	,6	,6	,6
	ALTO	45	26,8	26,8	27,4
	OPTIMO	122	72,6	72,6	100,0
	Total	168	100,0	100,0	

Figura 10

Items 8



Interpretación: De la tabla 18 y figura 8, el 72,3% de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la experiencia de la sincronización de los sistemas de gestión de seguridad en la información almacenada en la base de datos es óptima. Un 26,8% indica que es alto y un 6% un nivel promedio.

Tabla 19

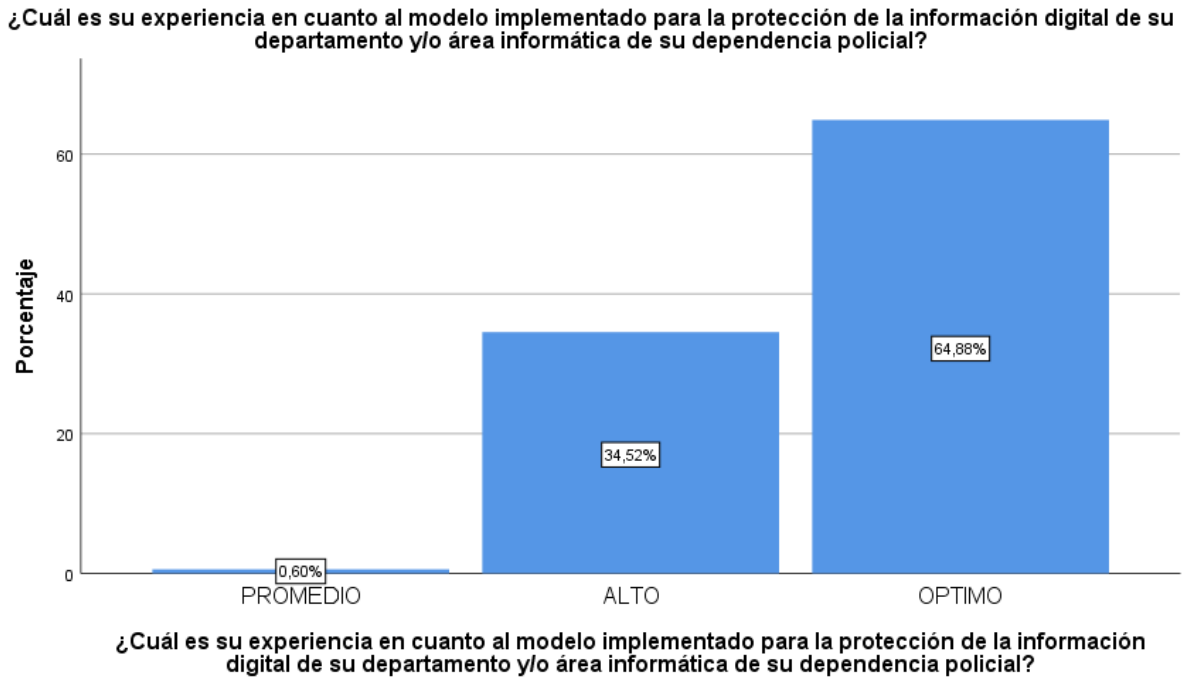
Items 9

¿Cuál es su experiencia en cuanto al modelo implementado para la protección de la información digital de su departamento y/o área informática de su dependencia policial?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	PROMEDIO	1	,6	,6	,6
	ALTO	58	34,5	34,5	35,1
	OPTIMO	109	64,9	64,9	100,0
	Total	168	100,0	100,0	

Figura 11

Items 10



Interpretación: De la tabla 19 y figura 8, el 60,1 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la experiencia del modelo implementa sobre la protección de la información digital en la dependencia que laboran es óptima. Un 39,3% indica un nivel alto y un 6% un nivel promedio.

Tabla 20

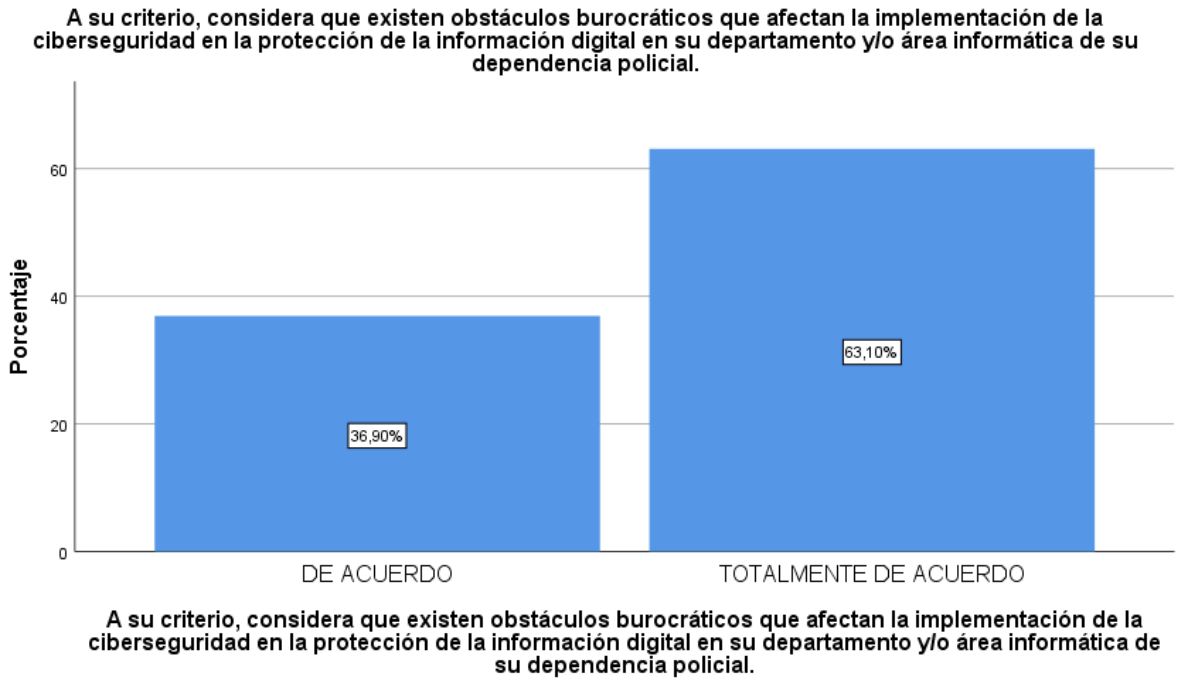
Items 10

A su criterio, considera que existen obstáculos burocráticos que afectan la implementación de la ciberseguridad en la protección de la información digital en su departamento y/o área informática de su dependencia policial.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DE ACUERDO	62	36,9	36,9	36,9
	TOTALMENTE DE ACUERDO	106	63,1	63,1	100,0
	Total	168	100,0	100,0	

Figura 12

Items 10



Interpretación: De la tabla 20 y figura 10, el 63,1 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP están totalmente de acuerdo en que se presentan obstáculos burocráticos que afectan la adecuada implementación en los elementos de protección en la información digital de su dependencia policial. Un 36,9% está de acuerdo.

Tabla 21

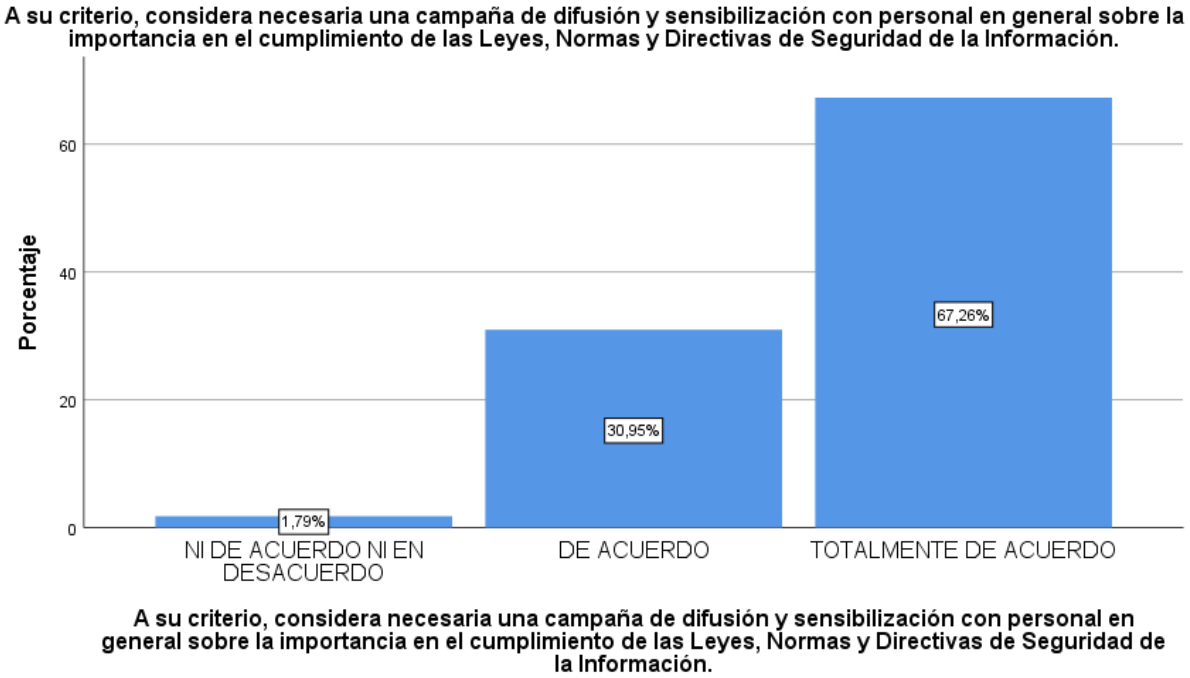
Items 11

A su criterio, considera necesaria una campaña de difusión y sensibilización con personal en general sobre la importancia en el cumplimiento de las Leyes, Normas y Directivas de Seguridad de la Información.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI DE ACUERDO NI EN DESACUERDO	3	1,8	1,8	1,8
	DE ACUERDO	52	31,0	31,0	32,7
	TOTALMENTE DE ACUERDO	113	67,3	67,3	100,0
	Total	168	100,0	100,0	

Figura 13

Items 11



Interpretación: De la tabla 21 y figura 11, el 67,3 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP están totalmente de acuerdo en que se necesita una campaña de difusión y sensibilización sobre la importancia del cumplimiento de las normas y directivas seguridad de la información. Un 31% está de acuerdo y un 1,8% no está ni acuerdo ni en desacuerdo.

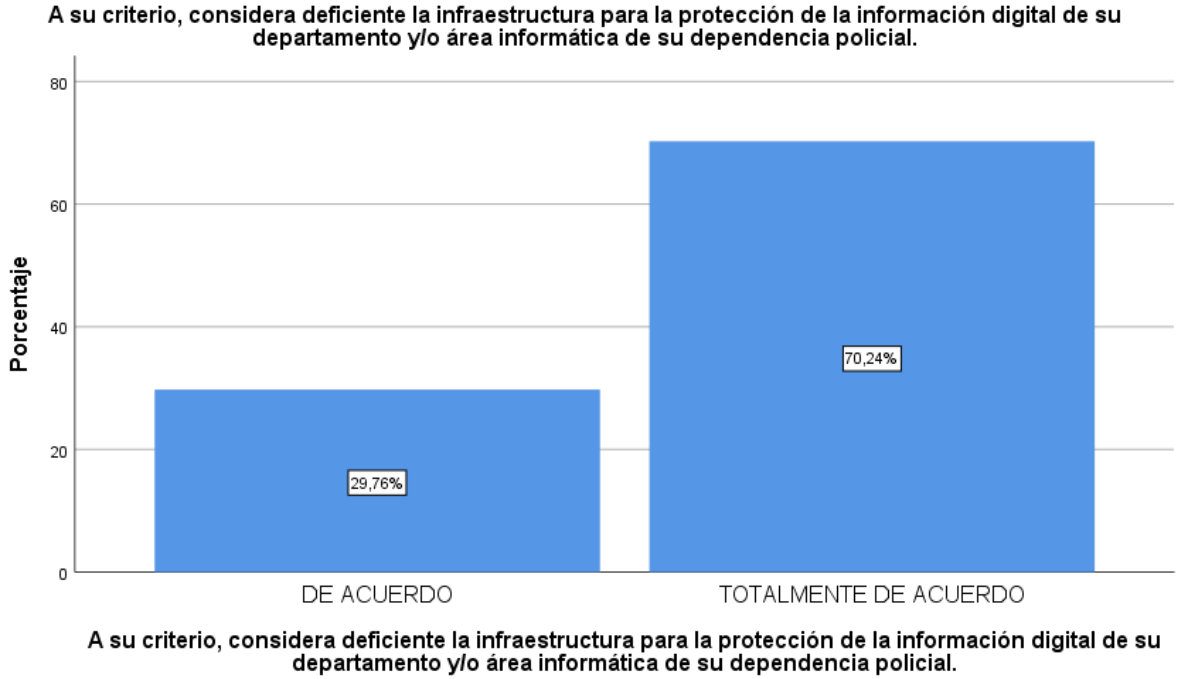
Tabla 22

Items 12

A su criterio, considera deficiente la infraestructura para la protección de la información digital de su departamento y/o área informática de su dependencia policial.					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DE ACUERDO	50	29,8	29,8	29,8
	TOTALMENTE DE ACUERDO	118	70,2	70,2	100,0
	Total	168	100,0	100,0	

Figura 14

Items 12



Interpretación: De la tabla 22 y figura 12, el 70,2 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP están totalmente de acuerdo en que consideran deficiente la infraestructura la protección de la información digital de la dependencia policial que pertenece. Un 29,8% están de acuerdo.

Tabla 23

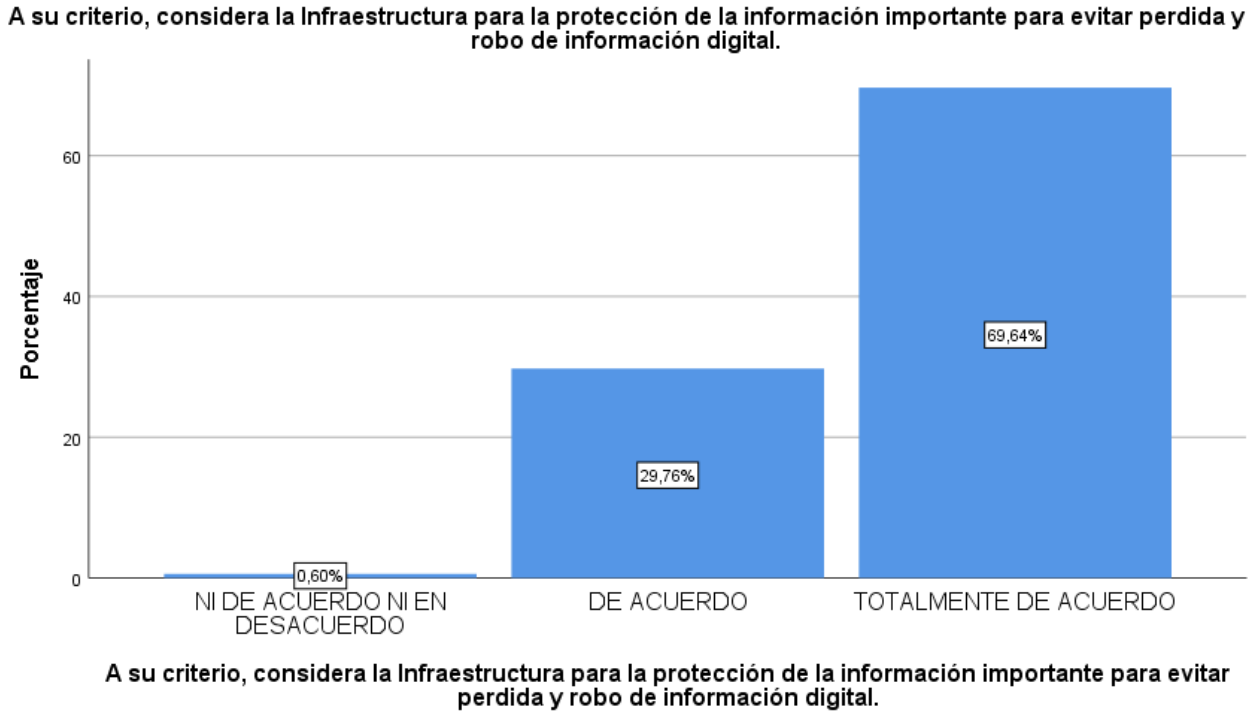
Items 13

A su criterio, considera la Infraestructura para la protección de la información importante para evitar perdida y robo de información digital.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI DE ACUERDO NI EN DESACUERDO	1	,6	,6	,6
	DE ACUERDO	50	29,8	29,8	30,4
	TOTALMENTE DE ACUERDO	117	69,6	69,6	100,0
	Total	168	100,0	100,0	

Figura 15

Items 13



Interpretación: De la tabla 23 y figura 13, el 69,3 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP están totalmente de acuerdo en que consideran importante la infraestructura para la protección de datos digitales y de esa manera evitar robos. Un 29,8% está de acuerdo y un 6% ni de acuerdo ni en desacuerdo.

Tabla 24

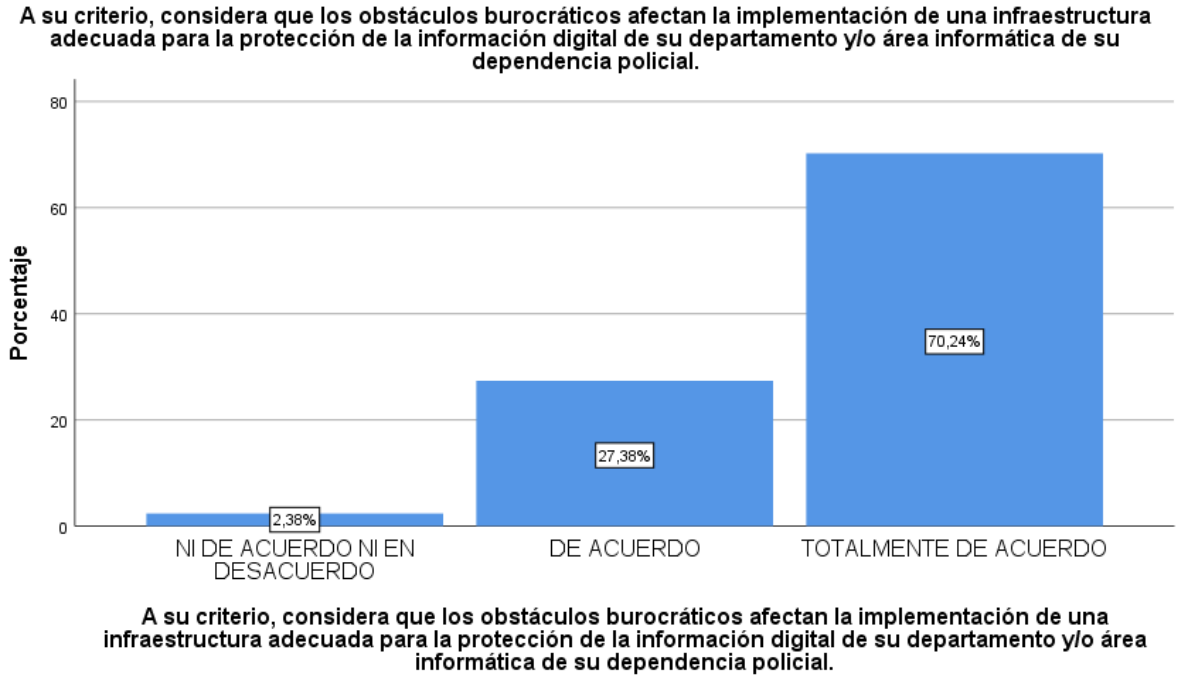
Items 14

A su criterio, considera que los obstáculos burocráticos afectan la implementación de una infraestructura adecuada para la protección de la información digital de su departamento y/o área informática de su dependencia policial.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI DE ACUERDO NI EN DESACUERDO	4	2,4	2,4	2,4
	DE ACUERDO	46	27,4	27,4	29,8
	TOTALMENTE DE ACUERDO	118	70,2	70,2	100,0
	Total	168	100,0	100,0	

Figura 16

Items 14



Interpretación: De la tabla 24 y figura 14, el 70,2 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP están totalmente de acuerdo en que consideran que los obstáculos burocráticos afectan la implementar de una infraestructura para proteger los datos e información digital de la dependencia policial que pertenecen. Un 27,4% está de acuerdo y un 2,4% ni de acuerdo ni en desacuerdo.

V. DISCUSIÓN DE RESULTADOS

El presente estudio tuvo como objetivo general determinar la relación que existe entre la utilidad de la ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023. De esa manera, según los resultados se determina que si existe influencia entre ambas variables, dado que la correlación de Spearman indica una correlativo de 0.753.

Dentro de este marco, la investigación de Pozo (2022) en su estudio halló que la ciberseguridad si guarda relación con las medidas de protección que adapta el estado ecuatoriano, puesto que, dentro de la era digitalizada es fundamental que las instituciones policiales se protejan de los ciberataques. Dado que son el principal riesgo que perjudican el desarrollo de los servicios y, sobre todo, las pérdidas considerables de recursos económicos y los daños a la reputación de la institución. Por lo expuesto anteriormente, se complementa con los resultados que se obtuvieron en el presente estudio dado se existe una relación entre ambas variables, puesto que la ciberseguridad es fundamental dentro de la era digital dado que funciona como el principal elemento para la protección de los datos y los sistemas contra posibles ataques digitales. Todo ello permitirá que se eviten fraudes y perdidas con la finalidad que se cumplan con las metas establecidas por la entidad.

Además, lo mencionado previamente, coincide con lo citado por Carlini (2016) en la que resalta que la ciberseguridad consiste en la práctica de proteger sistemas, redes y programas de ataques digitales. Por otro lado, según Open Web Application Security Project (OWASP) consiste en el procedimiento de corroborar que la información transmitida o almacenados son genuinos y provienen de una fuente autorizada para garantizar la seguridad de la institución.

Con respecto al primer objetivo específico, consistió en determinar la relación que existe entre las propiedades de la información y la protección de la información digital de la Policía Nacional del Perú, 2023. De esa manera, según los resultados que se hallaron en el

proceso de resultados el cual determinó que, si existe influencia entre ambas variables, dado que la correlación de Spearman indica una correlativo de 0.684. En ese sentido, según los resultados de la investigación de Correa (2022) existe incidencia significativa entre la variable ciberseguridad y la variable tratamiento de datos personales en una Municipalidad de Lima. Dado que, la variable ciberseguridad se registró un valor de estimación de 9.256 y un P valor de significancia de 0.000 en la prueba de Wald. De esa manera, se considera resultados homogéneos entre ambos estudios.

Por otro lado, sostiene que las propiedades de la información son importantes y fundamentales para que se protejan los datos disponibles, la integridad y, sobre todo, la confidencialidad de la información. El autor a través de los resultados obtenidos considera que la ciberseguridad a través de la protección de la información consiste en la capacidad de que se organice y se recopile datos, procesos y distintos soportes para que se resguarde el ciberespacio y todos los sistemas que se encuentran creados para salvaguardar la información de la institución, además que se encuentra canalizada para que haga frente a amenazas y la vulnerabilidad que presenta el internet ante las artimañas de terceros. Estos resultados son coincidentes con lo citado en la investigación de Cybersecurity Culture in Organizations, la European Union Agency for Cybersecurity (ENISA) en la que se hace hincapié a la importancia de las propiedades de la información a través de la confidencialidad aseguran que los datos que existen en los sistemas de la institución deben ser restringidos con solo acceso a personas autorizadas al manejo de información delicada. Puesto que; la integridad protege la información de alteraciones o modificaciones no autorizadas. Finalmente, la disponibilidad de la información busca que se garantice que los sistemas y datos estén disponibles y accesibles cuando se necesiten (ISO, 2018).

Con respecto al primer objetivo específico que consistió en determinar la relación entre las propiedades de la información y la protección de la información digital de la Policía Nacional del Perú, 2023. Según los resultados hallados se determina que, si existe influencia entre ambas variables, dado que la correlación de Spearman indica una correlativo de 0.684.

Con respecto al segundo objetivo específico que consistió en determinar la relación que existe entre la gestión de activos críticos y la protección de la información digital de la Policía Nacional del Perú, 2023. Según los resultados que se hallaron en el trabajo de campo, se determina que, si existe influencia entre ambas variables, dado que la correlación de Spearman indica una correlativo de 0.990. Al respecto, estos resultados son similares al de Cáceres (2021) que en su investigación indica una relación significativa entre los constructos señalados. Además, refiere que se debe hacer un análisis detallado sobre la gestión de activos que se presentan dentro de una entidad para conocer minuciosamente la multiplicidad de amenazas que se pueden presentar y, sobre todo, en las pedidas de propiedades de información digital. El autor resalta que una deficiente gestión de activos críticos en la entidad puede exponer rápidamente a que se vulnere los datos y se pueda generar perdidas y robos informáticos de propiedades intelectuales. Asimismo, los resultados de los estudios citados se respaldan con lo mencionado por el SANS Institute en el que señala que la ciberseguridad se caracteriza como un proceso en continua evolución. Este enfoque reconoce la naturaleza dinámica y en constante cambio de las amenazas cibernéticas y la necesidad de mantener una postura de seguridad adaptable y efectiva.

VI. CONCLUSIONES

Se concluye que sí existe una relación directa entre la utilidad de la ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023. Dado que el coeficiente de la correlación fue de 0,753 y es una correlación positiva considerable. Además, que, el 58,9% de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la implantación de marcos de protección de información digital dentro del área de informática es óptima, mientras que el 41% indica que es alto. En ese sentido, es preciso resaltar que la ciberseguridad es fundamental en el ecosistema digital que emplea la institución policial, ya que funciona como el factor determinante para la protección del sistema contra posibles ataques y amenazas digitales.

Según el primer objetivo específico planteado se concluye que sí existe una relación directa entre las propiedades de la información y la protección de la Información digital de la Policía Nacional del Perú, 2023. Ya que; el coeficiente de la correlación fue de 0,684 y es una correlación positiva considerable. Por otro lado, el 60,1 % de especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la experiencia del modelo implementa sobre la protección de la información digital en la dependencia que laboran es óptima. Un 39,3% indica un nivel alto y un 6% un nivel promedio. De tal manera que, las propiedades de la información en la ciberseguridad son aspectos importantes para que se protejan los datos, la integridad y confidencialidad de la información de la institución policial.

Según el segundo objetivo específico planteado se concluye que sí existe una relación directa entre la gestión de los activos críticos y la protección de la información digital de la Policía Nacional del Perú, 2023. Puesto que; el coeficiente de la correlación fue de 0,990 y es una correlación positiva perfecta. Así mismo, el 72,3% de especialistas que laboran en las

Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP sostienen que la experiencia de la sincronización de los sistemas de gestión de seguridad en la información almacenada en la base de datos es óptima. Un 26,8% indica que es alto y un 6% un nivel promedio. Además, que, una adecuada gestión de activos críticos busca proteger la información digital de la institución. Cabe resaltar que las actividades deben ser realizada por un profesional que sea el máximo responsable de gestionar los activos de para evitar complejidades en los datos almacenamos en los sistemas de información de la institución policial.

VII. RECOMENDACIONES

Se recomienda a los especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP que realicen proyectos integrales sobre tecnología de la información cuyo objetivo se basa en sensibilizar y capacitar a todos los trabajadores de diversas áreas de la institución en materia de ciberseguridad para que tengan el pleno conocimiento sobre la vital importancia que trae consigo el adecuado tratamiento de los datos digitales. Así mismo, implementar proyectos de tecnología blockchain para canalizar la conservación eficiente de las exactitudes de los datos vertidos en los sistemas de información de la institución, además que; tengan la capacidad de restablecer la integridad de la información.

Es fundamental mencionar que en el Perú, al existir la Ley de Protección de Datos Personales (Ley N° 29733), se recomienda al Ministerio del Interior implementar programas de prevención de delitos informáticos a todos los especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP con la finalidad de que tengan la capacidad inmediata de proveer distintos medios de protección de los datos digitales que trae consigo la institución para evitar fraudes y amenazas de inescrupulosos.

Se recomienda a los especialistas que laboran en las Oficinas de Tecnología, Informática y Comunicaciones (OFITIC) de la PNP que elaboren políticas de ciberseguridad con el objetivo que todos los colaboradores comprendan la importancia que tienen dichas políticas en la institución. Además de trabajar en conjunto con las autoridades pertinentes para realizar auditorías en materia de ciberseguridad para identificar las flaquezas que se presenta en la seguridad informática y los procedimientos que se deben ejecutar para disminuir los riesgos.

VIII. REFERENCIAS

Aguilar, D. E. (2014). *Estudio para el Desarrollo de un Modelo de Gestión de Riesgos y Seguridad de la Información para Instituciones Militares*. [Tesis de grado, Escuela Politécnica Nacional]. Bibdigital. https://bibdigital.epn.edu.ec/handle/15000/8642?mode=full

Alfaro, M. (2008). Apuntes sobre el gobierno corporativo en el Perú. *Foro Jurídico. Lima,* 08, 96-104. https://revistas.pucp.edu.pe/index.php/forojuridico/article/download/18498/18738

Álvarez, J. (2003). *Cómo hacer investigación cualitativa. Fundamentos y metodología.* Paidós. http://repositorio.utmachala.edu.ec/bitstream/48000/12501/1/Tecnicas-y-MetodoscualitativosParaInvestigacionCientifica.pdf

Amich, C., & Velásquez, A. (2014). La ciberdefensa y sus dimensiones globales y específicas en la estrategia de seguridad nacional española. ICADE. *Revista de la Facultad de Derecho*, (92), 59-76. https://doi.org/10.14422/icade.i92.y2014.002

Aquino, R., Chavez, J., Vidal, L., Ferreyro, L., Alvez, A., & Carozo, E. (2009). *Manual de Gestión de incidente de seguridad informática*. Lacnic. https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

Areitio, J. (2008). *Seguridad de la información*. Paraninfo. Biblioteca de la Universidad de Extremadura. Que se entiende por velocidad lectora. https://biblioguias.unex.es/c.php?g=572102&p=3944889

Areitio, J. (2008). *Seguridad de la información. Redes, informática, y sistemas de información.* Editorial Paraninfo. https://www.paraninfo.es/catalogo/9788497325028/seguridad-de-la-informacion--redes--informatica-y-sistemas-de-informacion

Arias, Y., Díaz, M., & Vargas, J. (2015). Elaboración de una guía de Gestión de Riesgos basados en la Norma NTC-31000 para el proceso de Gestión de Incidentes y Peticiones del área de Mesa de Ayuda de Empresas de Servicio de Tecnología en Colombia. [Trabajo de Grado, Universidad Católica de Colombia]. Repositorio Institucional de la Universidad Católica de Colombia, Bogotá. https://repository.ucatolica.edu.co/server/api/core/bitstreams/aa090ddc-1f24-4dee-

9562-aa22b4be8f3d/content

Boletín Semanal SBS (2019) Ciberseguridad: Una hoja de ruta para su desarrollo en los sistemas supervisados. https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/88

Borrero, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 4*(14). 1 - 17. https://dialnet.unirioja.es/servlet/articulo?codigo=7496888

Cáceres, F. (2021). Recomendaciones de ciberdefensa para la gestión segura del ciclo de vida de sistemas críticos. [Tesis de Maestría, Universidad de Buenos Aires]. Repositorio Institucional de la Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-2117_CaceresFF.pdf

Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *bie3: Boletín IEEE*, (2), 950-966. https://dialnet.unirioja.es/servlet/articulo?codigo=5998287

Correa, M. (2022). Ciberseguridad y su incidencia en el Tratamiento de Datos Personales en una Municipalidad Distrital de Lima Sur. [Tesis de Maestría, Universidad César Vallejo]. Repositorio Institucional de la Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/85975/Correa_CMM-SD.pdf

Crowdstrike (2021). Informe global de amenazas. Global Threat Report de CrowdStrike 2021. https://www.crowdstrike.com/resources/reports/global-threat-report-2021-latam/

Cuartas, J. (2007). Delito Informático en Colombia: Insuficiencias Regulativas, *El Derecho Penal y Criminología, 28,* 101-118. https://dialnet.unirioja.es/descarga/articulo/3311849.pdf

Davis, S. (2020). Conocimiento de los aspectos vinculados a la ciberseguridad que tiene el personal de las fuerzas navales de la Marina de Guerra del Perú. [Tesis para optar el grado de Maestro. Escuela de Posgrado, programa de Comando y Estado Mayor, Escuela Superior de Guerra Naval del Perú]. Repositorio ESUP. https://repositorio.esup.edu.pe/handle/20.500.12927/310

Demurtas, A. (2020). La Evolución normativa de la ciberseguridad en la Unión Europea y su impacto político a nivel de actores, objetivos y recursos. *Revista Análisis Jurídico-*

Político, *2*(3), 93-114. https://dialnet.unirioja.es/servlet/articulo?codigo=8696947

Decreto Supremo N° 106-2017-PCM. Se aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales -ACN

Escalante, O. (2018). Conflictos entre la gobernabilidad y la soberanía en las organizaciones multilaterales: estudio de la implementación de políticas de seguridad informática. [Tesis de Licenciatura, Repositorio Institucional de la Pontifica Universidad Católica del Perú. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/11994/ESCALANTE_TERAN_OSCAR_CONFLICTOS_GOBERNABILIDAD.pdf?sequence=1&isAllowed=y

Erb, M. (2014). *Gestión de Riesgo en la Seguridad Informática. facilitando el manejo seguro de la información en organizaciones sociales.* https://protejete.wordpress.com/

Gamboa, C. (2010). *Seguridad cibernética una necesidad mundial. San José: Impresión gráfica del Este S. A*. Universidad de Costa Rica. Programa Sociedad de la Información y el Conocimiento. https://www.kerwa.ucr.ac.cr/bitstream/handle/10669/500/libro%20completo%20Ciber.pdf?sequence=1

García, A., & Iglesias, E. (2017). *Economía digital en América Latina y el Caribe: Situación actual y recomendaciones.* Banco Interamericano de Desarrollo. http://dx.doi.org/10.18235/0012713

Gil, E. (2015). *Big data, privacidad y protección de datos. Madrid: Agencia Española de Protección de Datos*. XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos. Madrid. España. https://www.aepd.es/sites/default/files/2019-10/big-data.pdf

Gómez, A. (2011). Enciclopedia de la Seguridad informática. (2da Ed.). Alfaomega. http://biblio.fcedu.uner.edu.ar/derecha/novedades/pdf/19086.pdf

Haro, M. (2019). La Guerra de Cuarta Generación y sus efectos en la frontera norte ecuatoriana. Respuesta del Estado. *Res Non Verba Revista Científica*, 9(1), 121-141.

Galindo, C. (2005). De la Seguridad Nacional a la Seguridad Democrática: Nuevos problemas,

viejos esquemas. *Estudios Socio-Jurídicos*, *7*(SPE), 496-543. http://www.scielo.org.co/scielo.php?pid=S0124-05792005000300013&script=sci_arttext

Hernández, J. (2018). Estrategias Nacionales de Ciberseguridad en América Latina. Análisis GESI, Análisis 8. https://acortar.link/OGEiNO

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la Investigación. (Vol. 6, pp. 102-256). McGraw-Hill. https://www.semanticscholar.org/reader/3e42246ee04eeab4fcef7b4bd80c13c59bc21292

Hess, C. (2010). Ciberseguridad en Costa Rica. San José. Universidad de Costa Rica. Programa Sociedad de la Información y el Conocimiento. http://www.prosic.ucr.ac.cr/sites/default/files/documentos/ciberseguridad_2010.pdf

Hidalgo, J. (2014). Ingeniería del software y Ciberseguridad. IEEE. https://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO88-2014_Ingenieria_Software_Ciberseguridad_HidalgoTarrero.pdf

IBM Security. (2021). *IBM lanza servicios nuevos y mejorados para ayudar a simplificar la seguridad de la nube híbrida*. Ponemon Institute y patrocinada, analizada e informada por IBM Security.

Inoguchi, A., y Macha, E. (2017). Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016. [Tesis de Grado, Universidad San Ignacio de Loyola]. Repositorio de la Universidad San Ignacio de Loyola. https://repositorio.usil.edu.pe/entities/publication/9449a061-bfd2-4ecc-8cf1-770fba7cee45

ISO/IEC 27000:2018. (2018). Tecnología de la información - Técnicas de seguridad - Sistemas de Gestión de la Seguridad de la Información - Generalidades y vocabulario. Suiza, Suiza.

Izcara, S. (2014). *Manual de Investigación Cualitativa*. Editorial Fontamara. https://repositorio.minedu.gob.pe/handle/20.500.12799/4613

Kaspersky, E.(2021). Boletín de seguridad de Kaspersky, estadísticas de 2021. Preparados

para el futuro. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_sp.pdf

López, J. (2019). *ConsumoTIC*. https://consumotic.mx/tecnologia/e-mail-principal-vector-de-ciberataques-symantec/

Medina, J. (2006). Estándares para la seguridad en sistemas de información con Tecnologías de Información. [Tesis de Licenciatura, Universidad de Chile]. Repositorio Académico de la Universidad de Chile. http://repositorio.uchile.cl/bitstream/handle/2250/108414/medina_j.pdf?sequence=4&isAllowe=y

Merino, F., y Aliaga, A. (2017). Delitos informáticos y las salidas alternativas posibles revisadas desde el análisis económico del derecho. [Tesis de Licenciatura, Universidad de Chile]. Repositorio Académico de la Universidad de Chile. https://acortar.link/qmixif

NTP-ISO/IEC 27001. (2008). Año de la unidad paz y desarrollo. https://www.congreso.gob.pe/carpetatematica/2018/carpeta_122/normas_nacionales/

NTP-ISO/IECC 17799. (2015). Sistema de la Seguridad de Información. https://www.pmg-ssi.com/2015/03/ntp-isoiec-17799-norma-tecnica-peruana/

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

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

Pozo, L. (2022). Ciberseguridad y medidas de protección de la información adoptadas por el Estado ecuatoriano. [Trabajo de Investigación de Maestría, Instituto de Altos Estudios Nacionales Universidad de Posgrado del Estado]. Repositorio Digital IAEN. https://repositorio.iaen.edu.ec/handle/24000/6103

Sabino, C. (1992). El proceso de investigación. Ed. Panapo.

https://paginas.ufm.edu/sabino/ingles/book/proceso_investigacion.pdf

Seminario, F. (2020) Coronavirus y ciberseguridad bancaria: Auge de ciberataques ponen a prueba la seguridad. Recuperado de: https://iupana.com/2020/04/27/covid-19-ciberseguridad-bancaria-auge-ciberataques-ponen-prueba-seguridad/

SonicWall. (2021). *Informe de ciberamenazas de SonicWall*. el cambiante panorama del cibercrimen. https://www.sonicwall.com/medialibrary/es/infographic/2023-cyber-threat-report-infographic.pdf

Vargas, X. (2011). ¿Cómo hacer una investigación cualitativa? Redinfor. Servicios para el desarrollo. Editorial EXTETA. https://redinfor.com.pe/portal/2019/08/08/como-hacer-investigacion-cualitativa-vargas-2007/

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

Verinson (2023). Data Breach Investigations Report. Disponible en https://www.verizon.com/business/resources/reports/dbir/

Villarrubia, G. (2021). Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la política de seguridad y defensa nacional en la región Lima, 2018. [Tesis de grado, Centro de Altos Estudios Nacionales]. Repositorio institucional del CAEN. https://repositorio.caen.edu.pe/handle/20.500.13097/254

Zúñiga, J. (2017). Ciberseguridad y su incidencia en la protección de la información del Ejército del Perú. caso: COPERE 2013 – 2014. [Tesis de Maestría, Instituto Científico y Tecnológico del Ejército]. Repositorio ICTE - Institucional. http://repositorio.icte.ejercito.mil.pe/handle/ICTE/32

IX. ANEXOS

Anexo A: Matriz de Consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES / MÉTRICA	METODOLOGÍA
PROBLEMA GENERAL: ¿Qué relación existe entre la utilidad de la Ciberseguridad en la protección de la Información digital de la Policía Nacional del Perú, 2023?	OBJETIVO GENERAL: Determinar la relación entre la utilidad de la Ciberseguridad en la Protección de la Información digital de la Policía Nacional del Perú, 2023.	HIPÓTESIS GENERAL: Existe una relación directa entre la utilidad de la Ciberseguridad en la Protección de la Información digital de la Policía Nacional del Perú, 2023.	**VARIABLE INDEPENDIENTE:** **LA CIBERSEGURIDAD**	**Tipo de investigación:** Básica con enfoque cuantitativo **Nivel de la investigación:** Correlacional **Diseño de investigación:** No Experimental **Según el periodo de tiempo**: Transversal **Población:** Especialistas en informática de la PNP **Muestra:** 168 personas que labora en los centros informáticos de la PNP. **Técnicas de recolección:** Encuestas **Instrumento**: cuestionario **Herramientas Estadísticas:** Pruebas Estadística: Rho de Spearman
PROBLEMAS ESPECIFICOS: a) ¿Qué relación existe entre las propiedades de la Ciberseguridad y la protección de la Información digital de la Policía Nacional del Perú, 2023? b) ¿Qué relación existe entre la gestión de activos críticos de la ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023?	**OBJETIVOS ESPECIFICOS:** a) Determinar la relación de las propiedades de la Ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023. b) Determinar la relación de la Gestión de Activos Críticos de la ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023.	**HIPÓTESIS ESPECIFICOS:** a) Existe una relación directa entre las propiedades de la Ciberseguridad y la protección de la Información digital de la Policía Nacional del Perú, 2023. b) Existe una relación directa entre la Gestión de Activos Críticos de la ciberseguridad y la protección de la información digital de la Policía Nacional del Perú, 2023.	**VARIABLE DEPENDIENTE:** **PROTECCIÓN DE LA INFORMACIÓN DIGITAL DE LA POLICÍA NACIONAL DEL PERÚ** **MEDICIÓN:** • Porcentaje (%) • Escala de Likert. **META:** a) Mejora de infraestructuras de seguridad informática. b) Reducir incidencias informáticas	

Fuente: Elaboración propia

Anexo B: Validación y confiabilidad del Instrumento.

La validez se justifica con la apropiada idoneidad del cuestionario y sus respectivas preguntas de acerca de la investigación, el método utilizado para este fin es el juicio de experto. En ese sentido Hernández *et al.* (2018) indica que la validez garantiza que el instrumento usado posee la capacidad suficiente para medir aquella característica relevante en la investigación.

Según Ñaupas et al (2018) la confiabilidad se arraiga fuertemente en la invariación relevante de resultados provenientes del instrumento bajo condiciones semejantes de aplicación. Para el presente estudio se utiliza el software IBM SPSS Statistics para el cálculo ponderado del coeficiente Alfa de Cronbach, que según Ñaupas et al. (2018) y Hernández y Mendoza (2018), es un cociente oscilante entre 0 y 1, el cual, justificará la correlación entre el resultado estadístico y la recopilación de datos si es más próximo a la unidad, usados en iteraciones de categóricas.

Anexo C: Cuestionario de percepción de la utilidad de la ciberseguridad en la protección de la información digital de la Policía Nacional del Perú, 2023.

CUESTIONARIO

UNIDAD EJECUTORA:	
MACRO REGIÓN Y/O REGIÓN POLICIAL:	
NOMBRES Y APELLIDOS:	**CARGO:**

Instrucciones: A continuación, se presentan algunas preguntas para marcar y otras para que responda con sus propias palabras.

En el 1er grupo de preguntas, lea cada pregunta y marque con una equis (X) la opción que mejor le parezca.

1: En formación 2: Bajo 3: Promedio 4: Alto 5: Óptimo

En el 2do grupo de preguntas, lea cada pregunta y marque con una equis (X) la opción que mejor le parezca

1: En formación 2: Bajo 3: Promedio 4: Alto 5: Óptimo

En el 3er grupo de preguntas, lea cada pregunta y marque con una equis (X) la opción que mejor le parezca

1: Totalmente en desacuerdo 2: En desacuerdo 3: Ni de acuerdo ni en desacuerdo 4: De acuerdo 5: Totalmente de acuerdo

No hay preguntas correctas ni incorrectas.

1ER GRUPO DE PREGUNTAS

PERCEPCION DEL PERSONAL ESPECIALIZADO ACERCA DE LA CIBERSEGURIDAD	1	¿Cuál es su experiencia de la implementación de marcos de protección de la información digital en su departamento y/o área informática de su dependencia policial?	1	2	3	4	5
	2	¿Cuál es su experiencia del análisis del control de riesgos informáticos para su departamento y/o área informática de su dependencia policial?	1	2	3	4	5
	3	¿Cuál es su experiencia de la sincronización de los diferentes sistemas de gestión de seguridad para la información almacenada en las bases de datos de su departamento y/o área informática de su dependencia policial?	1	2	3	4	5
	4	¿Cuál es su experiencia en cuanto al modelo implementado para la protección de la información digital de su departamento y/o área informática de su dependencia policial?	1	2	3	4	5
	5	¿Cuál es el nivel de importancia, que cree Ud. de su departamento y/o área informática de su dependencia policial en la protección de la información digital?	1	2	3	4	5

2DO GRUPO DE PREGUNTAS

NIVEL DE CONOCIMIENTO DEL ESPECIALISTA	6	¿Cuál es su experiencia de la implementación de marcos de protección de la información digital en su departamento y/o área informática de su dependencia policial?	1	2	3	4	5
	7	¿Cuál es su experiencia del análisis del control de riesgos informáticos para su departamento y/o área informática de su dependencia policial?	1	2	3	4	5
	8	¿Cuál es su experiencia de la sincronización de los diferentes sistemas de gestión de seguridad para la información almacenada en las bases de datos de su departamento y/o área informática de su dependencia policial?	1	2	3	4	5
	9	¿Cuál es su experiencia en cuanto al modelo implementado para la protección de la información digital de su departamento y/o área informática de su dependencia policial?	1	2	3	4	5

3ER GRUPO DE PREGUNTAS

CONSIDERACIONES RESPECTO A INFRAESTRUCTURA, NORMAS Y PROCESOS EN GENERAL	10	A su criterio, considera que existen obstáculos burocráticos que afectan la implementación de la ciberseguridad en la protección de la información digital en su departamento y/o área informática de su dependencia policial.	1	2	3	4	5
	11	A su criterio, considera necesaria una campaña de difusión y sensibilización con personal en general sobre la importancia en el cumplimiento de las Leyes, Normas y Directivas de Seguridad de la Información.	1	2	3	4	5
	12	A su criterio, considera deficiente la infraestructura para la protección de la información digital de su departamento y/o área informática de su dependencia policial.	1	2	3	4	5
	13	A su criterio, considera la Infraestructura para la protección de la información importante para evitar perdida y robo de información digital.	1	2	3	4	5
	14	A su criterio, considera que los obstáculos burocráticos afectan la implementación de una infraestructura adecuada para la protección de la información digital de su departamento y/o área informática de su dependencia policial.	1	2	3	4	5

DATOS DEL EXPERTO:

Nombres	Guido Sergio
Apellidos	ESCALANTE CHEN
Institución(es) en la(s) que trabaja	**ESCUELA DE POSGRADO DE LA PNP**
Cargo actual	DOCENTE
Grado académico	MAESTRO EN INGENIERIA DE SISTEMAS

Fecha: DD de MES del 2023

Firma
D.N.I.: 43433794

DATOS DEL EXPERTO:

Nombres	**Sly Stalim**
Apellidos	**Sánchez Saavedra**
Institución(es) en la(s) que trabaja	**MININTER**
Cargo actual	**Administrador de Redes**
Grado académico	**Magister en Ingeniería de Sistemas**

Firma
D.N.I.: 44621336

DATOS DEL EXPERTO:

Nombres	**Carlos Eduardo**
Apellidos	**Aguilar Araujo**
Institución(es) en la(s) que trabaja	**BASE4 Security**
Cargo actual	**CSIRT Leader**
Grado académico	**Magister en Dirección de TI**

Firma

D.N.I.: 45102357

DATOS DEL EXPERTO:

Nombres	**Ing . Alexander Michael**
Apellidos	**LLANOS SANCHEZ**
Institución(es) en la(s) que trabaja	**Policía Nacional del Perú**
Cargo actual	**Participante en el XXI PROMACIPOL, con mención en Inteligencia**
Grado académico	**Magister**

Firma
D.N.I.: 44091528

MUCHAS GRACIAS POR SU COLABORACIÓN