UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Implementación ISO 27001 para el Control de Delitos Informáticos en la División de Prensa DIRCII PNP, Lima, 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Escobar Gutierrez, Jesus Alexander (ORCID: 0000-0002-5585-288X)

ASESOR:

Dr. Acuña Benites, Marlon Frank (ORCID: 0000-0001-5207-9353)

LÍNEA DE INVESTIGACIÓN

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA-PERÚ

2022

Dedicatoria

A Dios Padre Todo Poderoso, a mis padres y a mi familia por motivarme y ser la fuerza para cumplir exitosamente con este gran paso en mi carrera profesional.

Agradecimiento

A Dios Padre todo poderoso por guiarme y acompañarme en cada momento de esta maestría y en mi carrera como suboficial de la Policía Nacional del Perú; y, a todos los distinguidos docentes de la Maestría UCV que compartieron conmigo sus conocimientos y experiencias permitiéndome lograr con la presente tesis.

Índice de contenidos

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

La covid-19 cambió radicalmente el uso de las TIC debido a la necesidad de retomar labores u otras actividades; incrementó los peligros del ciberespacio aprovechados por cibercriminales. La tesis tiene el propósito determinar cómo incide la implementación de la ISO 27001 para el control de delitos informáticos en la División de Prensa DIRCII PNP, Lima, 2022. El enfoque es cuantitativo, tipo básica, diseño no experimental de tipo transversal y nivel correlacional causal.

Teniendo de muestra 50 personal PNP encuestados sobre las variables de estudio. Los resultados indicaron que la implementación ISO 27001 incide significativamente en el control de delitos informáticos, obteniendo que el coeficiente Alfa de Cronbach se aplicó a los 30 Ítems politómicas tipo Likert del instrumento usado, calculado mediante SPSS v25 es 0.930, demostrando con esto una confiabilidad Excelente. No se realizó prueba de normalidad porque se trabajó con niveles y no con números. Se obtuvo p_valor < 0,05 en todos los casos y el estadístico Tau-b de Kendall y Regresión ordinal, no paramétricas asume que el valor es ,904. Demostrando, que incide 81.2% positivamente en el control de delitos informáticos.

Concluyendo que el instrumento utilizado es aceptable y procedería su aplicación mejorando la seguridad de la información.

***Palabras clave**: Implementación ISO 27001, Control de Delitos Informáticos, Covid-19, Sistema de Gestión de la Seguridad de la Información.*

Abstract

The covid-19 radically changed the use of ICT due to the need to resume work or other activities; it increased the dangers of cyberspace exploited by cybercriminals. The purpose of the thesis is to determine the impact of the implementation of ISO 27001 for the control of cybercrime in the Press Division DIRCII PNP, Lima, 2022. The approach is quantitative, basic type, non-experimental design of transversal type and causal correlational level.

A sample of 50 PNP personnel were surveyed on the study variables. The results indicated that the implementation of ISO 27001 has a significant impact on the control of computer crimes, obtaining that the Cronbach's Alpha coefficient applied to the 30 Likert-types polytomous items of the instrument used, calculated using SPSS v25 is 0.930, thus demonstrating excellent reliability. No normality test was performed because we worked with levels and not with numbers. The p_value < 0.05 was obtained in all cases and the Kendall's Tau-b statistic and ordinal regression, non-parametric assumes that the value is .904. Demonstrating that it has a positive impact of 81.2% on the control of computer crimes.

Concluding that the instrument used is acceptable and its application would be appropriate to improve information security.

Keywords: ISO 27001 implementation, Computer Crime Control, Covid-19, Information Assets and ISMS.

I. INTRODUCCIÓN

Desde la aparición de la Covid-19 a nivel mundial, según el experto internacional de seguridad Arteaga (2020) se ha incrementado los peligros existentes y que rondaban el ciberespacio, viéndose afectado las cibernautas, empresas del sector público y privado. Debido a la gran necesidad de continuar con las actividades, se implementó a grueso modo el trabajo remoto; significando esto el inicio de soluciones para unos, pero para otros el comienzo de muchos problemas en su seguridad de la información, estando expuesto más que nunca a infinidad de vulnerabilidad y agravando las cosas, el desconocimiento los trabajadores del negocio de las disposiciones sobre seguridad de la información. La cibercriminalidad sumada a la desinformación, ha creado un espacio muy bien aprovechado por ciberdelincuentes y es aquí que se debe implantar soluciones que ayuden a disminuir y/o mitigar la exposición a ataques informáticos.

En un informe de la INTERPOL (2020) en una evaluación de la Organización International de Policía Criminal, muestran un alarmante incremento de los ciberataques durante la Covid-19 a nivel mundial, después de una evaluación sobre las repercusiones del confinamiento en lo que respecta a los ciberdelincuentes, sus objetivos de ataques han variado radicalmente a los de antes que “eran particulares y pequeñas empresas” por un aprovechamiento de la circunstancias, siendo ahora “grandes multinacionales, administraciones estatales e infraestructuras esenciales”. Debido al acelerador crecimiento de las empresas yorganizaciones en sistemas y redes para que su personal trabaje desde sus hogares, incrementó las vulnerabilidades en materia de seguridad informática que permitió a ciberdelincuentes apropiarse de datos e información; y así, obtener beneficios y ocasionar disfunciones.

Lo observado en el periodo de enero y abril, por un socio de INTERPOL del sector privado, logró detectar que producto de la incertidumbre relacionada a la COVID-19, las actividades de facinerosos se vieron reflejadas en 737 incidentes de tipo malware, 48 000 URL fraudulentos y 907 000 correos basura. Según Stock (2020) “Los ciberdelincuentes están creando nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica generada”.

Piera (2021) en lo que va su trayectoria profesional asegura que la mayor parte

de empresas, sean pequeñas o medianas no cuentan con un plan de seguridad formal. Plantea implementar un SGSI para una empresa y sus diversas áreas dependientes de esta que será administrada desde un servicio de TI unificado. Posteriormente, mediante un análisis y planificación desarrollar un plan director de seguridad empresarial; en el cual se evalúa sus niveles de seguridad informática a fin de identificar sus puntos débiles o fuertes, y ofrecer planes y propuestas que refuercen las medidas de seguridad. Para esto, empleó el conjunto de normas ISO 27k y otras normas del gobierno electrónico de España.

Aliaga (2021) la prevención de ataques informáticos en una empresa privada disminuiría de implementarse un sistema de ciberseguridad, que influiría positivamente en la identificación de las vulnerabilidades; conllevando al mejor desempeño de dicho negocio. Asegurando ser este modelo la solución idónea para la empresa.

Arias (2020) dar a conocer de forma adecuada los riesgos, vulnerabilidades, reducirlos y mitigarlos mediante el SGSI con la cual administran y controlar las ocurrencias, permitirá mantener a la empresa constantemente la mejora continua y alcanzar así el estado de madurez necesario. La innovación en los procesos que sean necesarios, fortalecerá el cuidado de los activos de información, en las instituciones.

En Perú, se viene escuchando con mayor frecuencia la aparición de ciberataques y según una nota periodística de la Agencia Peruana de Noticas Andina, ANDINA (2020) “Perú sufrió más de 28 000 000 de ataques de acceso remoto en 2020”, tras la COVID-19 y las medidas sanitarias del gobierno, debido que las empresas y organizaciones al no detener sus operaciones y cumplir con el distanciamiento social, implementaron el trabajo remoto.

Respecto al contexto local, el caso publicado en el diario El Comercio, que según Neyra (2020) “Hackers vulneraron plataforma del Bono Familiar Universal-BFU para apropiarse de dinero”, del 30 de mayo del 2020. La empresa de ciberseguridad Deep Security identificó las vulnerabilidades en el portal web donde se encontraban a los beneficiarios del BFU, reuniéndose con representantes de la PCM y la Reniec, les dieron a conocer que sus medidas de seguridad fueron las adecuadas y permitió la sustracción de miles de soles. A través de un reporte demostraron como habrían actuado los cibercriminales, suplantaron la identidad de

miles de beneficiarios quienes tras registrarse y recibir la clave de seguridad en chips que estos habrían adquirido, retiraron el dinero debido que no se presentaba el DNI físico.

La importancia para la profesión radica en la incidencia de la implementación de la ISO 27001 para el control de delitos informáticos, resulta positiva, ya que influye en mitigar las diversas posibilidades de tipos de pérdidas que no solo significarían dinero y tiempo sino también, el restablecerse de los daños causados a sus sistemas en general y activos de información. Asimismo, tiene como relevancia en el contexto social atender la necesidad de personas, empresas o entidades públicas en continuar sus operaciones de manera remotas, tras las medidas sanitarias dispuestas por los gobiernos a nivel mundial en las que se pidió distanciamiento social a fin de evitar y disminuir los contagios de la pandemia, del COVID-19.

Después que la realidad problemática fue descrita, se formula el problema general: ¿Cómo incide la implementación de la ISO/IEC 27001:2013 en el control de delitos informáticos en la División de Prensa DIRCII PNP, Lima, 2022? Asimismo, la formulación de tres problemas específicos que son: ¿Cómo incide la implementación de la ISO/IEC 27001:2013 en los daños de datos de la División de Prensa DIRCII PNP, Lima, 2022? ¿Cómo incide la implementación ISO/IEC 27001:2013 en los daños de sistemas y redes de la División de Prensa DIRCII PNP, Lima, 2022? ¿Cómo incide la implementación de la ISO/IEC 27001:2013 en las interceptaciones no autorizadas de la División de Prensa DIRCII PNP, Lima, 2022?

La justificación teórica está en la importancia de la propuesta de una implementación de la ISO/IEC 27001:2013 para la mejorar del control de delitos informáticos en base a los Políticas de Seguridad, Análisis de Riesgos y Desarrollo de Auditorias. Además, la aplicación de medidas es baja, los resultados de la investigación generar conocimiento en el área en base a instalar protección a la seguridad de la información la cual debe permitirse para el control de delitos informáticos.

La justificación práctica se enfoca se aborda sobre la División de Prensa de la DIRCII PNP, desde 26 abril del 2021 hasta 25 junio 2022, debido que se encuentra expuesto a sufrir ataques informáticos a sus activos de información y sistemas en general.

La justificación metodológica, la implementación de la ISO en esta área, permite

mejorar el control de los delitos informáticos, mediante la aplicación de las mejores prácticas que tiene la ISO 27001, que demuestra su valides y confiabilidad empleando la encuesta virtual para la recolección de datos que genera incertidumbre debido que se pierde la interacción con los encuestados los cuales podrían incurrir en una mala coherencia o percepción ocasionado falencias al analizar los datos. Por ello, en la encuesta debe darse preguntas que permitan analizar las dimensiones para obtener claridad y valides; se utilizó el software IBM SPSS Statistics para el análisis de los datos. Asimismo, el alcance de la investigación abarca la mencionada implementación de la ISO. Siendo identificada la escasez de investigaciones respecto a lo antes mencionado, es de importancia dar el presente estudio.

Para la problemática que se ha mencionado, se planteó el siguiente objetivo general: Determinar la incidencia de la implementación ISO/IEC 27001:2013 en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022. Asimismo, la formulación de tres objetivos específicos que son: Determinar la incidencia de la implementación de la ISO/IEC 27001:2013 en los daños de datos de la División de Prensa DIRCII PNP, Lima, 2022; Determinar la incidencia de la implementación de la ISO/IEC 27001:2013 en los daños de sistemas y redes de la División de Prensa DIRCII PNP, Lima, 2022; y Determinar la incidencia de la implementación de la ISO/IEC 27001:2013 en las Interceptaciones no autorizadas de la División de Prensa DIRCII PNP, Lima, 2022.

Y se formula la hipótesis general: La implementación ISO/IEC 27001:2013 incide positivamente en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022. Asimismo, se formulan las hipótesis específicas: La implementación ISO/IEC 27001:2013 incide positivamente en los daños de datos para el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022; La implementación ISO/IEC 27001:2013 incide positivamente en los daños de sistemas y redes para el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022; y La implementación ISO/IEC 27001:2013 incide positivamente en las interceptaciones no autorizadas para el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022.

II. MARCO TEÓRICO

Lopes et al. (2019) concluyeron en que una implementación de la lSO 27001 facilita el cumplimento de la Reglamento General de Protección de Datos (RGPD) de la UE; en los últimos 20 años, dicha regulación cambia la manera de manejar y proteger los datos en la totalidad de sectores, debido a que abarca el tema de forma unificada en la UE. Siendo este reglamento aplicable a los datos personales y no a todos los tipos de datos.

La seguridad de la información mejoró según tesis de maestría, mitigando riesgos informáticos, conllevando a disminuir los tiempos de respuesta ante ataques informáticos mediante la aplicación de la normar ISO 27009 debido que permitió identificar más ampliamente las vulnerabilidades y dar protección a los activos de la información de la organización. Propone una constante capacitación al personal sobre los riesgos y las acciones de respuestas por parte de la empresa (Chipulina, 2020).

En otra tesis, aseveran que es de suma importancia las auditorías a las disposiciones para la protección de la información que tienen las instituciones públicas. Mediante la aplicación del hackeo ético pueden identificar y manejar óptimamente las acciones que permitan mitigar las vulnerabilidades y reponerse antes ataques informáticos. Asimismo, promueve que las entidades realicen al menos un análisis de hackeo ético anual (Taipe, 2018).

Para las pequeñas y microempresas no es tangible la necesidad de contar con seguridad informática. Pero ante la tendencia de la interconexión y digitalizar la información, obvian las amenazas que se relación y lo expuestas que están ante ataques informáticos resultando para ellos en cuantiosas pérdidas económicas. Mediante la aplicación del ISO / IEC 27001:2013 se llevó la evaluación de riesgos a los activos de la información y con esto se alcanzó la identificación de vulnerabilidades y amenazas. Además, atiende la necesidad de la PYME demostrándoles un cálculo del retorno en la inversión en seguridad informática y el costo que originaria un ataque informático a la continuidad del negocio entre otros aspectos que muchos no pueden visualizar (Garay & Sanchez, 2021).

En una propuesta basada en el análisis de riesgos y específicamente en la aplicación del marco de la seguridad cibernética ISO/IEC 27001, permitió la formulación de políticas estratégicas diseñada en recomendaciones de soporte de

decisiones para la seguridad informática. En el modelo se pudo identificar el valor de prioridad (la cual es la clave para establecer recomendaciones prioritarias para la construcción de un SGSI) de la mitigación de amenaza en función de la puntuación de amenaza relativa de la implementación del cumplimiento del ISO/IEC 27001. Tras una evaluación estadística del sistema basado en el SGSI, sus resultados fueron aumento en el cumplimiento de la norma, influenciando en la disminución de amenazas y aumentó de efectividad en la mitigación de ataques cibernéticos (Razikin & Soewito, 2022).

Tang et al. (2021) ante la carencia de acciones que ayuden a proteger a desprevenidos en ser víctimas de delitos cibernéticos que se relacionan con la Covid-19, mediante la teoría del cultivo (realidad social que perjudica a diversos grupos desfavorecidos), se examina las cuentas oficiales de las redes sociales gubernamentales y las acciones de seguridad de la información para que las personas no sean estafadas durante la Covid-19. Tras el análisis se puede ver que los seguidores de dichas cuentas fueron influenciados en sus comportamientos y mejoraron sus acciones de protección y seguridad de la información. La investigación resalta la importancia de las redes sociales gubernamentales durante la Covid-19 en su seguridad informática. Desde temas básicos como mantener actualizado el antivirus en sus dispositivos a no ingresar a sitios web desconocidos, se pudo llegar a informar al sector de la población que usa redes sociales y se informaron sobre temas relacionados a delitos informáticos y la Covid-19, a través de canales oficiales disminuyendo un porcentaje de víctimas de delitos informáticos.

La necesidad de contar con herramientas de videoconferencias para el trabajo remoto y estudios que permitieran la interrelación social, interacción en tiempo real e intercambio de archivos durante el distanciamiento social, despertó el interés de ciberatacantes debido al incremento de sus usos y desconocimiento sobre los peligros existentes al emplearlas (Mediante la aplicación de diversos métodos se unían a reuniones públicas y compartían material que afectaba la sensibilidad de la audiencia y en otros casos enviaban software malicioso para espiar el computador). Convirtiéndose en todo un reto de configurar la seguridad y privacidad. En muchos casos, se realizó el modelado de amenazas y vulnerabilidades; asimismo se definió un plan para prevenir o mitigar potenciales amenazas a los sistemas a fin de

optimizar la seguridad (Hasan & Hasan, 2022).

Franco-Mora et al. (2019) no es exclusivo para grandes empresas sino más bien un aspecto vital para cualquier empresa establecer la seguridad de la información, a través de buenas prácticas permitirá ser competitivos; sin embargo, esto no deja de ser tedioso y costo adoptar un estándar para las pequeñas empresas. Las auditorias son la medida adecuada para el manejo de la seguridad y protección de la información debido que se apoyan en la prevención de incidentes y la mitigación de los riesgos que afecten a los activos de la información. Existen variedad de aplicaciones de auditoría que se ejecutan en el sector privado, pero son costosos, pero no garantiza documentar los servicios de anonimato y confidencialidad. Propone la herramienta llamada SANI implementada abarcando estas capacidades y probada en un escenario operativo real.

Sabillon et al. (2019) sigue demostrándose que el lado más débil de la ciberseguridad son los colaboradores y causan cuantiosas pérdidas a sus empresas, tras el empleo del Modelo de Capacitación en concientización sobre la Ciberseguridad (CATRAM) se capacitó a los diferentes trabajadores que hay en una organización, agrupándolos y brindándoles un contenido específico y objetivos definidos según su labor en la empresa. Esta ayuda a crear una cultura de seguridad de la información si se mantiene una capacitación permitiendo ir algo más que la prevención de incidentes a la ciberseguridad, actualizando al personal sobre el panorama actual de ciberamenazas.

Mirtsch et al. (2021) en un panorama en Alemania sobre la ISO/IEC 27001, se estima mediante el Modelo Probit (Un tipo de elección entre dos opciones) que las empresas no solo buscan contar con certificaciones sino también se refieren en sus sitios web a que sus socios se encuentran certificados. Siendo las empresas grandes las que tienen más opciones de certificarse y la mitad de estas del sector de servicios de TIC. Asimismo, mediante la aplicación para la minería de datos se explora la adopción del mencionado ISO en los estándares en sus sitios web, se obtuvo como hallazgos, que las empresas buscan beneficiarse de la implementación más que contar con la certificación y aprovechan la certificación indirecta (la certificación con que cuenta sus proveedores de centros de datos y nubes). Se demuestra como impulsor potencial de la certificación en las empresas, depende de su capacidad de innovación, del tamaño, afiliación de servicios de

tecnologías de información y comunicaciones.

Wu et al. (2021) en un análisis a la relación entre certificación ISO 27001 y el desempeño financiero corporativo que vienen empleando datos de empresas chinas cotizadas en la bolsa de valores, se observa el impacto de las decisiones corporativas en la obtención y difusión que se encuentra certificada se obtuvo que con el paso de tiempo aumenta el desempeño financiero gradualmente. Y el solo hecho de no dar a conocer que se cuenta con dicha certificación afecta el rendimiento de la empresa.

Tatiara et al. (2018) en Indonesia, en una investigación se analizaron los factores que inhiben la implementación de un SGSI apoyado en la ISO/IEC 27001, se recopilar datos de una encuesta a usuarios en la operación de un centro de datos, mediante el análisis de regresión lineal múltiple y prueba pareada resultaron múltiples factores impiden una implementación exitosa. Se concluyó que es necesario la participación constante y activa de todas las partes de una empresa para alcanzar el éxito en una implementación de un SGSI de forma continua. Para respaldar esta implementación en el futuro se de tener en cuenta lo siguiente: La alta dirección revisará la gestión de la retroalimentación. Asimismo, se debe comunicar y socializar a los empleados las políticas, las funciones, responsabilidades y procedimientos que se relacionan con la gestión de incidentes de la seguridad de información de manera regular. Además, informarles a todas las partes sobre las mejoras que se presentan cada año en la organización y realizar las revisiones periódicas a la implementación del SGSI según lo programado anualmente en el plan de gestión para los riesgos de la seguridad de la información.

Aldya et al. (2019) afirma que una de claves que permite alcanzar el éxito en una implementación de una SGSI en una organización es que se escoja un control de acuerdo con los requerimientos de la organización, teniendo como base la ISO/IEC 27001:2013 es necesario medir la capacidad de cada control aplicado. Asimismo, la ISO/27004:2013 brindó orientación sobre el desarrollo, uso de mediciones y medidas para la apreciación de la efectividad de los controles y grupos de control en el SGSI para establecer la ISO/IEC 27001. Mediante un estudio que tuvo como objetivo la medición de la efectividad del control del SGSI, se creó flujos de pasos en el establecimiento de objeto y los parámetros de medición y las métricas utilizadas con base a las medidas contendidas en el estándar ISO/IEC

27004:2013.

En la globalización de los mercados incrementa la necesidad del internet en diversos aspectos, volviendo un problema de primer nivel la seguridad informática para diferentes tipos organizaciones. Las actividades deben de estar orientadas a aplicar la mejora continua en lo que abarca la gestión de la información que son de suma importancia para las organizaciones. Se convierte en parte del patrimonio de la organización todo tipo de información archivos magnéticos, escritos o vistos por los trabajadores y se le debe de preservar durante todo su ciclo de vida. Por lo tanto, es fundamental implementar un SGSI eficiente que garantice una superioridad competitiva, ayudando a la organización a gestionar y proteger los activos de la información (Accerboni & Sartor, 2019).

Naidoo (2020) bajo el contexto de la Covid-19 en el mundo, al emplear un modelo que relaciona varios niveles para la exploración del aprovechamiento de la situación por parte de los ciberdelincuentes, se evaluó: factores situacionales, identidad de víctimas, suplantaciones de personas y fuentes oficiales, métodos de ataques y técnicas de ingeniería social. Al analizar documentos que registran la comisión de diversos ilícitos cibernéticos que se relacionan con la pandemia, una empresa de ciberseguridad evalúa y revela indicadores como van evolucionando continuamente en reacción a factores situacionales variantes. Tras la investigación se espera brindar recomendaciones orientadas a usuarios finales y organizaciones a fin de contribuir con la seguridad y la enfrentar de mejor manera los diversos desafíos que se vienen dando en el mundo digital.

Hawdon (2021) hoy en día es inimaginable vivir sin acceso a la internet (oscura o superficial), con el comienzo del uso de la World Wide Web se revoluciono la comunicación. La evolución de las TI trae ventajas y desventajas, y define a la acción de usar las TIC para cometer delitos como delitos cibernéticos, siendo sus víctimas las personas y empresas que se involucran con el uso de las TIC. Convirtiendo el ciberespacio en un peligro a pesar al que estamos expuesto debido a nuestro estilo de vida, a pesar que se difunden recomendaciones para el correcto uso. En las redes sociales se pudo identificar que la mayoría de víctimas son mujeres. Cabe resaltar el papel fundamental del autocontrol influye mucho en la probabilidad de ser víctima.

Hawdon (2020) tras declararse en 43 estados de los EE.UU. las personas se

quedarán en casa, se muto a la educación física a en línea y millones de personas perdieron sus trabajos y otros cambien a trabajo remoto, logrando el cambio de rutina. Las acciones ilícitas de las calles disminuyen y las que se dan en los hogares aumenta, comprobando con esto que las tasas de victimización se han alterado, convirtiéndolo a la cibervictimización la de mayor alza producto de la pandemia. Mediante un diseño que rastrea delitos cibernéticos antes y posteriores a la Covid-19, se realiza un experimento natural que evalúo como el confinamiento alteraría las actividades rutinarias de las personas y la probabilidad de ser cibervíctimas. En el modelo se tiene como variable al tiempo (Pre/Post Covid-19). Concluyendo tras los hallazgos, que la pandemia influyó en las ciberrutinas y cibervictimización variaron.

Gryszczynska (2021) la infodemia asociada a la desinformación en tiempos de pandemia, cambió los modus operandi e incremento los casos de ciberdelitos en Polinia. Por lo cual se sugirió adecuar su normativa a fin de reducir los frecuentes ciberataques ocurridos en la pandemia. Surge una necesidad de dar una mejor protección a usuarios sobre phishing a través de la educación de medidas de seguridad proactivas consistentes en el bloqueo de dominios de internet fraudulentos, que buscan obtener datos y recursos financieros de sus cibervíctimas.

Al observar la importancia para los países de Unión Europea el sector Marítimo debido a que el 90% del comercio se realiza por mar, se le considera infraestructura critica para los países, a pesar de ser un tipo de negocio tradicional de transporte, este se ha visto obligado a evolucionar al uso de las TIC a fin de optimizar las labores. Y con el incremento de ciberataques que han aparecido con la pandemia Covid-19, se da la importancia merecida a brindar la ciberseguridad a los puertos, dando cara a la transformación digital y a la situación actual en el ciberespacio. Se considera de suma urgencia del sector, invertir en la adecuación de acciones que identifiquen las vulnerabilidades y amenazas que mitiguen a los ciberataques; asegurando con esto a la continuidad laborar que es vital para los países. Por el momento no existe regulación del tema del sector marítimo-portuario, pero se dio un primer paso en el 2019, al publicar la guía de buenas prácticas de ciberseguridad portuaria (Bocayuva, 2021).

Tras adoptar la implementación de controles obligatorios a la seguridad cibernética en la República de Moldavia (SCRM), las organizaciones públicas

garantizan su protección de datos. En un análisis entre la SCRM y el ISO 27001, cuya intención es cumplir con estándares internacionales se ve reflejada en la Estrategia de Seguridad Nacional de la Información para 2019-2024, garantizando la seguridad de los datos y recursos de las organizaciones de manera efectiva y verificados en el transcurso del tiempo. Asimismo, se busca aumentar las organizaciones públicas cuenten con la certificación ISO y garantizar los niveles internacionales de ciberseguridad y con esto atraer la inversión extranjera. Con los resultados obtenidos se recomienda: Crear SGSI, realizar a los sistemas auditorías internas y externas para saber sobre las tendencias, alienación de los SCRM a los controles de seguridad que contiene la ISO 27001. Se considera de suma importancia garantizar un nivel aceptable de seguridad cibernética y ser obligatoria la implementación y certificación de los estándares (Alexei, 2021).

Ali Jassim et al. (2022) la ISO 27001 se le podría considerar de base para la evaluación de un SGSI. Asimismo, al comparar las dos versiones de ISO, se observó que: ISO/IEC 27001:2005 (Alcanza a la organización, en sus necesidades, en su contexto y en las expectativas de las partes interesadas, determina el alcance de su SGSI, establece procedimientos que tomen oportunidades y riesgos a la seguridad de la información, planificación y control operativo). Y la ISO/IEC 27001:2013 (Define requisitos contractuales legales y reglamentos de seguridad, asegura que el rango siga siendo suficiente, compromiso de la gestión, establece roles y sus respectivas responsabilidades, define el enfoque de evaluación de riesgos, asegura el establecimiento de objetivos y planes de SGSI, establece periodos planificados de evaluación, implementa un plan de tratamiento de riesgos y las aplicaciones de controles. Asimismo, las organizaciones que certificarse del ISO/IEC 27001:2013 obtienen los beneficios como: Mayor credibilidad y aumento de la confianza de las partes interesadas, y destacan en comparación a sus competidores. Se debe contar con diagnóstico de la realidad actual de su SGSI para tener éxito en la implementación.

En el Perú, desde marzo 2020, uno de los problemas que mayor incidencia a alcanzado son las acciones delictivas mediante el uso de sistemas informáticos, la cual fue regulada por la Ley n.°30096, Ley de Delitos Informáticos, del 2013; la cual fue modificada por la Ley n.°30171, en 2014. Teniendo presente Delito Informático se considera aquellas conductas que buscan burlar o dañar los sistemas de

seguridad de dispositivos electrónicos y activos de información comprometiendo la disponibilidad, integridad y confidencialidad. Debido al confinamiento nuestra forma de adquirir activos, pagos de servicios, educación y otros ha evolucionado a un mundo informático con muchos beneficios y nos expone a amenazas y vulnerabilidades; y, por ende, son aprovechadas por cibercriminales. Siendo los delitos más que se cometen el fraude informático y la suplantación de la identidad (Vinelli, 2021).

Se sugiere normalizar a la Estafa Básica dentro de la Ley de Delitos Informáticos de nuestro país, con la finalidad de contrarrestar y disminuir los índices de impunidad. Así, se sancionaría a los agentes delictivos que emplean las TIC para estafar y provocar la equivocación de sus víctimas con la finalidad de apoderarse de sus pertenencias. Tras analizar la gran cantidad de publicaciones fraudulentas por las redes sociales que no están normalizadas, debido que los agentes después de perpetrar sus fechorías se ocultan en el anonimato y esto genera impunidad (Vargas, 2022).

Se considera SGSI, al “conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base los riesgos a los que enfrenta la organización” (Gómez & Fernandez, 2018). Al implantar un SGSI se establece formalizar los procesos y la definición de responsabilidades, basándose a planes, políticas y procedimientos que constarán como información documentada de la organización. Dichos procesos serán de Gestión (Para controlar el funcionamiento y su mejora continua del sistema de gestión) y el proceso de Seguridad (Tratará los aspectos que relación a la seguridad de la información). Asimismo, al diseñar un SGSI se debe aplicar un proceso de mejora continua, partiendo de la última versión a la que le adaptaremos los requerimientos y recursos con que cuenta la organización; solo así, será mejor adoptado por los interesados logrando evolucionar gradualmente y con menor esfuerzo. Para la implantación de un SGSI según la normativa estándar.

La clave para la mantener a las empresas competentes y sobrevivir, es cuidar sus activos de la información a través de una gestión de riesgos eficaz. La ISO 27001 norma la evaluación de los riesgos y la selección de los controles de seguridad. La ISO 27001 está basada en las mejores prácticas comprobadas internacionalmente. Toma metodologías de Evaluación y Tratamiento de Riesgos,

Objetivos de la Gestión, Políticas y alcance de la Seguridad y protección de la Información y la Selección de Controles. Asimismo, aconseja sobre el software que evaluara los riesgos. Se debe tener presente que la ISO/IEC 27001 puede contar con la ISO/IEC 27002 como herramienta de apoyo, debido que cuenta con recomendaciones sobre la implantación de medidas a la seguridad informática y la cual incluye un capítulo que describe estas (Calder & Watkins, 2019).

La ISO/IEC 27001:2013 para Calder (2017) “es la versión actual de la especificación de la norma internacional para un SGSI, neutral respecto al vendedor e independiente de la tecnología”. Se aplica a todo tipo de organización y sectores en cualquier lugar del mundo. El anexo A de la ISO 27001, contiene 14 áreas de control, que identifican objetivos de control y cada una de estas por una o más controles; a la vez, cada uno de los controles numerados secuencialmente haciendo un número de 114 subcláusulas. Este anexo está alineado a la ISO 27002.

Para la descripción de las dimensiones de la variante ISO/ IEC 27001:2013 es una norma internacional de la Seguridad de Información, la cual asegura la disponibilidad, integridad y confidencialidad, de la información y sistemas de una organización. A continuación, se mostrará 3 dimensiones, siendo la Dimensión 1: Análisis de Riesgos, es la identificación de posibles amenazas y vulnerabilidades, lo cual podría hacerlo personal interno o externo; y se apoya en el uso de metodologías, las más conocidas Magerit (Metodología de Análisis y Gestión de Riesgos de los SI de los Administradores Públicas), Mehari, Marion y el Modelo McCumber entre otras. Con la finalidad de reducir riesgos y los costes de recuperación ante ataques no sean excesivamente elevado para la organización. La Dimensión 2: Políticas de Seguridad, son aquellos procedimientos y pautas que brindan soporte a la seguridad según los establecido en los requisitos legales y del negocio; la cual debe ser constantemente revisada, actualizada y comunicada a todo el personal de la organización para su estricto cumplimiento; la metodología que se usa es para definir lo que se puede o no hacer, y se plantean diversos mecanismos de prevención, de protección lógica, detección y recuperación. Dimensión 3: Desarrollo de Auditorias, proceso de agrupar, recoger y evaluar evidencias determinando si un sistema asegura los activos, manteniendo la integridad y cumple los objetivos de una organización; con el fin de que se esté dando un uso eficaz, eficiente y efectivo total de los recursos (Postigo, 2020).

Y para la descripción de las dimensiones de la variante delitos informáticos, González et al. (2018) a finales de los 90, como se venía expandiendo el uso del internet a nivel mundial, se comenzó a emplear el termino Delitos Informáticos al describir aquellos delitos que se cometieron a través del uso de computadoras y/o redes informáticas. Integrantes del denominado grupo 8, se reunión en Lyon-Francia y abordaron los temas relacionados con los problemas emergentes al internet e iniciaron a diseñar el Tratado Delitos Informáticos; con la finalidad de implementar medidas preventivas y evitar que este tipo de delito crezca imparable. Con el pasar del tiempo se convierte en más frecuente. Dimensión 1: Daños a los datos consiste en el acto humano de borrar y/o modificar parcial o total sin tener derecho alguno sobre los activos de información de una empresa u otra persona. Dimensión 2: Daños a los Sistemas y Redes consiste en el acto humano de borrar y/o modificar parcial o total sin tener derecho alguno. Dimensión 3: Interceptaciones no autorizadas que consiste en captación de datos o programas a través de mecanismos tecnológicos sin autorización, con el propósito de obstaculizar el normal funcionamiento de una organización.

Vivimos una era digital producto de las convergencias de las comunicaciones y dispositivos electrónicos; sin embargo, estas tecnologías son explotadas con fines delictivos. Los Delitos Cibernéticos (Cybercrimes) son el desafío constante de los países en mantener sus normas legales actualizadas y alienadas a los acontecimientos diarios. Se puede aprender jurídicamente de experiencias en otros países (Clough, 2010).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

La investigación es tipo básica, dado que “estas son las que conducen a un conjunto de respuestas probables, orientadas a responder aquellas grandes interrogantes, las que forman parte del saber universal, del modo de vida y bienestar social” (Esteban, 2018). Permite crear conocimiento y teorías a pesar de no tener una aplicación inmediata.

La investigación tendrá enfoqué cuantitativo porque el proceso de la investigación se centra en mediciones numéricas y análisis de su estadística, empleando la observación de manera de recolección de datos y los analiza respondiendo las preguntas de la investigación. Plantea, concreta y delimitada el problema que estudiamos. Revisa lo anteriormente ya investigado y la literatura existente. Brinda como conclusión a lo investigado un marco teórico de orientación. Tras recolectar datos se plantean hipótesis que comprueban la veracidad del estudio. Asimismo, si los resultados hipótesis confirman se toma como evidencia a favor, y si las hipótesis refutan se dejan de lado para buscar mejores explicaciones y proponer nuevas hipótesis. Teniendo como base el conocimiento del sujeto, se capta su experiencia y es aceptada; debido que permite analizar los patrones de la conducta del personal PNP (Otero, 2018).

El diseño es no experimental, ya que no se manipularon a las variables y de tipo transversal al realizarse durante un solo momento. Asimismo, es correlacional causal en visto a que se mide la repercusión de la variable independiente implementación de la ISO 27001:2013 sobre la variable dependiente control de delitos informáticos (Rodríguez & Mendivelso, 2018).

Se tendrá en la presente tesis el nivel explicativo debido que mostrará las posibles inferencias y causas de análisis del fenómeno estudiado. Y es utilizado el método Hipotético deductivo, se contrastará las hipótesis causales y los resultados logrados.

3.2. Variables y operacionalización

Variable Independiente:

Implementación de la ISO / IEC 27001:2013 que tiene las dimensiones: Análisis de Riesgos, Políticas de Seguridad y Desarrollo de Auditorías.

Definición Conceptual:

Deane et al. (2019) en los que abarca la seguridad y protección de la información viene ser el estándar más empleado por diversos tipos de organizaciones y es aplicada para asegurar los activos de la información. Brinda pautas de uso internacional para cualquier organización. Además, garantiza un alto nivel de confiabilidad y seguridad que atrae a clientes. Podría resultar en algunos casos costosa por necesitar de personal experto del tema de la implementación de esta ISO. Asimismo, para evaluar y medir el uso en organizaciones se escoge métodos de investigación empírica como la encuesta en línea (con la herramienta SelectSurvey) que permite recolectar datos relacionados a las necesidades de los interesados de una organización. Como variable Independiente es de alta relevancia en consecuencia a su repercusión que genera la variable Dependientes porque agrupan diversas acciones y beneficios para el estudio de una población.

Kurnianto et al. (2018) en una investigación mediante el uso de la ISO/IEC 27001:2013, se evalúa la gestión de la seguridad para la protección de la información que se construyó con PHP, que alcanzó el proceso madurez; asimismo, se analizó las deficiencias para brindar recomendaciones y mapas de ruta. Como resultado de la investigación, se asevera que el proceso de la seguridad de información en el Ministerio del Interior de Indonesia ha sido insuficientemente bueno. Además, se indica a la ISO para calificar la madurez del proceso de la gestión de la seguridad de información. Por último, se acondiciona un anexo de la ISO a la realidad de área, obteniendo un resultado óptimo para resolver el problema de la débil seguridad de la información y debe de mejorar periódicamente. (Anexo 7)

Variable Dependiente:

Control de Delitos Informáticos que tiene las dimensiones: Interceptaciones no autorizadas, Daños de datos y Daños de Sistemas y Redes.

Definición Conceptual:

En un libro en homenaje al experto jurídico, doctor, Felipe Villavicencio; define que los delitos informáticos es la criminalidad informática y que se debe de estudiar y abordar aspectos como el desarrollo tecnológico y la realidad en que surgen.

Asimismo, la adopción de la Ley de delitos información es necesaria para la prevención actos que afecten la disponibilidad, confidencialidad e integridad de los sistemas informáticos, redes y activos de información; se trata de mantener tipificada como delitos la comisión de dichos actos (Cornejo, 2021).

El control de delitos informáticos debe de abarca por toda persona o todo tipo de organización debido que sus actividades diarias se ven expuestas al usar el internet que es indispensable para interrelacionarse con otros. Siendo una gran dificultad identificar y perseguir a los autores quienes mayormente se mantienen en el anonimato. La intervención de los estados se debe al perjuicio de los bienes jurídicos que se tienen que proteger (Patrimonio, intimidad, indemnidad sexual entre otros) y todo aquello que se relacione en ese contexto (Zelada, 2021). (Anexo 7).

Operacionalización de variables:

Villavicencio et al. (2019) implica escoger los indicadores alienados a cada variable, teniendo como base el significado dado en las dimensiones. Asimismo, se debe incluir en las especificaciones esta investigación con el fin de medir una variable. La operacionalización de variables es presentarlas en una tabla y extraer sus partes para facilitar comprenderla inequívocamente. La operacionalización es mostrar al lector la forma que se ha conceptualizado y operativizado las variables, como también la manera a tratar las variables estadísticamente. En una tabla de doble entrada presenta las variables estudiadas, conteniendo las filas variables y las columnas las características de estas. Por tal motivo, la operacionalización brindará una función metodológica de guiar la definición de los objetivos del proyecto que investigamos. Por último, la denominada matriz de consistencia es un esquema llevado a una tabla en la que se explica resumidamente las partes de proyecto de investigación. (Anexo 7)

Bauce et al. (2018) se debe de expresar claramente señalando la importancia de la operacionalización de las variables que se han establecido en el proyecto de investigación; así como también, la facilidad para medir las variables y la construcción de herramientas para la recopilación de datos y así una medición total de las variables. Se trata de encontrar indiciadores para las dimensiones establecidas. La operacionalización de la variable es pasar de un concepto

abstracto a un concepto cuantificable al que le definirán sus dimensiones; teóricamente es someter a la contrastación empírica y con esto tomar métodos más frecuentes. (Anexo 1)

3.3. Población, muestra y muestreo

La población, es la agrupación finita o infinita de sujetos, objetos u otros con características comunes. Viene ser el total de elementos del estudio y se le puede decir a población, universo debido que tienen las mismas características. El investigador la delimita según lo definido en la formulación de estudio. Los tipos de poblaciones las son finita (se conoce la cantidad de sujetos) y la infinita (se desconoce la cantidad de sujetos o supera los 100 000 sujetos la conforman población) (Arias & Covinos, 2021).

La población a estudiar son 100, personal PNP (Efectivos policiales entre Oficiales y Suboficiales, personal CAS y locadores de servicios) de la División de Prensa DIRCII PNP (Con conocimientos en comunicaciones y otras carreras universitarias y técnicas a fines). De los cuales se debe de controlar delitos informáticos que cometan durante sus labores.

Muestra, es parte del universo, solo un subconjunto de la población a estudiar. Al emplear fórmulas se obtiene la cantidad de componentes a estudiar, siendo esta la parte a presentar de la población (Mucha & Lora, 2021). Para la investigación el tamaño de la muestra fue de 50 personas. (Anexo 3).

Muestreo según Viedma (2018) es método para recolectar información y ejecutar inferencias sobre una población partiendo del análisis de una parte, la muestra. El muestreo es de tipo probabilístico, aleatorio simple debido a que se usan métodos buscando que los sujetos tengan similares probabilidades de ser elegidos para ser representados como parte de una muestra, son los más utilizados para mostrar mayor representatividad. Entre los métodos probabilísticos, el muestreo aleatorio simple se utiliza la técnica conociendo a todos los elementos que conforman la población, dándole un número correlativamente a cada sujeto y luego al azar se escoge a los sujetos hasta completar la muestra que requerimos. El método es simple y de poca utilidad práctica ante poblaciones grandes (Hernández & Carpio, 2019).

3.4. Técnicas e instrumentos de recolección de datos

La técnica a usar, es la conocida como encuesta, en cual la información es recolectada a través de esta y se utiliza los indicadores de cada una de las dimensiones y se generan ítems que son cuestionarios para ver la valides y confiabilidad con lo que se mide a cada una de las variables.

Para la prueba de confiabilidad se utilizó el coeficiente Alfa de Cronbach, fue aplicado a los 30 Ítems politómicas tipo Likert del instrumento usado, fue calculado a través del SPSS v25 y se obtuvo de resultado 0.930, demostrando con esto una confiabilidad Excelente, debido que se encuentra en el rango de 0.8-1.0. Concluyendo que el instrumento utilizado es aceptable y procedería su aplicación.

Tabla 1

Valoración de la fiabilidad de ítems según el coeficiente Alfa de Cronbach.

Estadísticas de fiabilidad

Alfa de Cronbach	N de Ítems
,930	30

Fuente: Propia Elaboración (2022).

Instrumento a utilizar es el cuestionario, empleándolo para encuestar al personal PNP de la División de Prensa DIRCII para el control delitos informáticos que comentan al realizar sus labores. La recopilación, proceso e interpretación de la data, se hace a través de las TIC.

3.5. Procedimientos

En esta investigación se desarrolló mediante los procedimientos que a continuación se menciona: primero, al comenzar el proceso de la recolección de datos se coordinó y pidió la participación del personal PNP de la División de Prensa DIRCII en la tesis. También, se les hizo saber los objetivos a efectuar con el desarrollar de la investigación, las dimensiones y los indicadores estimados para cada una de las variables, están detalladas y como estas se alinean con el proceso de recolección de datos, procesamiento e interpretación de datos de los participantes, los mismos que se obtuvieron cumpliendo las medidas de bioseguridad que fueron establecidas por el gobierno con la finalidad de evitar la propagación de la Covid-19. Tras obtener

la autorización del personal PNP, se inició la planificación de la tesis de investigación; asimismo, se identificó los instrumentos a usar en la recolección de datos y del programa informático en el procesamiento de los datos recolectados.

Posteriormente, se comenzó a desarrollar los objetivos de la investigación, iniciando con la búsqueda y valoración de las referencias bibliográficas que ayudo a realizar el presente trabajo de investigación. Subsiguientemente se aplicó una encuesta virtual al personal PNP utilizando los instrumentos de medición de variables y con esto, se ingresó el total de datos al programa informático IBM SPSS Statistics 23.0 para su análisis. Por último, se evaluó los datos que se obtuvieron y se construyó tablas para ser interpretados y evaluar las hipótesis planteadas en este trabajo de investigación.

3.6. Método de análisis de datos

Para el presente trabajo de investigación se utilizaron los instrumentos autorizados por medio del juicio de expertos con la finalidad de comprobar su valides. Según (Stedman, 2021) “el análisis de datos es el proceso de examinar conjuntos de datos para encontrar tendencias y sacar conclusiones sobre la información que contienen”. Para realizar la prueba y validar la hipótesis se aplicó el estadístico de Tau B de Kendall y Regresión ordinal, asimismo, se halló el coeficiente del Alfa de Cronbach para ponderar el nivel de fiabilidad de la magnitud del control de delitos informáticos para personal PNP de la División de Prensa DIRCII.

Amrhein et al. (2018) se utiliza la estadística descriptiva para identificar los niveles. Adicionalmente se emplea la estadística inferencial con lo que se contrasta a las hipótesis por medio de la correlación de estimación de parámetros.

3.7. Aspectos éticos

El presente trabajo de investigación, es de autoría propia y consistió en recolección, procesamiento e interpretación de datos por el autor, están las fuentes bibliográficas correctamente referenciadas según las normas de la American Psychological Association (APA) séptima edición. Asimismo, el presente trabajo de investigación estará evaluado por medio del programa informático Turnitin, obteniendo el generar el debido reporte de originalidad según lo establecido en la resolución del Vicerrectorado de Investigación n.°008-2017-VI/UCV y en los

lineamientos emanados por la Universidad César Vallejo con la Resolución Vicerrectorado de Investigación n.°110-2022/UCV. En lo que fue la recolección de la data se usó la técnica de la encuesta y sus respuestas se utilizaron en el procesamiento e interpretación, tras previamente informar sobre los objetivos y la finalidad del trabajo de investigación al personal PNP, los mismos que brindaron su aprobación.

IV. RESULTADOS

Descripción de resultados

Para la variable 1

Se procesó los datos, y estos se detallan en tabla 2, la variable Implementación de ISO 27001, en la División de Prensa DIRCII PNP y de sus dimensiones Análisis de Riesgo, Política de Seguridad y Desarrollo de Auditorías. Mediante el Baremo Practico se obtuvo que el dato: mínimo es 15 y el dato máximo 41, y se agruparán en 3 grupos, de 8 números, al cual categorizamos en: bajo, medio y alto.

Tabla 2

Encuestados y Porcentajes de los niveles de la Variable ISO27001.

Nivel	Encuestados	Porcentaje
bajo	3	6%
Medio	3	6%
Alto	44	88%
Total	50	100%

Fuente: Propia Elaboración (2022).

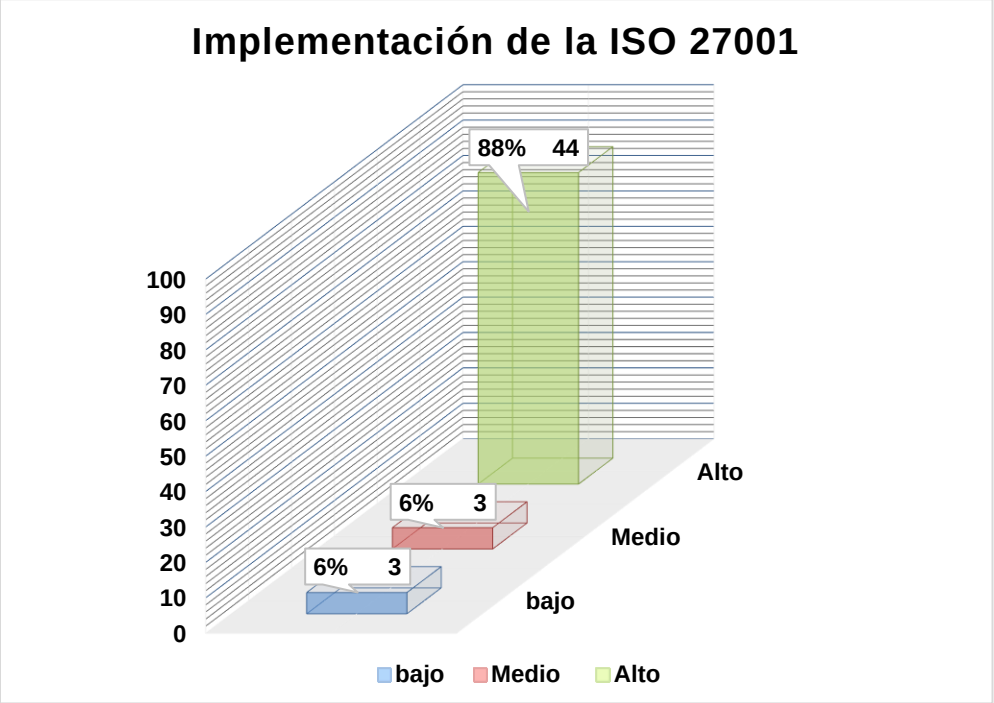


Figura 1: Porcentajes y Encuestados de la Implementación ISO27001.

Fuente: Propia Elaboración (2022).

Asimismo, para la Tabla 2, en los resultados el personal PNP de la DIRCII encuestado opinaron 3 de ellos que es el 6% que la Implementación de la ISO 27001 es bajo, otros 3 que es el 6% opinaron que es medio y los otros 44 que es el 88% opinaron que es bueno.

Tabla 3

Niveles de las dimensiones de la Implementación ISO 27001.

Dimensión 1: Análisis de Riesgos			Dimensión 2: Políticas de Seguridad			Dimensión 3: Desarrollo de Auditorías		
Nivel	**Encuestados**	**Porcentaje**	**Nivel**	**Encuestados**	**Porcentaje**	**Nivel**	**Encuestados**	**Porcentaje**
bajo	6	12%	**bajo**	4	8%	**bajo**	4	8%
Medio	6	12%	**Medio**	28	56%	**Medio**	28	56%
Alto	38	76%	**Alto**	18	36%	**Alto**	18	36%
Total	50	100%	**Total**	50	100%	**Total**	50	100%

Propia Elaboración (2022).

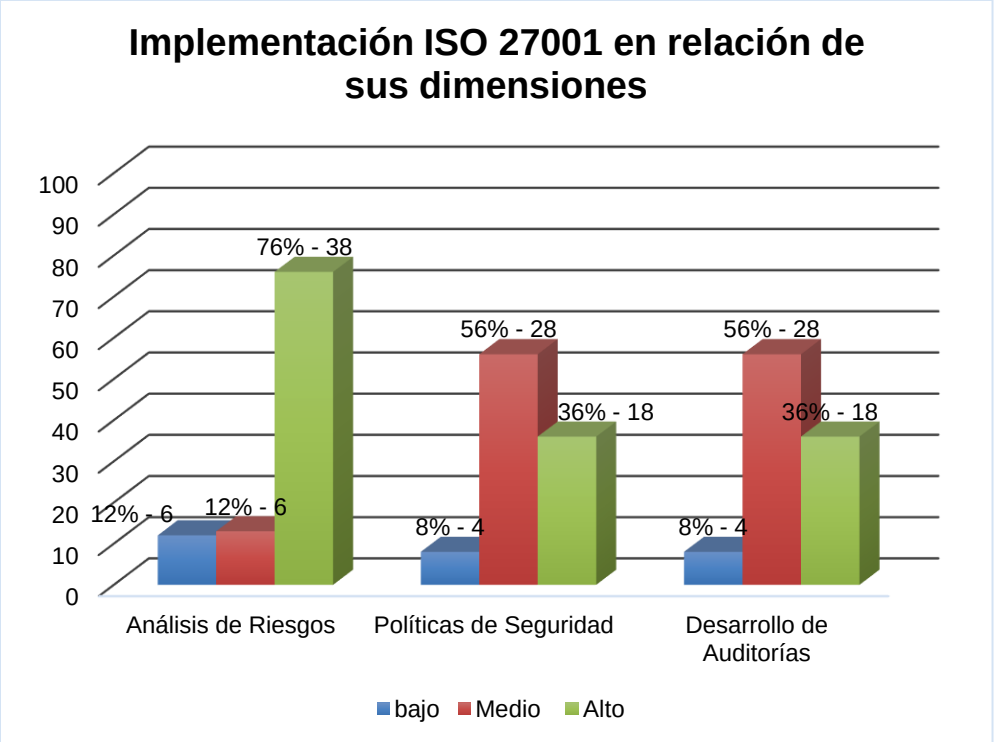


Figura 2: Niveles de las dimensiones de la Implementación ISO 27001.

Fuente: Propia Elaboración (2022).

Se procesó los datos, y estos se detallan en tabla 4, la variable Control de Delitos Informáticos, en la División de Prensa DIRCII PNP y de sus dimensiones Daños de datos, Daños de Sistemas y Redes, y la Interceptaciones no autorizadas. Mediante el Baremo Practico se obtuvo que el dato: mínimo es 15 y el dato máximo 41, y se agruparán en 3 grupos, de 8 números, al cual categorizamos en: bajo, medio y alto.

Tabla 4

Encuestados y Porcentajes de los niveles de la Variable Control de Delitos Informáticos.

Nivel	Encuestados	Porcentaje
bajo	5	10%
Medio	2	4%
Alto	43	86%
Total	50	100%

Fuente: Propia Elaboración (2022).

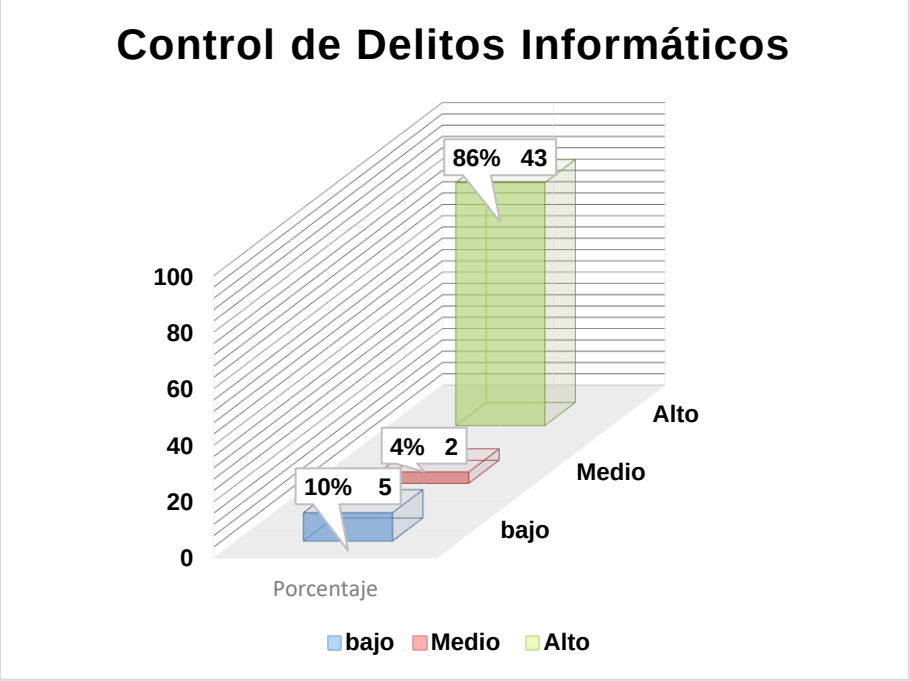


Figura 3: Encuestados y Porcentajes de la Implementación Control de Delitos Informáticos.

Fuente: Propia Elaboración (2022).

Asimismo, para la Tabla 5, en los resultados el personal PNP de la DIRCII encuestado opinaron 5 de ellos que es el 10% que la Implementación de la ISO 27001 es bajo, otros 2 que es el 4% opinaron que es medio y los otros 43 que es el 86% opinaron que es bueno.

Tabla 5

Niveles de las dimensiones del Control de Delitos Informáticos.

Dimensión 1: Daños de datos			Dimensión 2: Daños de Sistemas y Redes			Dimensión 3: Interceptaciones no autorizadas		
Nivel	**Encuestados**	**Porcentaje**	**Nivel**	**Encuestados**	**Porcentaje**	**Nivel**	**Encuestados**	**Porcentaje**
bajo	6	12%	**bajo**	5	10%	**bajo**	2	4%
Medio	8	16%	**Medio**	7	14%	**Medio**	11	22%
Alto	36	72%	**Alto**	38	76%	**Alto**	37	74%
Total	50	100%	**Total**	50	100%	**Total**	50	100%

Fuente: Propia Elaboración (2022).

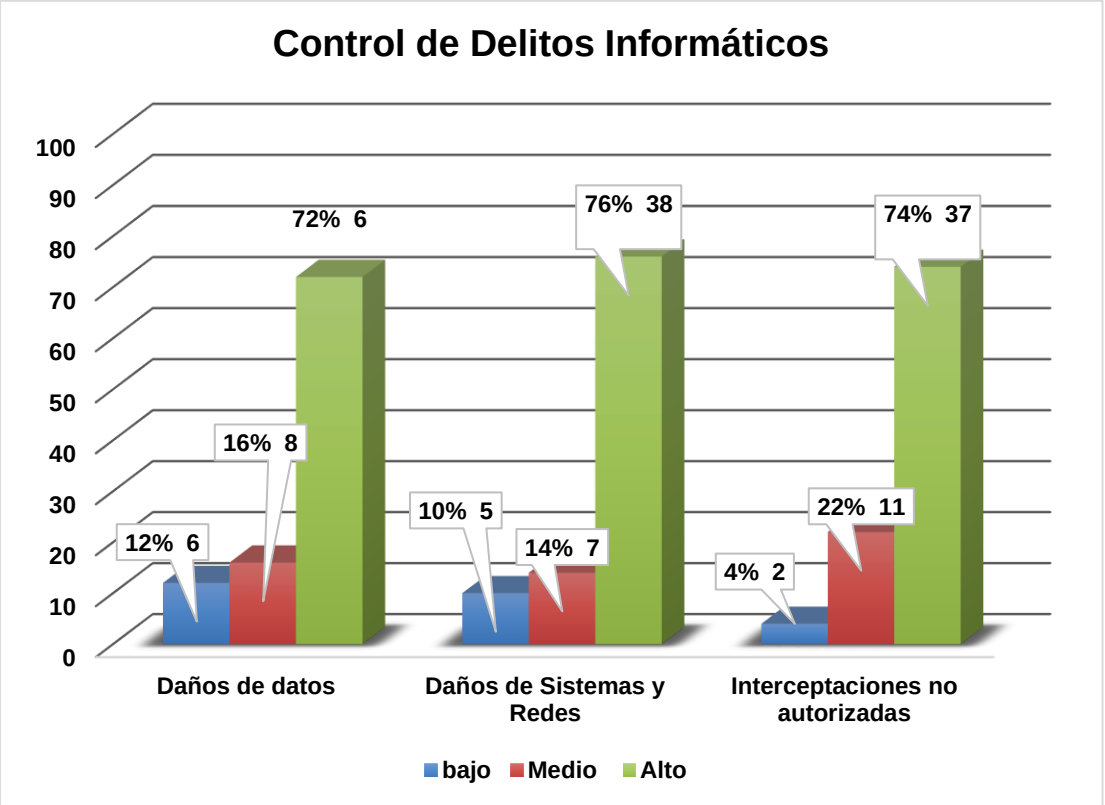


Figura 4: Niveles de las dimensiones de la Control de Delitos Informáticos.

Fuente: Propia Elaboración (2022).

Prueba de hipótesis

Hipótesis general

H0: La implementación ISO / IEC 27001:2013 incide positivamente en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022.

H1: La implementación ISO / IEC 27001:2013 no incide positivamente en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022.

Nivel de la confianza es: 95%
Margen de error es: 5%
Estadístico de Prueba: Regresión Logístico Ordinal y Nagelkerke

En la tabla 6, muestra que la información sobre la implementación ISO / IEC 27001:2013 incide positivamente en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022. Lo obtenido es: p_valor < 0,05 en todos los casos y el estadístico Tau-b de Kendall asume que el valor es ,904. Por lo tanto, se prueba que incide positivamente en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022.

Tabla 6

Información sobre la implementación ISO 27001 incide positivamente en el control de delitos informáticos.

Medidas simétricas

		Valor	Error estándar asintótico[a]	T aproximada[b]	Significación aproximada
Ordinal por ordinal	Tau-b de Kendall	,904	,060	3,386	,001
N de casos válidos		50			

a. No se presupone la hipótesis nula.

b. Utilización del error estándar asintótico que presupone la hipótesis nula.

Fuente: Propia Elaboración (2022).

En la Tabla 7, se muestra la estimación de parámetros sobre la implementación ISO 27001 incide positivamente en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022. Además, se observa que el coeficiente Wald asociado a cada una de las pruebas es mayor que 5. Afirmando, que (Wald=268,890>5; Sig.= ,000<0,05), siendo predictor (Wald = 580,042> 5; sig. =,000 < 0,05).

Tabla 7

Estimaciones de los parámetros – Prueba de Wald para las variables implementación ISO 27001 y control de delitos informáticos.

Estimaciones de parámetro

			Desv.				Intervalo de confianza al 95%	
		Estimación	Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[CateVar2 = 1]	-23,699	,984	580,042	1	,000	-25,627	-21,770
	[CateVar2 = 2]	-22,156	1,172	357,163	1	,000	-24,453	-19,858
Ubicación	[CateVar1=1]	-24,881	1,517	268,890	1	,000	-27,855	-21,907
	[CateVar1=2]	-23,558	,000	.	1	.	-23,558	-23,558
	[CateVar1=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

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

Fuente: Propia Elaboración (2022).

En la Tabla 8, los estadísticos de la prueba Pseudo R cuadrado que es para analizar el grado de la variabilidad. De los tres estadísticos, se asume el mayor valor (coeficiente de Nagelkerke) entre todos los casos. Asimismo, se obtuvo de medida que la Implementación de la ISO 27001 incide en el Control De Delitos Informáticos en 81.2%.

Tabla 8

Prueba Pseudo R cuadrado.

Pseudo R cuadrado

Cox y Snell	,506
Nagelkerke	,812
McFadden	,722

Función de enlace: Logit.

Fuente: Propia Elaboración (2022).

La significancia asintótica bilateral está en .000 < 0.05, entonces que la hipótesis nula que tengo se aceptó y la hipótesis alterna, se rechaza.

Prueba de hipótesis específica 1

La Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Datos para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022.

Tabla 9

Tabla de Correlaciones Prueba de hipótesis específica 1

			Implementación ISO 27001	Daños de datos
Tau_b de Kendall	Implementación ISO 27001	Coeficiente de correlación	1,000	,691**
		Sig. (bilateral)	.	,000
		N	50	50
	Daños de datos	Coeficiente de correlación	,691**	1,000
		Sig. (bilateral)	,000	.
		N	50	50

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

Fuente: Propia Elaboración (2022).

α= 0,05=5%, p= 0,000 y r=0,691

Con un nivel de significancia al 95%, se observa que el valor calculado es menor que el asumido (0,000<0,05), esto indica aceptar la hipótesis alterna y rechazar la nula. Por consiguiente, existe, la Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Datos para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022. Es decir, existe es muy buena asociación o relación (0,80 a 1,00) entre la Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Datos para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022; entonces, que para el Control de Delitos Informáticos en los Daños de Datos depende de la Implementación ISO / IEC 27001:2013.

Prueba de hipótesis específica 2

La Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Sistemas y Redes para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022.

Tabla 10

Tabla de Correlaciones Prueba de hipótesis específica 2

			Implementación ISO 27001	Daños de Sistemas y Redes
Tau_b de Kendall	Implementación ISO 27001	Coeficiente de correlación	1,000	,569**
		Sig. (bilateral)	.	,000
		N	50	50
	Daños de Sistemas y Redes	Coeficiente de correlación	,569**	1,000
		Sig. (bilateral)	,000	.
		N	50	50

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

Fuente: Propia Elaboración (2022).

α= 0,05=5%, p= 0,000 y r=0,569

Con un nivel de significancia al 95%, se observa que el valor calculado es menor que el asumido (0,000<0,05), esto indica aceptar la hipótesis alterna y rechazar la nula. Por consiguiente, existe, la Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Sistemas y Redes para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022. Es decir, existe, es moderada asociación o relación (0,40 a 0,59) entre la Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Sistemas y Redes para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022; entonces, que para el Control de Delitos Informáticos en los Daños de Sistemas y Redes depende de la Implementación ISO / IEC 27001:2013.

Prueba de hipótesis específica 3

La Implementación ISO / IEC 27001:2013 incide positivamente en las Interceptaciones no autorizadas para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022.

Tabla 11

Tabla de Correlaciones Prueba de hipótesis específica 3

			Implementación ISO 27001	Interceptaciones no autorizadas
Tau_b de Kendall	Implementación ISO 27001	Coeficiente de correlación	1,000	,535**
		Sig. (bilateral)	.	,000
		N	50	50
	Interceptaciones no autorizadas	Coeficiente de correlación	,535**	1,000
		Sig. (bilateral)	,000	.
		N	50	50

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

Fuente: Propia Elaboración (2022).

α= 0,05=5%, p= 0,000 y r=0,535

Con un nivel de significancia al 95%, se observa que el valor calculado es menor que el asumido (0,000<0,05), esto indica aceptar la hipótesis alterna y rechazar la nula. Por consiguiente, existe, la Implementación ISO / IEC 27001:2013 incide positivamente en las Interceptaciones no autorizadas para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022. Es decir, existe es moderada asociación o relación (0,40 a 0,59) entre la Implementación ISO / IEC 27001:2013 incide positivamente en las Interceptaciones no Autorizadas para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022; entonces, que para el Control de Delitos Informáticos en las Interceptaciones no autorizadas depende de la Implementación ISO / IEC 27001:2013.

V. DISCUSIÓN

En lo que respecta a la intensión de conocer al objetivo general de esta presente investigación es determinar la incidencia de la implementación ISO / IEC 27001:2013 en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022; se puede decir que en los resultados obtenidos de nuestra Hipótesis General, el personal PNP de la División de Prensa de la DIRCII PNP, muestra que la información sobre la implementación ISO / IEC 27001:2013 incide positivamente en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022. Lo obtenido es: p_valor < 0,05 en todos los casos y el estadístico Tau-b de Kendall asume que el valor es ,904. Por lo tanto, se prueba que incide positivamente en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022. Además, se observa que el coeficiente Wald asociado a cada una de las pruebas es mayor que 5. Afirmando, que (Wald=268,890>5; Sig.= ,000<0,05), siendo predictor (Wald = 580,042> 5; sig. =,000 < 0,05). los estadísticos de la prueba Pseudo R cuadrado que es para analizar el grado de la variabilidad. De los tres estadísticos, se asume el mayor valor (coeficiente de Nagelkerke) entre todos los casos. Asimismo, se obtuvo de medida que la Implementación de la ISO 27001 incide en el Control De Delitos Informáticos en 81.2%. La significancia asintótica bilateral está en .000 < 0.05, entonces que la hipótesis nula que tengo se aceptó y la hipótesis alterna, se rechaza.

En la relación con los hallazgos obtenidos, estos guardan relación con lo mostrado por Díaz (2021) quien al respecto buscó determinar la percepción de la implementación de la NTP ISO / IEC 27001:2014, se pudo apreciar en términos generales de sus resultados obtenidos de su Hipótesis General que, el 50 % de los encuestados expresaron tras el respectivo balance que la necesidad de implementar es regular, por motivos que su SGSI atiende los requerimientos de seguridad para información sobre sus procesos y operaciones diarias en sus respectivas entidades.

Sin embargo, los resultados obtenidos tras la investigación de Arias (2020) demostraron que en la implementación de la ISO 27001 en el Departamento de TIC de la una empresa privada en el Perú, cuya intención es garantizar la disponibilidad, integridad y confidencialidad de la información, resultando de su Hipótesis General que según los entrevistados, coincidieron que es importante contar con una norma

como esta debido que guía los pasos para mejorar las medidas de seguridad de sus activos de información apoyándose a una adecuada gestión de riesgos que permite ubicarlos y tratarlos. Este autor soporta su investigación en tesis, artículos y otros sobre SGSI apoyados en una ISO 27001.

Asimismo, teniendo presente lo referido por Tatiara et al. (2018) en su investigación que tuvo como objetivo general, analizar los principales factores que inhiben la implementación del SGSI apoyado en la ISO/IEC 27001, y obtuvo de hipótesis general en la cual recopilaron datos de una encuesta a usuarios en la operación de un centro de datos que, es necesario la participación constante y activa de todas las partes de una empresa para alcanzar el éxito en una implementación de un SGSI de forma continua.

Además, teniendo presente la teoría de Calder & Watkins (2019) que la clave para la mantener a las empresas competentes y sobrevivir, es cuidar sus activos de la información a través de una gestión de riesgos eficaz. La ISO 27001 está basada en las mejores prácticas comprobadas internacionalmente. Toma metodologías de Tratamiento de Riesgos y Evaluación, Objetivos de la Gestión, Políticas y alcance de la Seguridad de la Información y la Selección de Controles.

Se obtuvo que el coeficiente Alfa de Cronbach aplicado a 30 Ítems politómicas tipo Likert del instrumento usado, dio de resultado 0.930, demostrando con esto una confiabilidad Excelente, debido que se encuentra en el rango de 0.8-1.0. Concluyendo que el instrumento utilizado es aceptable y procedería su aplicación. Ambas variables tienen su valor de significancia de .000, no son normales, por ese motivo, se empleó la prueba estadística Tau b Kendall, no paramétricas.

En la investigación de Huerta (2020) mediante los hallazgos obtenidos en cuanto a sus hipótesis específicas planteadas, un nivel de significancia estadística p valor= 0,000; permitió el rechazo de su hipótesis nula y dar la aceptación de su hipótesis general que propuso, demostrando estadísticamente que la implementación influye de forma positiva, bajo esa metodología identificó y estableció el nivel de sus riesgos y vulnerabilidades en la empresa, determinando medidas de control para mitigarlos.

Por otro lado, en la intensión de conocer sobre el Objetivo Específico 1, sobre la determinar la incidencia de la implementación de la ISO / IEC 27001:2013 en los daños de datos de la División de Prensa DIRCII PNP, Lima, 2022; se obtuvo como resultado de la Hipótesis Especifica 1 que, del personal PNP de la División de Prensa DIRCII; con un nivel de significancia al 95%, se observa que el valor calculado es menor que el asumido (0,000<0,05), esto indica aceptar la hipótesis alterna y rechazar la nula. Por consiguiente, existe, la Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Datos para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022. Es decir, existe es muy buena asociación o relación (0,80 a 1,00) entre la Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Datos para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022; entonces, que para el Control de Delitos Informáticos en los Daños de Datos depende de la Implementación ISO / IEC 27001:2013. Teniendo presente que el personal PNP es consciente que sin autorización no debo modificar parcial o total los activos de información de la organización. Tampoco deben de borrar parcial o total los activos de información de la organización. Asimismo, no deben permitir que terceros realicen actividades que puedan dañar o borrar los activos de información de la organización. Y ante posibles actividades que hallan dañado o borrar los activos de información de la organización, informarán oportunamente. Además, deben de confirmar la debida autorización antes de borrar o modificar activos de la información de la organización.

Estos guardan relación con los hallazgos obtenidos por Díaz (2020) guarda relación con respecto a su objetivo específico de investigación que es la determinación de la percepción de una implementación de las cláusulas de ejecución de la NTP ISO/IEC 27001:2014, obtuvo de resultado de su Hipótesis Especifica que en esta se percibe como regular y que su valor más alto asciende a 57.9% de lo expresado por sus encuestados; debido que han percibido en un nivel regular el SGSI en sus ítem sobre “1) se relacionan con la formulación y seguimiento de las tareas del POI, 2) que la gestión de riesgos de la seguridad de la información producto del monitoreo del SGSI contribuyen a afrontar los nuevos contextos de su entidad, la suscripción de nuevos contratos, convenios o adendas; así como la medición de la efectividad de los contratos, convenios y planes

ejecutados en sus entidades conforme a lo planteado en las preguntas del cuestionario".

Sin embargo, en los resultados obtenidos por Arias (2020) con respecto a su objetivo específico, demostraron que en lo que respecta a los resultados obtenidos de su Hipótesis Especifico que, sus entrevistados coincidieron, que la ISO 27001, ayudo a gestionar la información de una empresa de manera segura basado en un SGSI, que permitió atenuar el impacto de los riesgo y mitigarlos, evitando cuantiosas pérdidas económicas y sanciones que están asociadas a las vulneraciones de datos, permitiendo obtener beneficios a la empresa, siendo posible fidelizar a los clientes y ofrecer nuevos negocios a clientes. Asimismo, protegió y mejorar la reputación de la organización, cumpliendo con requisitos comerciales, legales y reglamentarios, dando de manera efectiva mejoras a los procesos de trabajo de la institución, ya que ISO 27001 no solo es usa para para poder proteger la información, sino que también influyó en los procesos y gestión de la institución.

Asimismo, teniendo presente la teoría de Fernández (2018) en su investigación presentada en una revista considera la información empresarial como un bien inmaterial y que es propiedad del titular y debe de adoptar las medidas necesarias para su debida protección. Se tiene presente que los Daños a los Datos consiste en el acto humano de borrar y/o modificar parcial o total sin tener derecho alguno sobre los activos de información de una empresa u otra persona.

Por otro lado, en la intensión de conocer sobre el Objetivo Específico 2, sobre la Determinar la incidencia de la implementación de la ISO / IEC 27001:2013 en los daños de sistemas y redes de la División de Prensa DIRCII PNP, Lima, 2022; los resultados obtenidos de la Hipótesis Especifica 2 que, del personal PNP de la DIRCII, Con un nivel de significancia al 95%, se observa que el valor calculado es menor que el asumido (0,000<0,05), esto indica aceptar la hipótesis alterna y rechazar la nula. Por consiguiente, existe, la Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Sistemas y Redes para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022. Es decir, existe, es moderada asociación o relación (0,40 a 0,59) entre la Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Sistemas y Redes para el Control

de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022; entonces, que para el Control de Delitos Informáticos en los Daños de Sistemas y Redes depende de la Implementación ISO / IEC 27001:2013. Teniendo presente que el personal PNP es consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a los sistemas o programas informáticos de la organización, no deben hacerlo. Y que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a las redes informáticas de la organización, no deben hacerlo. Asimismo, no permitir que terceros realicen actividades que puedan dañar y/o borrar los sistemas o redes de la organización. Además, deben de informar oportunamente a mis superiores de posibles actividades que hallan dañado o borrado los sistemas y/o redes de la organización. Y, por último, confirmarán la debida autorización antes de borrar o modificar los sistemas y/o redes de la organización.

Estos guardan relación con los hallazgos obtenidos por Díaz (2020) en su Objetivo Específico de determinar la percepción de implementar las cláusulas de ejecución de la NTP ISO/IEC 27001:2014, se aprecia que esta se percibió como regular, debido que el valor más alto ascendería a los 57.9% por lo expresado por sus encuestados; debido que han percibido en un nivel regular el SGSI en sus ítem sobre “1) se relaciona con la formulación y seguimiento de las tareas del POI, 2) que la gestión de riesgos de la seguridad de la información producto del monitoreo del SGSI contribuyen a afrontar los nuevos contextos de su entidad, la suscripción de nuevos contratos, convenios o adendas; así como la medición de la efectividad de los contratos, convenios y planes ejecutados en sus entidades conforme a lo planteado en las preguntas del cuestionario”.

Sin embargo, en los resultados obtenidos por Arias (2020) en su Objetivo Específico, demostraron su resultado de su Hipótesis Específica, que sus entrevistaron coincidieron en la necesidad de poder determinar una guía que apoye la gestión de la planificación, haciendo presente la guía PMBOK, la cual brinda las acciones necesarias para generar la elaboración de la planificación de manera adecuada, aumentar el control de los riesgos, mejorando la calidad y la eficiencia de la planificación. Realizando un diagrama de Gantt, ayudó a orientar y organizar el empleo adecuado de los recursos, estableciendo las tareas y definiendo las actividades necesarias que se realizará en el transcurso de la implementación,

estableciendo los tiempos realistas.

Asimismo, teniendo presente la teoría de Vinelli (2021) uno de los problemas que mayor incidencia son las acciones delictivas mediante el uso de sistemas informáticos, la que es regulada por la Ley n.°30096, Ley de Delitos Informáticos, del 2013; y fue modificada por la Ley n.°30171, en 2014. Teniendo presente Delito Informático se considera aquellas conductas que buscan burlar o dañar los sistemas de seguridad de dispositivos electrónicos y activos de información comprometiendo la disponibilidad, integridad y confidencialidad. Asimismo, que debido al confinamiento nuestra forma de adquirir activos, pagos de servicios, educación y otros, ha evolucionado a un mundo informático con muchos beneficios y nos expone a amenazas y vulnerabilidades; y, por ende, son aprovechadas por cibercriminales. Además, que Chipulina (2020) trató sobre la mejora de la seguridad de la información accionando en la mitigación de riesgos informáticos, disminuir los tiempos de respuesta ante ataques informáticos debido que permitió identificar más ampliamente las vulnerabilidades y dar protección a los activos de la información de la organización. Propone una constante capacitación al personal sobre los riesgos y las acciones de respuestas por parte de una empresa.

Por otro lado, en la intensión de conocer sobre el Objetivo Específico 3, sobre la determinar la incidencia de la implementación de la ISO / IEC 27001:2013 en las Interceptaciones no autorizadas de la División de Prensa DIRCII PNP, Lima, 2022; los resultados obtenidos de la Hipótesis Específica 3, del personal PNP de la DIRCII, con un nivel de significancia al 95%, se observa que el valor calculado es menor que el asumido (0,000<0,05), esto indica aceptar la hipótesis alterna y rechazar la nula. Por consiguiente, existe, la Implementación ISO / IEC 27001:2013 incide positivamente en las Interceptaciones no autorizadas para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022. Es decir, existe es moderada asociación o relación (0,40 a 0,59) entre la Implementación ISO / IEC 27001:2013 incide positivamente en las Interceptaciones no Autorizadas para el Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022; entonces, que para el Control de Delitos Informáticos en las Interceptaciones no autorizadas depende de la Implementación ISO / IEC 27001:2013. Teniendo presente que el personal PNP es consciente que la interceptación de datos de

programas informáticos a través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos. Y son consciente que la interceptación de las redes a través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos. Y que no permiten que, sin autorización, terceros realicen actividades de interceptación de datos de programas informáticos y/o redes a través de mecanismos tecnológicos. Además, que informan oportunamente a mis superiores, sobre posibles actividades que intercepten información sobre la organización. Y en ningún momento, apoyaría la interceptación de terceros a los activos de la información.

Estos guardan relación con los hallazgos obtenidos por Díaz (2020) con respecto a su Objetivo Específico, en buscó determinar la percepción de implementar de cláusulas para la mejora continua con la NTP ISO/IEC-27001:2014, quien obtuvo de resultado de su Hipótesis Específica, se apreciar que esta es percibida como regular, dado que el valor más alto asciende a 60.5% según lo expresado por sus encuestados; que han percibido que en un nivel regular en el SGSI de sus entidades: “1) la documentación del incumplimiento de los requisitos de la NTP ISO/IEC-27001:2014, 2) los planes de acción para corregir los incumplimientos, y 3) los informes frecuentes de las acciones de mejora continua, contribuyen a mejorar la seguridad de la información de sus entidades, conforme a lo planteado en las preguntas del cuestionario”.

Sin embargo, en los resultados obtenidos por Arias (2020) en su Objetivo Específico, demostraron que, del resultado obtenido de su Hipótesis Específica, que coincidieron sus entrevistados en que la implementación consiste en poner en ejecución lo planificado, respetando los tiempos asignados a tareas organizadas y los recursos ya establecidos, bajo un personal responsable. Estableciendo las políticas necesarias permitiendo así tener los resultados esperados, además redacta dos entregables para la guía y gestión del uso que son el manual de procedimientos y su uso del manual de riesgo. Debido que él estudió de manera detallada las políticas, los requisitos, resultados de la evaluación de riesgos determinando el contenido de los documentos y la clasificación de los resultados.

Asimismo, teniendo presente la teoría de Clough (2010) Los Delitos Cibernéticos (Cybercrimes) son el desafío constante de los países en mantener sus normas legales actualizadas y alienadas a los acontecimientos diarios. Se puede

aprender jurídicamente de experiencias en otros países. Las Interceptaciones no autorizadas consiste en captación de datos o programas a través de mecanismos tecnológicos sin autorización, con el propósito de obstaculizar el normal funcionamiento de una organización. Por último, Vivimos una era digital producto de las convergencias de las comunicaciones y dispositivos electrónicos; sin embargo, estas tecnologías son explotadas con fines delictivos.

VI. CONCLUSIONES

En este trabajo de investigación:

Primera: Se determinó la incidencia de la implementación ISO / IEC 27001:2013 en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022; se obtuvo de medida que la Implementación de la ISO 27001 incide en el Control De Delitos Informáticos en 81.2%.

Segunda: Se determinó la incidencia de la implementación de la ISO / IEC 27001:2013 en los daños de datos de la División de Prensa DIRCII PNP, Lima, 2022; existe, r=0,691 es muy buena asociación o relación (0,80 a 1,00) entre la Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Datos para el Control de Delitos Informáticos.

Tercera: Se determinó la incidencia de la implementación de la ISO / IEC 27001:2013 en los daños de sistemas y redes de la División de Prensa DIRCII PNP, Lima, 2022; existe, r=0,569 es moderada asociación o relación (0,40 a 0,59) entre la Implementación ISO / IEC 27001:2013 incide positivamente en los Daños de Sistemas y Redes para el Control de Delitos Informáticos.

Cuarta: Se determinó la incidencia de la implementación de la ISO / IEC 27001:2013 en las Interceptaciones no autorizadas de la División de Prensa DIRCII PNP, Lima, 2022; existe, r=0,535 es moderada asociación o relación (0,40 a 0,59) entre la Implementación ISO / IEC 27001:2013 incide positivamente en las Interceptaciones no Autorizadas para el Control de Delitos Informáticos.

VII. RECOMENDACIONES

Primera: El director de Comunicación e Imagen Institucional-DIRCII de la PNP debe establecer implementar un ISO / IEC 27001:2013 para el control de delitos informáticos, en la División de Prensa DIRCII PNP. Sus lineamientos de gestión se deben enforcar en medidas para mitigar las amenazas y gestionar los riesgos a la seguridad de los activos de información, respaldados en el instrumento de esta investigación. Debe de evitarse tanto movimiento de personal.

Segunda: El director de Comunicación e Imagen Institucional-DIRCII de la PNP debe establecer la capacitación constantemente e informar a todos el personal PNP que labora en la División de Prensa DIRCII PNP sobre las medidas para garantizar la seguridad de los activos de información. Respaldados en el instrumento de esta investigación.

Tercera: El director de Comunicación e Imagen Institucional-DIRCII de la PNP debe revisar la gestión de la retroalimentación. Asimismo, Establecer se comunique y se socialice al personal PNP las políticas, las funciones, responsabilidades y procedimientos que se relacionan con su gestión de incidentes de la seguridad de información de manera constante.

Cuarta: El director de Comunicación e Imagen Institucional-DIRCII de la PNP debe establecer se le informe al personal PNP sobre las mejoras que se presentan cada año en la organización y realizar las revisiones periódicas a la implementación del SGSI según lo programado anualmente en el plan de gestión de riesgos de la seguridad de la información.

REFERENCIAS

Accerboni, F., & Sartor, M. (9 de mayo de 2019). Quality Management: Tools, Methods, and Standards. UK, UK: Emerald Publishing Limited. Obtenido de https://web.s.ebscohost.com/ehost/detail/detail?vid=0&sid=0ebdf52e-b54b-4591-8121-45a693b986f5%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=1949715&db=e000xww

Aldya, A., Sutikno, S., & Rosmansyah, Y. (1 de julio de 2019). Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard. IOP Publishing, Vol.550 (1), 12020. Obtenido de https://www.proquest.com/docview/2561102098/abstract/E90DABA794184192PQ/1?accountid=37408

Alexei, A. (2 de enero de 2021). ensuring information security in public organizations in the republic of moldova through the iso 27001 standard. DSpace Repository, Vol. IV, no. 1 (2021), 84 - 94. Obtenido de https://jss.utm.md/wp-content/uploads/sites/21/2021/03/JSS-1-2021_84-94.pdf

Ali Jassim, N., Moneim Al-Zahir, B., & Makki Khazraji, A. (2 de marzo de 2022). diagnosing the current information systems security department in the information technology department according to the international standard (ISO/IEC 27001: 2013). Journal of Management Information & Decision Sciences, 2022 Special Issue, 1-8. Obtenido de https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=2b6aa768-eef0-470d-b8b8-5867b090daee%40redis

Aliaga, C. (2021). Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información. Implementación de un Sistema de Ciberseguridad para la prevención de los ataques cibernéticos en la Empresa Radiadores Fortaleza, 2021. Universidad César Vellejo, Perú. Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/70776/Aliaga_YCA-SD.pdf?sequence=1&isAllowed=y

Amrhein, V., Trafimow, D., & Greenland, S. (19 de junio de 2018). Inferential Statistics Are Descriptive Statistics. PeerJ preprints. Obtenido de

https://www.proquest.com/docview/2071996993?pq-origsite=primo&parentSessionId=wAmx2OHtumXwY%2Fmy2aaswEQv5fv8DcrEpw2T0RajlTg%3D

ANDINA. (31 de marzo de 2020). Perú sufrió más de 28 millones de ataques de acceso remoto en 2020. Obtenido de https://andina.pe/agencia/noticia-peru-sufrio-mas-28-millones-ataques-acceso-remoto-2020-839524.aspx

Arias Quispe, E. . (2020). Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao. UCV, Callao, Perú. Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QES-SD.pdf?sequence=1&isAllowed=y

Arias, E. (2020). Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información. Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao. Universidad César Vallejo, Lima, Perú. Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QES-SD.pdf?sequence=1&isAllowed=y

Arias, J., & Covinos, M. (2021). Diseño y metodología de la investigación. Arequipa, Perú. Obtenido de http://repositorio.concytec.gob.pe/handle/20.500.12390/2260

Arteaga, F. (12 de mayo de 2020). Real Instituto Elcano. Obtenido de https://www.realinstitutoelcano.org/analisis/ciberseguridad-en-tiempos-de-pandemia-repaso-a-la-covid-19/

Bauce, G., Córdova, M., & Avila, A. (2018). Operacionalización de variables. Revista del Instituto Nacional de Higiene “Rafael Rangel”, 43-49. Obtenido de https://revista.vps.co.ve/wp-content/uploads/2020/12/Revista-cientifica_vol_49_2.pdf#page=52

Bocayuva, M. (27 de mayo de 2021). Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic. (B. S. Heidelberg, Ed.) WMU journal of maritime affairs, Vol.20 (2), 173-192. Obtenido de https://link.springer.com/content/pdf/10.1007/s13437-021-00240-4.pdf

Bohorquez, A. (2021). Maestro en Ingeniería de Sistemas con Mención en

Tecnologías de la. Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020. Universidad César Vallejo, Perú. Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/63128/Bohorquez_SAI-SD.pdf?sequence=1&isAllowed=y

Calder, A. (2017). ISO 27001 ANEXO A. En A. Calder, ISO27001/ISO27002: una Guía de Bolsillo (pág. 64). Reino Unido: IT Governance Ltd. Obtenido de https://ebookcentral.proquest.com/lib/bibliioucv/reader.action?docID=5255172

Calder, A., & Watkins, S. (2019). Information security risk management for ISO 27001/ISO 27002 (Tercera ed.). (E. :. Cambridge, Ed.) Reino Unido: IT Governance Publishing, 2019. Obtenido de https://web.p.ebscohost.com/ehost/ebookviewer/ebook/ZTAwMHh3d19fMjI0NzQ3N19fQU41?sid=8f9c23f6-9c96-4169-ab99-62dd25fea69e@redis&vid=0&format=EB&rid=1

Chaves, E., & Rodríguez, L. (21 de mayo de 2018). Análisis de confiabilidad y validez de un cuestionario sobre entornos personales de aprendizaje (PLE). Revista Ensayos Pedagógicos, 71 a la 106 . Obtenido de https://www.revistas.una.ac.cr/index.php/ensayospedagogicos/article/view/10645/13202

Chipulina, L. (2020). Aplicación de la norma ISO 27009 para prevenir riesgos del sistema de información en la empresa Telefónica, Surquillo. Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información. Universidad César Vallejo, Lima, Perú. Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/58557/Chipulina_PL-SD.pdf?sequence=1&isAllowed=y

Clough, J. (2010). Principles of cybercrime. EE.UU: Cambridge: Cambridge University Press. Obtenido de https://web.s.ebscohost.com/ehost/ebookviewer/ebook/ZTAwMHh3d19fMzE3NjQ2X19BTg2?sid=a31932ae-a6f0-43fd-bdb6-bf9ac341f6dd@redis&vid=0&format=EB&rid=1

Cornejo, J. (2021). Criminalidad Informática y la Discusión Sobre el Bien Jurídico Protegido en los Delitos Informáticos. Perú. Obtenido de

https://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/182684/Cornejo%20Arismedi.pdf?sequence=1&isAllowed=y

Dávalos, W. (2021). Plan del Proyecto de Investigación. “Análisis y diseño de una aplicación tecnológica para automatizar el marco de gestión de ciberseguridad, basado en la norma ISO / IEC 27032”. Universidad Internacional de Ecuador, Ecuador. Obtenido de https://repositorio.uide.edu.ec/bitstream/37000/4641/1/T-UIDE-0150.pdf

Deane, J., Goldberg, D., Rakes, T., & Rees, L. (1 de enero de 2019). The Effect of Information Security Certification Announcements on the Market Value of the Firm. nformation technology and management 20.3, 107–121. Obtenido de https://link.springer.com/article/10.1007/s10799-018-00297-3#citeas

Díaz Lara, V. L. (2021). Percepción de la implementación de la NTP-ISO/IEC 27001:2014 en base a la información documentada del gobierno central del. UVC, Lima, Lima, Perú. Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/76216/Diaz_LVL-SD.pdf?sequence=1&isAllowed=y

Esteban, N. (2018). TIPOS DE INVESTIGACIÓN. Obtenido de https://core.ac.uk/download/pdf/250080756.pdf

Fernández Díaz, C. (enero de 2018). El delito de daños y el espionaje empresarial: dos ataques compatibles conta la información como bien inmaterial. InDret Revista para el análisis del derecho. Obtenido de https://raco.cat/index.php/InDret/article/view/368909/462744

Franco-Mora, D. C., Porras-Castro, H. O., Corredor-Chavarro, F. A., & Calderón-Bogotá, C. (6 de diciembre de 2019). SANI: Assistant for Information Security Auditing on ISO/IEC 27001. Visión Electrónica. Obtenido de https://revistas.udistrital.edu.co/index.php/visele/article/view/18434/17386

Garay, L., & Sanchez, A. (2021). Propuesta de mejora de la gestión de seguridad de la información en la empresa mobiliaria PEVISO Ingenieros SAC Lima – Perú, 2020. Propuesta de mejora de la gestión de seguridad de la información en la empresa mobiliaria PEVISO Ingenieros SAC Lima – Perú, 2020. Escuela de Post Grado NEUMANN, Tacna, Perú. Obtenido de https://repositorio.epneumann.edu.pe/xmlui/bitstream/handle/20.500.12892/273/TRABAJO_DE_INV_MTI_SANCHEZ_SE%c3%91A_GARAY_QUISBE

RT.pdf?sequence=1&isAllowed=y

Gómez, L., & Fernandez, P. (2018). Cómo Implantar Un SGSI Según ISO/IEC 27001. En L. Gómez Fernández, P. Fernández Rivero, & AENOR (Ed.), Cómo Implantar Un SGSI Según ISO/IEC 27001 (2018 ed., pág. 13). Colombia, Colombia, Colombia: Alfaomega. Obtenido de https://www.alphaeditorialcloud.com/reader/como-implantar-un-sgsi-segun-isoiec-27001?location=12

González, J., Bermeo, J., Villacreses, E., & Guerrero, J. (2018). Delitos Informáticos: Una Revisión En Latinoamérica. En C. d. UTMACH (Ed.), Conference Proceedings UTMACH, 2, págs. 180-185. Ecuador. Obtenido de https://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/article/view/262/215

Gryszczynska, A. (1 de agosto de 2021). The impact of the COVID-19 pandemic on cybercrime. Bulletin of the Polish Academy of Sciences. Technical sciences, Vol.69 (4). Obtenido de https://journals.pan.pl/dlibra/publication/137933/edition/120374/content

Hasan, R., & Hasan, R. (8 de abril de 2022). Chapter 7 - Novel AI and Data Science Advancements for Sustainability in the Era of COVID-19. Academic Press, 181-199. Obtenido de https://www.elsevier.com/books/novel-ai-and-data-science-advancements-for-sustainability-in-the-era-of-covid-19/chang/978-0-323-90054-6

Hawdon, J. (10 de noviembre de 2021). Cybercrime: Victimization, Perpetration, and Techniques. (N. Y. US, Ed.) American Journal of Criminal Justice . Obtenido de https://link.springer.com/content/pdf/10.1007/s12103-021-09652-7.pdf

Hawdon, J., Part, K., & Dearden, T. E. (10 de junio de 2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. (N. Y. US, Ed.) American Journal of Criminal Justice, Vol.45 (4), 546-562. Obtenido de https://link.springer.com/content/pdf/10.1007/s12103-020-09534-4.pdf

Hawdon, J., Parti, K., & Dearden, T. E. (10 de junio de 2020). Cybercrime in America amid COVID-19: the Initial. (N. Y. US, Ed.) American journal of criminal justice, Vol.45 (4), 546-562. Obtenido de https://link.springer.com/content/pdf/10.1007/s12103-020-09534-4.pdf

Hernández, C., & Carpio, N. (15 de enero de 2019). Introducción a los tipos de muestreo. Alerta, Revista científica del Instituto Nacional de Salud, 2, 76. Obtenido de https://camjol.info/index.php/alerta/article/download/7535/7746

Huerta Agurto, C. (2020). Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019. UCV, Lima, Perú. Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/46037/Huerta_ACA-SD.pdf?sequence=1&isAllowed=y

INTERPOL. (4 de agosto de 2020). Organización International de Policía Criminal-INTERPOL. Obtenido de Organización International de Policía Criminal-INTERPOL: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19#:~:text=Dominios%20malignos%20%2D%20Se%20ha%20producido,coronavirus%E2%80%9D%20o%2

Kurnianto, A., Isnanto, R., & Puji Widodo, A. (1 de enero de 2018). Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs. E3S Web de Conferencias, 31. Obtenido de https://www.e3s-conferences.org/articles/e3sconf/pdf/2018/06/e3sconf_icenis2018_11013.pdf

Lopes, I., Guarda, T., & Oliveira, P. (22 de agosto de 2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. Journal of Information Systems Engineering & Management. Obtenido de https://www.researchgate.net/profile/Teresa-Guarda/publication/335358551_Implementation_of_ISO_27001_Standards_as_GDPR_Compliance_Facilitator/links/5dfa207fa6fdcc2837290260/Implementation-of-ISO-27001-Standards-as-GDPR-Compliance-Facilitator.pdf

Mirtsch, M., Kinne, J., & Blind, K. . (1 de febrero de 2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001:A Web Mining-Based Analysis. IEEE Transactions On Engineering Management, Vol.68 (1), p.87-100. Obtenido de https://ieeexplore.ieee.org/ielx7/17/9269132/09082865.pdf

Mucha, L., & Lora, M. (2021). Técnica de muestreo para investigación cuantitativa: aplicación informática. Perú, Perú. Obtenido de http://www.scielo.org.bo/pdf/rpc/v09n08/v09n08a12.pdf

Naidoo, R. (3 de mayo de 2020). A multi-level influence model of COVID-19 themed cybercrime. European journal of information systems, Vol.29 (3), 306-321. Obtenido de https://www.tandfonline.com/doi/pdf/10.1080/0960085X.2020.1771222?needAccess=true

Neyra, C. (30 de mayo de 2020). Hackers vulneraron plataforma del Bono Familiar Universal para apropiarse de dineroHackers vulneraron plataforma del Bono Familiar Universal para apropiarse de dinero. Sucesos. Obtenido de https://elcomercio.pe/lima/sucesos/coronavirus-en-peru-hackers-vulneraron-plataforma-del-bono-familiar-para-apropiarse-de-dinero-noticia/

Otero, A. (2018). Enfoqués de investigación. Obtenido de https://www.researchgate.net/profile/Alfredo-Otero-Ortega/publication/326905435_ENFOQUES_DE_INVESTIGACION/links/5b6b7f9992851ca650526dfd/ENFOQUES-DE-INVESTIGACION.pdf

Piera, I. (2021). Desarrollo de un SGSI para un grupo empresarial. Máster Universitario en Ciberseguridad. Universidad de Alicante, España. Obtenido de http://rua.ua.es/dspace/handle/10045/115801

Postigo, A. (2020). Seguridad Informática. Madrid, España, España: Paraninfo. Obtenido de https://books.google.es/books?hl=es&lr=&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=seguridad+inform%C3%A1tica&ots=-HZWji9Ui6&sig=EUh2e7yb9ql9r53U56pTkazuuFk#v=onepage&q=seguridad%20inform%C3%A1tica&f=false

Prue_Ref. (12 de enero de 2020). PNP. Obtenido de www.policia.gob.pe

Razikin, K., & Soewito, B. (16 de marzo de 2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. Revista de informática egipci. Obtenido de https://reader.elsevier.com/reader/sd/pii/S1110866522000226?token=AC89B0B86E051DA055EC80C2A423340ED2468BBA46996BA62E620BD27B3

A41ED4F8E116F29FFB61C94132C6F94D2CA35&originRegion=us-east-1&originCreation=20220430222127

Rodríguez, M., & Mendivelso, F. (14 de septiembre de 2018). Diseño de investigación de corte transversal. Revista médica sanitas, 141-147. Obtenido de https://www.researchgate.net/profile/Fredy-Mendivelso/publication/329051321_Diseno_de_investigacion_de_Corte_Transversal/links/5c1aa22992851c22a3381550/Diseno-de-investigacion-de-Corte-Transversal.pdf

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano M., J. J. (1 de julio de 2019). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. Journal of Cases on Information Technology (JCIT), Vol.21 (3) , p.26-39. Obtenido de https://www.igi-global.com/gateway/article/227676#pnlRecommendationForm

Stedman, C. (1 de mayo de 2021). Análisis o analítica de datos. ComputerWeekly.es. Obtenido de https://www.computerweekly.com/es/definicion/Analisis-o-analitica-de-datos

Stock, J. (4 de agosto de 2020). INTERPOL. Obtenido de INTERPOL: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19#:~:text=Dominios%20malignos%20%2D%20Se%20ha%20producido,coronavirus%E2%80%9D%20o%2

Taipe, D. (2018). la auditoría de seguridad informática y su relación en la ciberseguridad en el sector público año 2018. para optar el grado académico de magíster en ingeniería informática. Universidad Nacional de Piura, Piura, Perú. Obtenido de https://repositorio.unp.edu.pe/bitstream/handle/20.500.12676/2361/INFOR-TAI-DOM-2020.pdf?sequence=1&isAllowed=y

Tang, Z., Warkentin, M., S. Miller, A., & Zhou, Z. . (1 de abril de 2021). Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. Government Information Quarterly. Obtenido de

https://doi.org/10.1016/j.giq.2021.101572

Tatiara, R., Fajar, A. N., Siregar, B., & Gunawan, W. (2018). Analysis of factors that inhibiting implementation of. Journal of Physics: Conference Series. Obtenido de https://iopscience.iop.org/article/10.1088/1742-6596/978/1/012039/pdf

Vargas, W. (2022). Doctor en Derecho. Necesidad de tipificar la estafa básica en la ley de delitos informáticos para reducir la impunidad en el Perú. Universidad Cesár Vallejo, Perú, Perú, Perú. Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/83704

Viedma, C. (2018). Estadística descriptiva e inferencial. Amdrid, España. Obtenido de https://d1wqtxts1xzle7.cloudfront.net/57894581/Estadistica_descriptiva_e_inferencial_-_Carlos_De_La_Puente_Viedma-with-cover-page-v2.pdf?Expires=1652501411&Signature=dZZzdift7lK0bVqWlFg69SUG4-eqbFiy9zrsTQpIgtma8D2N47myVsWU0A7Dh7Esg0R46pWtchSDvxd~JKtcuJk9f

Villavicencio, E., Torracchi, E., Pariona, M., & Alvear, M. (enero de 2019). ¿cómo plantear las variables de una investigación?: operacionalización de las variables. Revista OACTIVA UC Cuenca, 4, 9-14. Obtenido de https://oactiva.ucacue.edu.ec/index.php/oactiva/article/view/289/500

Vinelli, R. (29 de marzo de 2021). Los delitos informáticos y su relación con la criminalidad económica. Ius et Praxis. Obtenido de https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/4995/5428

Wu, W., Shi, K., Wu, C.-H., & Liu, J. (1 de agosto de 2021). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. Journal of Global Information Management, Vol.30 (3), p.1-16. Obtenido de https://www.igi-global.com/viewtitle.aspx?TitleId=281712&isxn=9781799897279

Zelada, E. (17 de mayo de 2021). Delitos informáticos: ¿nuevas formas de criminalidad? deleyes. Obtenido de https://www.deleyes.pe/files/post/274525633-1621261417.pdf

ANEXOS

Anexo 1: Operacionalización de la Variables

Variable de estudio	Definición conceptual	Definición operacional	Dimensión	Indicadores	Escala de medición
Implementación ISO 27001	Deane et al. (2019) en el campo de la seguridad de la información viene ser el estándar más empleado por diversos tipos de organizaciones y es aplicada para asegurar los activos de la información. Brinda pautas de uso internacional para cualquier organización. Además, garantiza un alto nivel de confiabilidad y seguridad que atrae a clientes. Podría resultar en algunos casos costosa por necesitar de personal experto del tema de la implementación de esta ISO. Asimismo, para evaluar y medir el uso en organizaciones se escoge métodos de investigación empírica como la encuesta en línea (con la herramienta SelectSurvey) que permite recolectar datos relacionados a las necesidades de los interesados de una organización. Como variable Independiente es de alta relevancia en consecuencia a su repercusión que genera la variable Dependientes porque agrupan diversas acciones y beneficios para el estudio de una población.	Kurnianto et al. (2018) en una investigación mediante el uso de la ISO / IEC 27001:2013, se evalúa la gestión de la seguridad de información que se construyó con PHP, que alcanzó el proceso madurez; asimismo, se analizó las deficiencias para brindar recomendaciones y mapas de ruta. Como resultado de la investigación, se asevera que el proceso de la seguridad de información en el Ministerio del Interior de Indonesia ha sido insuficientemente bueno. Además, se indica a la ISO para calificar la madurez del proceso de la gestión de la seguridad de información. Por último, se acondiciona un anexo de la ISO a la realidad de área, obteniendo un resultado óptimo para resolver el problema de la débil seguridad de la información y debe de mejorar periódicamente.	Análisis de Riesgos	Impacto	Escala Ordinal Likert Nunca (1) A veces (2) Siempre (3)
				Amenazas	
			Políticas de Seguridad	Requisitos legales	
				Objetivo del negocio	
			Desarrollo de Auditorías	Evaluar	
Control de Delitos Informáticos	En un libro en homenaje al experto jurídico, doctor, Felipe Villavicencio; define que los delitos informáticos es la criminalidad informática y que	El control de delitos informáticos debe de abarca por toda persona o todo tipo de organización debido que sus actividades	Daños de datos	Preventivo	Escala Ordinal Likert

	se debe de estudiar y abordar aspectos como el desarrollo tecnológico y la realidad en que surgen. Asimismo, la adopción de la Ley de delitos información es necesaria para la prevención actos que afecten la integridad, confidencialidad y disponibilidad de los sistemas informáticos, redes y activos de información; se trata de mantener tipificada como delitos la comisión de dichos actos (Cornejo, 2021).	diarias se ven expuestas al usar el internet que es indispensable para interrelacionarse con otros. Siendo una gran dificultad identificar y perseguir a los autores quienes mayormente se mantienen en el anonimato. La intervención de los estados se debe al perjuicio de los bienes jurídicos que se tienen que proteger (Patrimonio, intimidad, indemnidad sexual entre otros) y todo aquello que se relacione en ese contexto (Zelada, 2021).		Correctivo	Nunca (1)
			Daños de Sistemas y Redes	Preventivo	
				Correctivo	A veces (2)
			Interceptaciones no autorizadas	Preventivo	Siempre (3)
				Correctivo	

Fuente: Elaboración propia (2022).

Anexo 2: Instrumentos para la Recolección de Datos

Cuestionario sobre la implementación de la ISO 27001:2013.

El presente cuestionario es de carácter anónimo y sus respuestas se utilizarán para interpretar resultados acordé a la realidad, por ese motivo se le pide demostrar su profesionalismo marcando con una X.

Autor: Mg. Meneses Claudio, Brian Andreé.

Adaptado para la investigación.

Valoración	Categoría
1	Nunca
2	A veces
3	Siempre

Código	Dimensiones	Ítems
AR	Análisis de Riesgos	1,2,3,4,5
PS	Políticas de Seguridad	6,7,8,9,10
DA	Desarrollo de Auditorías	11,12,13,14,15

N.º	Ítem	Nunca	A veces	Siempre
1	Soy consciente de los riesgos existen en el ciberespacio.			
2	Soy consciente que estos riesgos están identificados por nuestra organización.			
3	Continúo realizando acciones que significan poner en riesgo a la organización.			
4	No permito que terceros realicen acciones que signifiquen poner en riesgo a la organización.			
5	Continúo realizando acciones que incrementan los riesgos ya identificados por la organización.			
6	Cumplo con las políticas de seguridad de la organización.			
7	Creo que las políticas de seguridad de la información, mejoran la protección de la organización.			
8	Creo que las políticas de seguridad de la información deben ser cumplida por todos los integrantes de la organización.			
9	Creo que se deben actualizar las políticas de seguridad en la organización.			

10	Realizo mis labores según lo dispuesto en las políticas de seguridad.			
11	Piensas que las auditorias son importantes y necesarias en nuestra organización.			
12	Piensas que permitirán fortalecen la seguridad de la gestión de los sistemas de información.			
13	Las auditorias deben poner más énfasis en las áreas que más presentan descuidos y errores a la seguridad.			
14	Piensas que las auditorias ven las acciones de seguridad preventivas, detectivas y correctivas.			
15	Crees que una auditoria permitiría mejorar y corregir el desempeño de tus labores.			

Cuestionario sobre control de delitos informáticos.

El presente cuestionario es de carácter anónimo y sus respuestas se utilizarán para interpretar resultados acordé a la realidad, por ese motivo se le pide demostrar su profesionalismo marcando con una X.

Autor: Mg. Meneses Claudio, Brian Andreé.

Adaptado para la investigación.

Valoración	Categoría
1	Nunca
2	A veces
3	Siempre

Código	Dimensiones	Ítems
DD	Daños de datos	16, 17, 18, 19, 20
DSR	Daños de Sistemas y Redes	21, 22, 23, 24, 25
INA	Interceptaciones no autorizadas	26, 27, 28, 29, 30

N.º	Ítem	Nunca	A veces	Siempre
16	Soy consciente que sin autorización no debo modificar parcial o total los activos de información de la organización.			
17	Soy consciente que sin autorización no debo borrar parcial o total los activos de información de la organización.			
18	Permito que terceros realicen actividades que puedan dañar o borrar los activos de información de la organización.			
19	Ante posibles actividades que hallan dañado o borrar los activos de información de la organización, informo oportunamente.			
20	Confirmo la debida autorización antes de borrar o modificar activos de la información de la organización.			
21	Soy consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a los sistemas o programas informáticos de la organización, no debo hacerlo.			

22	Soy consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a las redes informáticas de la organización, no debo hacerlo.			
23	Permito que terceros realicen actividades que puedan dañar y/o borrar los sistemas o redes de la organización.			
24	Informo oportunamente a mis superiores de posibles actividades que hallan dañado o borrado los sistemas y/o redes de la organización.			
25	Confirmo la debida autorización antes de borrar o modificar los sistemas y/o redes de la organización.			
26	Soy consciente que la interceptación de datos de programas informáticos a través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos.			
27	Soy consciente que la interceptación de las redes a través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos.			
28	Permito que, sin autorización, terceros realicen actividades de interceptación de datos de programas informáticos y/o redes a través de mecanismos tecnológicos.			
29	Informo oportunamente a mis superiores, sobre posibles actividades que intercepten información sobre la organización.			
30	En ningún momento, apoyaría la interceptación de terceros a los activos de la información.			

Fichas de Instrumentos

Ficha técnica de Instrumento 1

Nombre: Cuestionario sobre la implementación de la ISO 27001:2013.

Finalidad: Determinar la repercusión de la implementación de la ISO / IEC 27001:2013.

Autor(es): Deane et al. (2019). El efecto de los anuncios de certificación de seguridad de la información en el valor de mercado de la empresa. Tecnología y gestión de la información.

Sujetos de aplicación: Personal que labora en la División de Prensa DIRCII PNP (Con conocimientos en Comunicaciones y otras carreras universitarias y técnicas).

Administración: Individual.

Ámbito de Aplicación: División de Prensa DIRCII PNP.

Duración de la toma de datos: 40 minutos.

Ficha técnica de Instrumento 2

Nombre: Cuestionario Control de Delitos Informáticos.

Finalidad: Determinar la repercusión del Control de Delitos Informáticos, en la División de Prensa DIRCII PNP, 2022.

Autor(es): Zelada (2021). Delitos informáticos: ¿nuevas formas de criminalidad? De Leyes.

Sujetos de aplicación: Personal que labora en la División de Prensa DIRCII PNP (Con conocimientos en Comunicaciones y otras carreras universitarias y técnicas).

Administración: Individual.

Ámbito de Aplicación: División de Prensa DIRCII PNP.

Duración de la toma de datos: 40 minutos.

Anexo 3: Cálculo del tamaño de la muestra

El universo o población que se cuenta es de 100 personal PNP, la muestra la identificaremos a utilizarse en la presente investigación se obtendrá al aplicar la ecuación para hallar tamaño de muestra, como se puede apreciar a continuación:

$$n = \frac{k^2 * p * q * N}{\left(e^2 * (\mathrm{N}-1)\right) + k^2 * p * q} \qquad (1)$$

Dónde:

e: error deseado que es esperado al 5%=0.05

p: proporción de sujetos con misma característica de estudio dentro de la población, normalmente se considera 0.5

q: Probabilidad de fracaso, normalmente se espera considerar sea 0.5

n: tamaño de muestra a estudiar

N: tamaño del universo o población.

k: constante que depende del nivel de confianza, del cual se espera 1.0, significando un 95% de nivel de confianza.

Se reemplaza, los datos de la ecuación 1:

$$n = \frac{1.0^2 * 0.5 * 0.5 * 100}{\left(0.05^2 * (100-1)\right) + 1.0^2 * 0.5 * 0.5}$$

=50.25125

En la presente tesis la muestra será de 50 personal PNP.

Anexo 4: Validación de Instrumentos

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA IMPLEMENTACIÓN DE LA ISO 27001:2013.

N.º	Dimensiones / Ítem	Pertinencia 1		Relevancia 2		Claridad 3		Sugerencias
	Análisis de Riesgos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Soy consciente de los riesgos existen en el ciberespacio.	x		x		x		
2	Soy consciente que estos riesgos están identificados por nuestra organización.	x		x		x		
3	Continúo realizando acciones que significan poner en riesgo a la organización.	x		x		x		
4	No permito que terceros realicen acciones que signifiquen poner en riesgo a la organización.	x		x		x		
5	Continúo realizando acciones que incrementan los riesgos ya identificados por la organización.	x		x		x		
	Políticas de Seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	Cumplo con las políticas de seguridad de la organización.	x		x		x		
7	Creo que las políticas de seguridad de la información, mejoran la protección de la organización.	x		x		x		
8	Creo que las políticas de seguridad de la información deben ser cumplida por todos los integrantes de la organización.	x		x		x		
9	Creo que se deben actualizar las políticas de seguridad en la organización.	x		x		x		
10	Realizo mis labores según lo dispuesto en las políticas de seguridad.	x		x		x		
	Desarrollo de Auditorías	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	Pienso que las auditorias son importantes y necesarias en nuestra organización.	x		x		x		
12	Pienso que las auditorias fortalecen la seguridad de la gestión de los sistemas de información.	x		x		x		
13	Pienso que las auditorias deben supervisar con más énfasis, las áreas del negocio que presentan más problemas.	x		x		x		
14	Pienso que las auditorias supervisan como se realizan las acciones de seguridad preventivas, detectivas y correctivas del negocio.	x		x		x		
15	Creo que una auditoria permitiría mejorar y corregir el desempeño de tus labores.	x		x		x		

Observaciones (precisar si hay suficiencia): EXISTE PERTINENCIA

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

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE EL CONTROL DE DELITOS INFORMÁTICOS.

N.º	Dimensiones / Ítem	Pertinencia 1		Relevancia 2		Claridad 3		Sugerencias
	Daños de datos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Soy consciente que sin autorización no debo modificar parcial o total los activos de información de la organización.	x		x		x		
17	Soy consciente que sin autorización no debo borrar parcial o total los activos de información de la organización.	x		x		x		
18	Permito que terceros realicen actividades que puedan dañar o borrar los activos de información de la organización.	x		x		x		
19	Ante posibles actividades que hallan dañado o borrar los activos de información de la organización, informo oportunamente.	x		x		x		
20	Confirmo la debida autorización antes de borrar o modificar activos de la información de la organización.	x		x		x		
	Daños de Sistemas y Redes	**Si**	**No**	**Si**	**No**	**Si**	**No**	

21	Soy consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a los sistemas o programas informáticos de la organización, no debo hacerlo.	x		x		x		
22	Soy consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a las redes informáticas de la organización, no debo hacerlo.	x		x		x		
23	Permito que terceros realicen actividades que puedan dañar y/o borrar los sistemas o redes de la organización.	x		x		x		
24	Informo oportunamente a mis superiores de posibles actividades que hallan dañado o borrado los sistemas y/o redes de la organización.	x		x		x		
25	Confirmo la debida autorización antes de borrar o modificar los sistemas y/o redes de la organización.	x		x		x		
	Interceptaciones no autorizadas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
26	Soy consciente que la interceptación de datos de programas informáticos a través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos.	x		x		x		
27	Soy consciente que la interceptación de las redes a través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos.	x		x		x		
28	Permito que, sin autorización, terceros realicen actividades de interceptación de datos de programas informáticos y/o redes a través de mecanismos tecnológicos.	x		x		x		
29	Informo oportunamente a mis superiores, sobre posibles actividades que intercepten información sobre la organización.	x		x		x		
30	En ningún momento, apoyaría la interceptación de terceros a los activos de la información.	x		x		x		

Observaciones (precisar si hay suficiencia): EXISTE PERTINENCIA

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

Apellidos y nombres del juez validador: Dr. Marlon Frank Acuña Benites

DNI: 42097456

Especialidad del validador: Investigador

22 de mayo del 2022.

1. Pertinencia: El ítem corresponde al concepto teórico formulado.

2. Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.

3. Claridad: Se entiende sin dificultad alguna el enunciado del ítem es conciso, exacto y directo.

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

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA IMPLEMENTACIÓN DE LA ISO 27001:2013.

N.º	Dimensiones / Ítem	Pertinencia 1		Relevancia 2		Claridad 3		Sugerencias
	Análisis de Riesgos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Soy consciente de los riesgos existen en el ciberespacio.	x		x		x		
2	Soy consciente que estos riesgos están identificados por nuestra organización.	x		x		x		
3	Continúo realizando acciones que significan poner en riesgo a la organización.	x		x		x		
4	No permito que terceros realicen acciones que signifiquen poner en riesgo a la organización.	x		x		x		
5	Continúo realizando acciones que incrementan los riesgos ya identificados por la organización.	x		x		x		
	Políticas de Seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	Cumplo con las políticas de seguridad de la organización.	x		x		x		
7	Creo que las políticas de seguridad de la información, mejoran la protección de la organización.	x		x		x		
8	Creo que las políticas de seguridad de la información deben ser cumplida por todos los integrantes de la organización.	x		x		x		
9	Creo que se deben actualizar las políticas de seguridad en la organización.	x		x		x		
10	Realizo mis labores según lo dispuesto en las políticas de seguridad.	x		x		x		
	Desarrollo de Auditorías	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	Pienso que las auditorias son importantes y necesarias en nuestra organización.	x		x		x		
12	Pienso que las auditorias fortalecen la seguridad de la gestión de los sistemas de información.	x		x		x		
13	Pienso que las auditorias deben supervisar con más énfasis, las áreas del negocio que presentan más problemas.	x		x		x		
14	Pienso que las auditorias supervisan como se realizan las acciones de seguridad preventivas, detectivas y correctivas del negocio.	x		x		x		
15	Creo que una auditoria permitiría mejorar y corregir el desempeño de tus labores.	x		x		x		

Observaciones (precisar si hay suficiencia): EXISTE PERTINENCIA

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

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE EL CONTROL DE DELITOS INFORMÁTICOS.

N.º	Dimensiones / Ítem	Pertinencia 1		Relevancia 2		Claridad 3		Sugerencias
	Daños de datos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Soy consciente que sin autorización no debo modificar parcial o total los activos de información de la organización.	x		x		x		
17	Soy consciente que sin autorización no debo borrar parcial o total los activos de información de la organización.	x		x		x		
18	Permito que terceros realicen actividades que puedan dañar o borrar los activos de información de la organización.	x		x		x		
19	Ante posibles actividades que hallan dañado o borrar los activos de información de la organización, informo oportunamente.	x		x		x		
20	Confirmo la debida autorización antes de borrar o modificar activos de la información de la organización.	x		x		x		
	Daños de Sistemas y Redes	**Si**	**No**	**Si**	**No**	**Si**	**No**	
21	Soy consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a los sistemas o programas informáticos de la organización, no debo hacerlo.	x		x		x		

22	Soy consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a las redes informáticas de la organización, no debo hacerlo.	x		x		x		
23	Permito que terceros realicen actividades que puedan dañar y/o borrar los sistemas o redes de la organización.	x		x		x		
24	Informo oportunamente a mis superiores de posibles actividades que hallan dañado o borrado los sistemas y/o redes de la organización.	x		x		x		
25	Confirmo la debida autorización antes de borrar o modificar los sistemas y/o redes de la organización.	x		x		x		
	Interceptaciones no autorizadas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
26	Soy consciente que la interceptación de datos de programas informáticos a través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos.	x		x		x		
27	Soy consciente que la interceptación de las redes a través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos.	x		x		x		
28	Permito que, sin autorización, terceros realicen actividades de interceptación de datos de programas informáticos y/o redes a través de mecanismos tecnológicos.	x		x		x		
29	Informo oportunamente a mis superiores, sobre posibles actividades que intercepten información sobre la organización.	x		x		x		
30	En ningún momento, apoyaría la interceptación de terceros a los activos de la información.	x		x		x		

Observaciones (precisar si hay suficiencia): EXISTE PERTINENCIA

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

Apellidos y nombres del juez validador: Mg. Fernando Javier OVALLE ASENCIOS. **DNI:** 41581658.

Especialidad del validador: Investigador

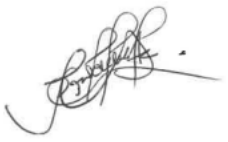
22 de mayo el 2022.

1. Pertinencia: El ítem corresponde al concepto teórico formulado.

2. Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.

3. Claridad: Se entiende sin dificultad alguna el enunciado del ítem es conciso, exacto y directo.

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



Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA IMPLEMENTACIÓN DE LA ISO 27001:2013.

N.º	Dimensiones / Ítem	Pertinencia 1		Relevancia 2		Claridad 3		Sugerencias
	Análisis de Riesgos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Soy consciente de los riesgos existen en el ciberespacio.	x		x		x		
2	Soy consciente que estos riesgos están identificados por nuestra organización.	x		x		x		
3	Continúo realizando acciones que significan poner en riesgo a la organización.	x		x		x		
4	No permito que terceros realicen acciones que signifiquen poner en riesgo a la organización.	x		x		x		
5	Continúo realizando acciones que incrementan los riesgos ya identificados por la organización.	x		x		x		
	Políticas de Seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	Cumplo con las políticas de seguridad de la organización.	x		x		x		
7	Creo que las políticas de seguridad de la información, mejoran la protección de la organización.	x		x		x		
8	Creo que las políticas de seguridad de la información deben ser cumplida por todos los integrantes de la organización.	x		x		x		
9	Creo que se deben actualizar las políticas de seguridad en la organización.	x		x		x		
10	Realizo mis labores según lo dispuesto en las políticas de seguridad.	x		x		x		
	Desarrollo de Auditorías	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	Pienso que las auditorias son importantes y necesarias en nuestra organización.	x		x		x		
12	Pienso que las auditorias fortalecen la seguridad de la gestión de los sistemas de información.	x		x		x		
13	Pienso que las auditorias deben supervisar con más énfasis, las áreas del negocio que presentan más problemas.	x		x		x		
14	Pienso que las auditorias supervisan como se realizan las acciones de seguridad preventivas, detectivas y correctivas del negocio.	x		x		x		
15	Creo que una auditoria permitiría mejorar y corregir el desempeño de tus labores.	x		x		x		

Observaciones (precisar si hay suficiencia): EXISTE PERTINENCIA

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

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE EL CONTROL DE DELITOS INFORMÁTICOS.

N.º	Dimensiones / Ítem	Pertinencia 1		Relevancia 2		Claridad 3		Sugerencias
	Daños de datos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Soy consciente que sin autorización no debo modificar parcial o total los activos de información de la organización.	x		x		x		
17	Soy consciente que sin autorización no debo borrar parcial o total los activos de información de la organización.	x		x		x		
18	Permito que terceros realicen actividades que puedan dañar o borrar los activos de información de la organización.	x		x		x		
19	Ante posibles actividades que hallan dañado o borrar los activos de información de la organización, informo oportunamente.	x		x		x		
20	Confirmo la debida autorización antes de borrar o modificar activos de la información de la organización.	x		x		x		
	Daños de Sistemas y Redes	**Si**	**No**	**Si**	**No**	**Si**	**No**	
21	Soy consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a los sistemas o programas informáticos de la organización, no debo hacerlo.	x		x		x		

22	Soy consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a las redes informáticas de la organización, no debo hacerlo.	x		x		x		
23	Permito que terceros realicen actividades que puedan dañar y/o borrar los sistemas o redes de la organización.	x		x		x		
24	Informo oportunamente a mis superiores de posibles actividades que hallan dañado o borrado los sistemas y/o redes de la organización.	x		x		x		
25	Confirmo la debida autorización antes de borrar o modificar los sistemas y/o redes de la organización.	x		x		x		
	Interceptaciones no autorizadas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
26	Soy consciente que la interceptación de datos de programas informáticos a través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos.	x		x		x		
27	Soy consciente que la interceptación de las redes a través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos.	x		x		x		
28	Permito que, sin autorización, terceros realicen actividades de interceptación de datos de programas informáticos y/o redes a través de mecanismos tecnológicos.	x		x		x		
29	Informo oportunamente a mis superiores, sobre posibles actividades que intercepten información sobre la organización.	x		x		x		
30	En ningún momento, apoyaría la interceptación de terceros a los activos de la información.	x		x		x		

Observaciones (precisar si hay suficiencia): EXISTE PERTINENCIA

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

Apellidos y nombres del juez validador: Mg. Roy Pérez Pichis. **DNI:** 42346887.

Especialidad del validador: Investigador

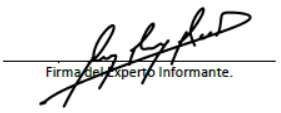
22 de mayo el 2022.

1. Pertinencia: El ítem corresponde al concepto teórico formulado.

2. Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.

3. Claridad: Se entiende sin dificultad alguna el enunciado del ítem es conciso, exacto y directo.

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



Firma del Experto Informante.

Anexo 5: Autorización de la organización para publicar su identidad en los resultados de la investigación

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA ORGANIZACIÓN PARA PUBLICAR SU IDENTIDAD EN LOS RESULTADOS DE LAS INVESTIGACIONES

Datos Generales

Nombre de la Organización:	RUC: 20165465009
Dirección de Comunicación e Imagen Institucional de la Policía Nacional Del Perú.	
Nombre del Titular o Representante legal: Director de Comunicación e Imagen Institucional.	
Nombres y Apellidos Manuel Gustavo Vidarte Perrigo.	DNI: 09940319

Consentimiento:

De conformidad con lo establecido en el artículo 7º, literal "f" del Código de Ética en Investigación de la Universidad César Vallejo [*], autorizo [X], no autorizo [ ] publicar LA IDENTIDAD DE LA ORGANIZACIÓN, en la cual se lleva a cabo la investigación:

Nombre del Trabajo de Investigación	
Implementación ISO 27001 para el Control de Delitos Informáticos en la División de Prensa DIRCII PNP, Lima, 2022.	
Nombre del Programa Académico: MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN.	
Autor: Nombres y Apellidos Jesús Alexander Escobar Gutiérrez.	DNI: 42234862.

En caso de autorizarse, soy consciente que la investigación será alojada en el Repositorio Institucional de la UCV, la misma que será de acceso abierto para los usuarios y podrá ser referenciada en futuras investigaciones, dejando en claro que los derechos de propiedad intelectual corresponden exclusivamente al autor (a) del estudio.

Lugar y Fecha: 26 julio 2022.

Firma:

POLICÍA NACIONAL DEL PERÚ DIRCA

OA - 245198
Manuel Gustavo VIDARTE PERRIGO
CORONEL PNP

(*) Código de Ética en Investigación de la Universidad César Vallejo-Artículo 7º, literal " f " **Para difundir o publicar los resultados de un trabajo de investigación es necesario mantener bajo anonimato el nombre de la institución donde se llevó a cabo el estudio, salvo el caso en que haya un acuerdo formal con el gerente o director de la organización, para que se difunda la identidad de la institución.** Por ello, tanto en los proyectos de investigación como en los informes o tesis, no se deberá incluir la denominación de la organización, pero sí será necesario describir sus características.

Anexo 6: Aspectos administrativos.

6.1. Recursos y Presupuesto

6.1.1. Recursos Humanos

Para este trabajo de investigación es considerado todas las actividades que se realizaron, en vista a esto, se considera todos los costos de recursos humanos, se incluyen la recolección, procesamiento e interpretación de la data, las fuentes bibliográficas y movilidad. Asimismo, es considerado a algunas coordinaciones presenciales necesarias que se hicieron, cada una de las actividades se encuentra especificada en la Tabla 12.

Tabla 12

Presupuesto de Recursos Humanos

Recursos	Descripción	Monto
Data	Recolección y procesamiento	S/3,000.00
Referencias	Fuentes bibliográficas	S/200.00
Transporte	Movilidad	S/100.00
	Total	S/3,300.00

Fuente: elaboración propia (2022).

6.1.2. Recursos de Hardware

Se consideró un equipo fue utilizado en la presente investigación, la cual fue una computadora portátil y una impresa de sistema continuo, como se encuentra especificada en la Tabla 13.

Tabla 13

Presupuesto de Recursos Hardware

Recursos	Descripción	Monto
Equipo	Computadora portátil (Marca Lenovo, Core I7 12Th)	S/4,500.00
Impresora	Epson multifuncional	S/800.00
	Total	S/5,300.00

Fuente: elaboración propia (2022).

6.1.3. Recursos de Software

Para el proceso de la recolección y procesamiento de datos fue utilizado el software llamado SPSS de IBM, como se encuentra especificada en la Tabla 14.

Tabla 14

Presupuesto de Recursos Software

Recursos	Descripción	Monto
Licencia	IBM SPSS Statistics (Un usuario) con tablas personalizadas y estadística avanzada; muestreo complejo y pruebas; y pronósticos y árboles de decisión.	S/1,400.00
Ofimática	Microsoft 365 Business Premium	S/400.00
	Total	S/1,800.00

Fuente: elaboración propia (2022).

6.1.4. Presupuesto

Con la sumatoria de los presupuestos anteriormente mencionados se obtiene el presupuesto total que se requiere para el trabajo de investigación, como se encuentra especificada en la Tabla 15.

Tabla 15

Presupuesto total

Sumatoria de costos	Monto
Presupuesto de Recursos Humanos	S/3,300.00
Presupuesto de Recursos Hardware	S/5,300.00
Presupuesto de Recursos Software	S/1,800.00
Presupuesto total	S/10,400.00

Fuente: elaboración propia (2022).

6.2. Financiamiento

En este trabajo de investigación desarrollado en la Universidad César Vallejo, se llevó un estudio con el cual se fortalece el conocimiento de área correspondiente. Todo el presupuesto antes explicado será financiad por la División de Prensa DIRCII PNP (Recursos de Hardware) y por el suscrito investigador (Presupuesto de Recursos Humanos y Recursos Software).

Tabla 16

Financiamiento

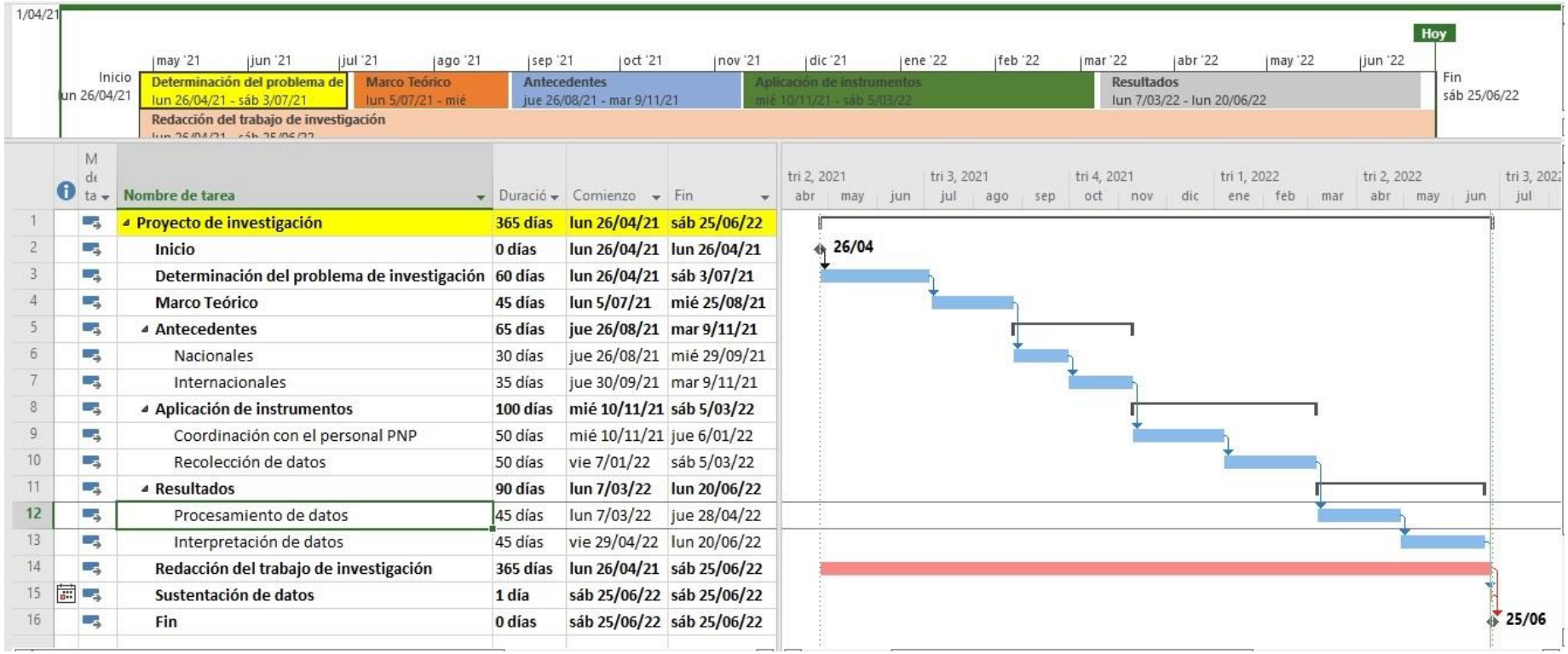
Entidad Financiadora	Monto	Porcentaje
La División de Prensa DIRCII PNP		50.97%
Presupuesto de Recursos Hardware	S/5,300.00	
EL suscrito investigador		49.03%
Presupuesto de Recursos Software	S/3,300.00	
Presupuesto de Recursos Software	S/1,800.00	
Financiamiento total	S/10,400.00	100%

Fuente: elaboración propia (2022).

6.3. Cronograma de Ejecución

En este Cronograma de Ejecución se mostrará específicamente las tareas y periodos que tomará el realizar la presente investigación.

Figura 5: Cronograma de ejecución



Fuente: Elaboración propia (2022).

Anexo 7: Matriz de consistencia

TÍTULO: Implementación ISO 27001 para el Control de Delitos Informáticos en la División de Prensa DIRCII PNP, Lima, 2022.

AUTOR: JESÚS ALEXANDER ESCOBAR GUTIERREZ

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES				
Problema general:	**Objetivo general:**	**Hipótesis general:**	**V 1: Implementación ISO 27001**				
			Dimensiones	**Indicadores**	**Ítems**	**Escala de medición**	**Niveles y rangos**
¿Cómo incide la implementación de la ISO / IEC 27001:2013 en el control de delitos informáticos en la División de Prensa DIRCII PNP, Lima, 2022?	Determinar la incidencia de la implementación ISO / IEC 27001:2013 en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022.	La implementación ISO / IEC 27001:2013 incide positivamente en el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022.	Análisis de Riesgos	Impacto	Del 1 al 5	Escala Ordinal Likert Nunca (1) A veces (2) Siempre (3)	Baja [15 -22] Media [23 - 30] Alta [31 -41]
				Amenazas			
Problemas específicos:	**Objetivos específicos:**	**Hipótesis especificas:**	Políticas de Seguridad	Requisitos legales	Del 6 al 10		
				Objetivo del negocio			
Problema específico 1:	**Objetivo específico 1:**	**Hipótesis específica 1:**					
¿Cómo incide la implementación de la ISO / IEC 27001:2013 en los daños de datos de la División de Prensa DIRCII PNP, Lima, 2022?	Determinar la incidencia de la implementación de la ISO / IEC 27001:2013 en los daños de datos de la División de Prensa DIRCII PNP, Lima, 2022.	La implementación ISO / IEC 27001:2013 incide positivamente en los daños de datos para el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022.	Desarrollo de Auditorías	Evaluar	Del 11 al 15		

			V 2: Control de Delitos Informáticos				
			Dimensiones	**Indicadores**	**Ítems**	**Escala de medición**	**Niveles y rangos**
Problema específico 2: ¿Cómo incide la implementación ISO / IEC 27001:2013 en los daños de sistemas y redes de la División de Prensa DIRCII PNP, Lima, 2022?	**Objetivo específico 2:** Determinar la incidencia de la implementación de la ISO / IEC 27001:2013 en los daños de sistemas y redes de la División de Prensa DIRCII PNP, Lima, 2022.	**Hipótesis específica 2:** La implementación ISO / IEC 27001:2013 incide positivamente en los daños de sistemas y redes para el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022.	Daños de datos	Preventivo	Del 16 al 20	Escala Ordinal Likert Rara vez (1) Varias veces (2) Siempre (3)	Baja [15 -22] Media [23 - 30] Alta [31 -41]
				Correctivo			
			Daños de Sistemas y Redes	Preventivo	Del 21 al 25		
				Correctivo			
Problema específico 3: ¿Cómo incide la implementación de la ISO / IEC 27001:2013 en las interceptaciones no autorizadas de la División de Prensa DIRCII PNP, Lima, 2022?	**Objetivo específico 3:** Determinar la incidencia de la implementación de la ISO / IEC 27001:2013 en las Interceptaciones no autorizadas de la División de Prensa DIRCII PNP, Lima, 2022.	**Hipótesis específica 3:** La implementación ISO / IEC 27001:2013 incide positivamente en las interceptaciones no autorizadas para el control de delitos informáticos, en la División de Prensa DIRCII PNP, 2022.	Interceptaciones no autorizadas	Preventiva	Del 26 al 30		
				Correctiva			

Nivel-Diseño de investigación	Población y muestra	Técnicas e Instrumentos	Estadística por utilizar
Tipo investigación: Básica. **Diseño:** No experimental. Corte transversal. Correlacional causal. **Método:** Hipotético deductivo. **Enfoque:** Tipo Cuantitativo.	**Población: 100** Personal que labora en la División de Prensa DIRCII PNP (Con conocimientos en Comunicaciones y otras carreras universitarias y técnicas). Efectivos policiales entre Oficiales y Suboficiales, personal CAS y locadores de servicios. **Tipo de muestreo:** Probabilística-aleatoria simple. **Tamaño de muestra:**	**Variable 1:** Implementación ISO 27001. **Técnica:** Encuesta. **Instrumentos:** Cuestionario virtual. **Autor:** Deane et al. (2019). El efecto de los anuncios de certificación de seguridad de la información en el valor de mercado de la empresa. Tecnología y gestión de la información. **Año:** 2019. **Monitoreo: 2022** **Ámbito de aplicación**	**Descriptiva:** Se utiliza la estadística descriptiva para identificar los niveles y aplicó el instrumento de recolección de datos, posteriormente fue procesada en SPSS 23. **Inferencial:** Se emplea la estadística inferencial con lo que se contrasta a las hipótesis por medio de la correlación de estimación de parámetros. No se realizó prueba de normalidad porque se trabajó con niveles y no con

Nivel: Explicativo	50 personal PNP.	División de Prensa DIRCII PNP. **Forma de administración:** Individual	números. Se obtuvo p_valor < 0,05 en todos los casos y el estadístico **Tau-b de Kendall y Regresión ordinal,** no paramétricas asume que el valor es ,904. Demostrando, que incide 81.2% Se halló el coeficiente Alfa De Cronbach que permitió cuantificar el nivel de fiabilidad de la magnitud del Control de Delitos Informáticos durante la Covid-19 en personal PNP que labora en la División de Prensa DIRCII PNP.
		Variable 2: Control de Delitos Informáticos. **Técnica:** Encuesta. **Instrumentos:** Cuestionario virtual. **Autor:** Zelada (2021). Delitos informáticos: ¿nuevas formas de criminalidad? De Leyes. **Año:** 2021. **Monitoreo: 2022** **Ámbito de aplicación**	

		División de Prensa DIRCII PNP. **Forma de administración:** Individual	

Fuente: Elaboración propia (2022).

Anexo 8: Formulario Virtual en Google Forms

Cuestionario sobre la implementación de la ISO 27001:2013

1. Soy consciente de los riesgos existen en el ciberespacio. *

- ◯ Nunca
- ◯ A veces
- ◯ Siempre

2. Soy consciente que estos riesgos están identificados por nuestra organización. *

- ◯ Nunca
- ◯ A veces
- ◯ Siempre

3. Continúo realizando acciones que significan poner en riesgo a la organización. *

- ◯ Nunca
- ◯ A veces
- ◯ Siempre

4. No permito que terceros realicen acciones que signifiquen poner en riesgo a la organización. *

- ◯ Nunca
- ◯ A veces
- ◯ Siempre

5. Continúo realizando acciones que incrementan los riesgos ya identificados por la organización. *

- ◯ Nunca
- ◯ A veces
- ◯ Siempre

6. Cumplo con las políticas de seguridad de la organización. *

- ◯ Nunca
- ◯ A veces
- ◯ Siempre

7. Creo que las políticas de seguridad de la información, mejoran la protección de la organización. *

- ◯ Nunca
- ◯ A veces
- ◯ Siempre

8. Creo que las políticas de seguridad de la información deben ser cumplida por todos los integrantes de la organización. *

- ◯ Nunca
- ◯ A veces
- ◯ Siempre

9. Creo que se deben actualizar las políticas de seguridad en la organización. *

- Nunca
- A veces
- Siempre

10. Realizo mis labores según lo dispuesto en las políticas de seguridad. *

- Nunca
- A veces
- Siempre

11. Pienso que las auditorías son importantes y necesarias en nuestra organización. *

- Nunca
- A veces
- Siempre

12. Pienso que las auditorías fortalecen la seguridad de la gestión de los sistemas de información. *

- Nunca
- A veces
- Siempre

13. Pienso que las auditorías deben supervisar con más énfasis, las áreas del negocio que presentan más problemas. *

- Nunca
- A veces
- Siempre

14. Pienso que las auditorías supervisan como se realizan las acciones de seguridad preventivas, detectivas y correctivas del negocio. *

- Nunca
- A veces
- Siempre

15. Creo que una auditoría permitiría mejorar y corregir el desempeño de tus labores. *

- Nunca
- A veces
- Siempre

Atrás Siguiente Borrar formulario

Este contenido no ha sido creado ni aprobado por Google. Notificar uso inadecuado - Términos del Servicio - Política de Privacidad

Google Formularios

Cuestionario sobre Control de Delitos Informáticos

16. Soy consciente que sin autorización no debo modificar parcial o total los activos de información de la organización. *

- Nunca
- A veces
- Siempre

17. Soy consciente que sin autorización no debo borrar parcial o total los activos de información de la organización. *

- Nunca
- A veces
- Siempre

18. Permito que terceros realicen actividades que puedan dañar o borrar los activos de información de la organización. *

- Nunca
- A veces
- Siempre

19. Ante posibles actividades que hallan dañado o borrar los activos de información de la organización, informo oportunamente. *

- Nunca
- A veces
- Siempre

20. Confirmo la debida autorización antes de borrar o modificar activos de la información de la organización. *

- Nunca
- A veces
- Siempre

21. Soy consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a los sistemas o programas informáticos de la organización, no debo hacerlo. *

- Nunca
- A veces
- Siempre

22. Soy consciente que, de poder acceder sin autorización a modificar y/o borrar parcial o totalmente a las redes informáticas de la organización, no debo hacerlo. *

- Nunca
- A veces
- Siempre

23. Permito que terceros realicen actividades que puedan dañar y/o borrar los sistemas o redes de la organización. *

- Nunca
- A veces
- Siempre

24. Informo oportunamente a mis superiores de posibles actividades que hallan * dañado o borrado los sistemas y/o redes de la organización.

- Nunca
- A veces
- Siempre

25. Confirmo la debida autorización antes de borrar o modificar los sistemas y/o * redes de la organización.

- Nunca
- A veces
- Siempre

26. Soy consciente que la interceptación de datos de programas informáticos a * través de mecanismos tecnológicos, sin autorización de la organización, están prohibidos.

- Nunca
- A veces
- Siempre

27. Soy consciente que la interceptación de las redes a través de mecanismos * tecnológicos, sin autorización de la organización, están prohibidos.

- Nunca
- A veces
- Siempre

28. Permito que, sin autorización, terceros realicen actividades de * interceptación de datos de programas informáticos y/o redes a través de mecanismos tecnológicos.

- Nunca
- A veces
- Siempre

29. Informo oportunamente a mis superiores, sobre posibles actividades que * intercepten información sobre la organización.

- Nunca
- A veces
- Siempre

30. En ningún momento, apoyaria la interceptación de terceros a los activos de * la información.

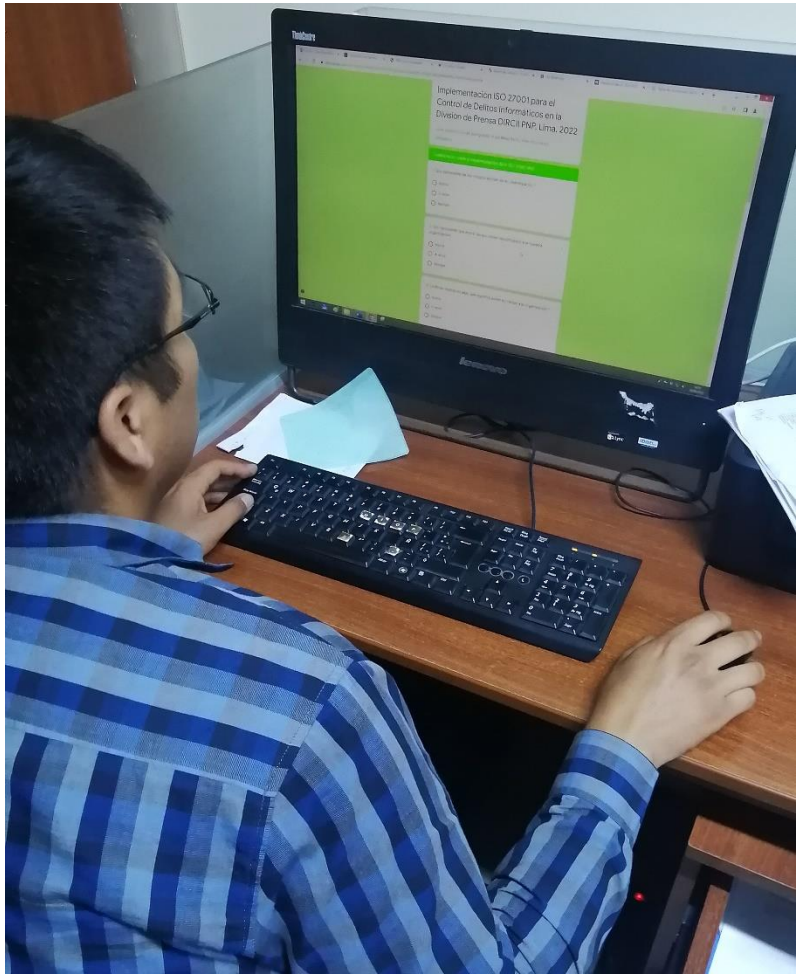
- Nunca
- A veces
- Siempre

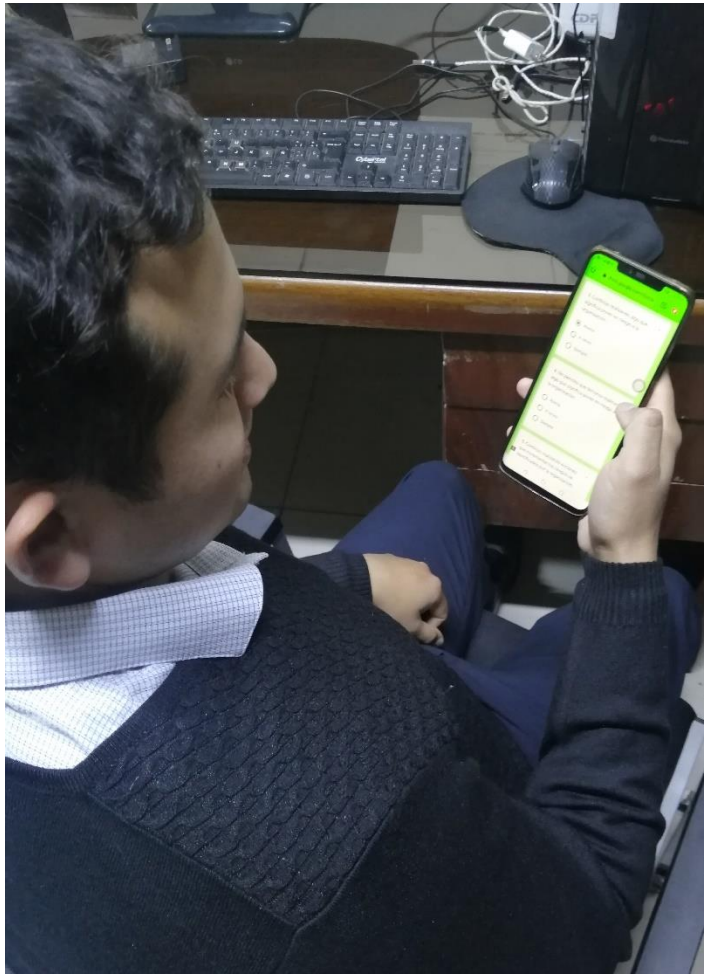
Atrás Enviar Borrar formulario

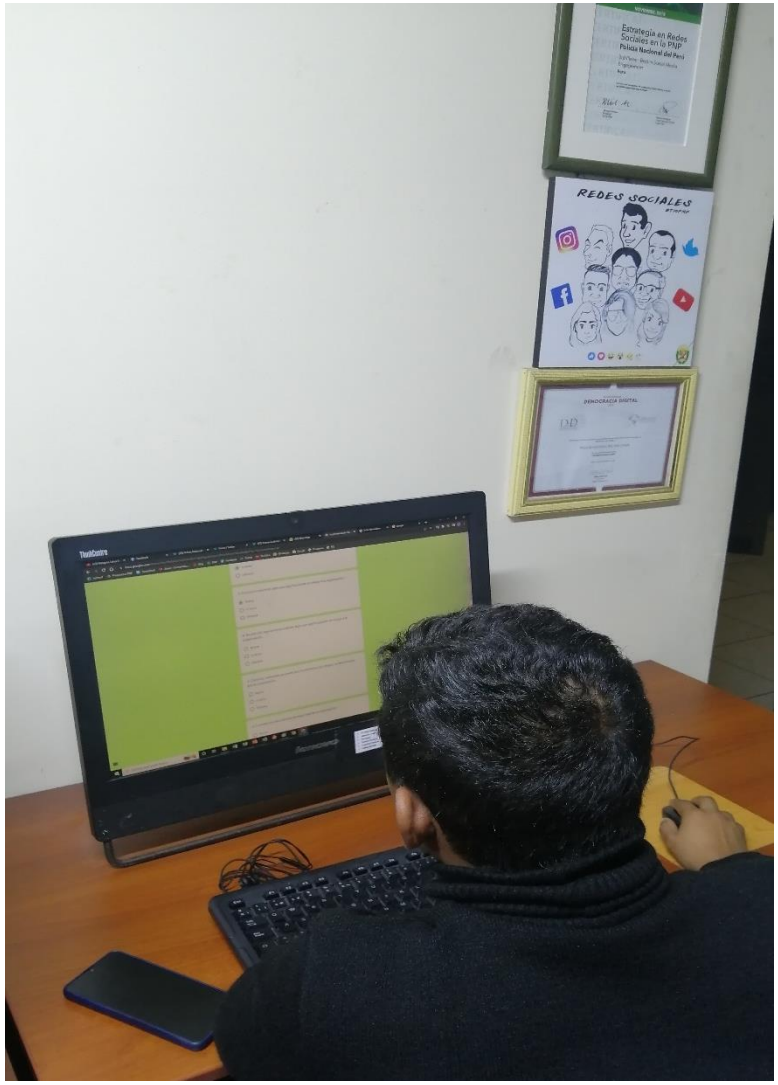
Este contenido no ha sido creado ni aprobado por Google. Notificar uso inadecuado - Términos del Servicio - Política de Privacidad

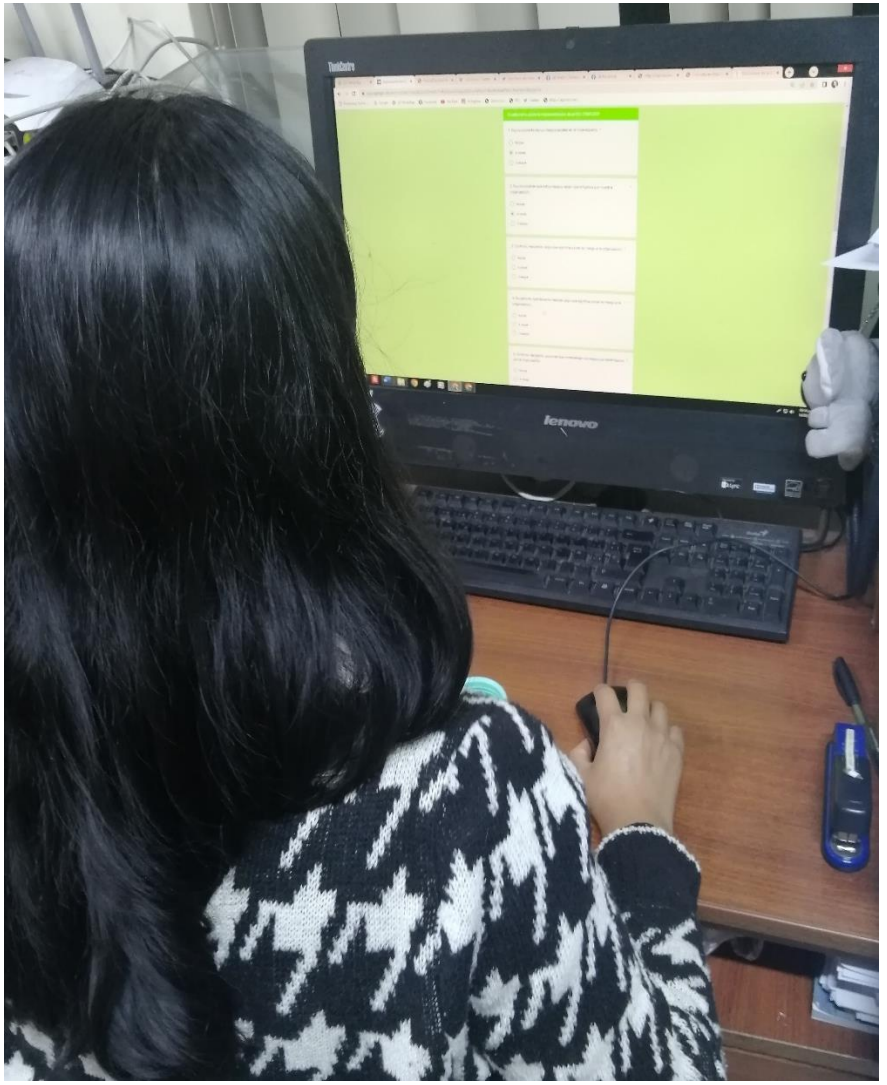
Google Formularios

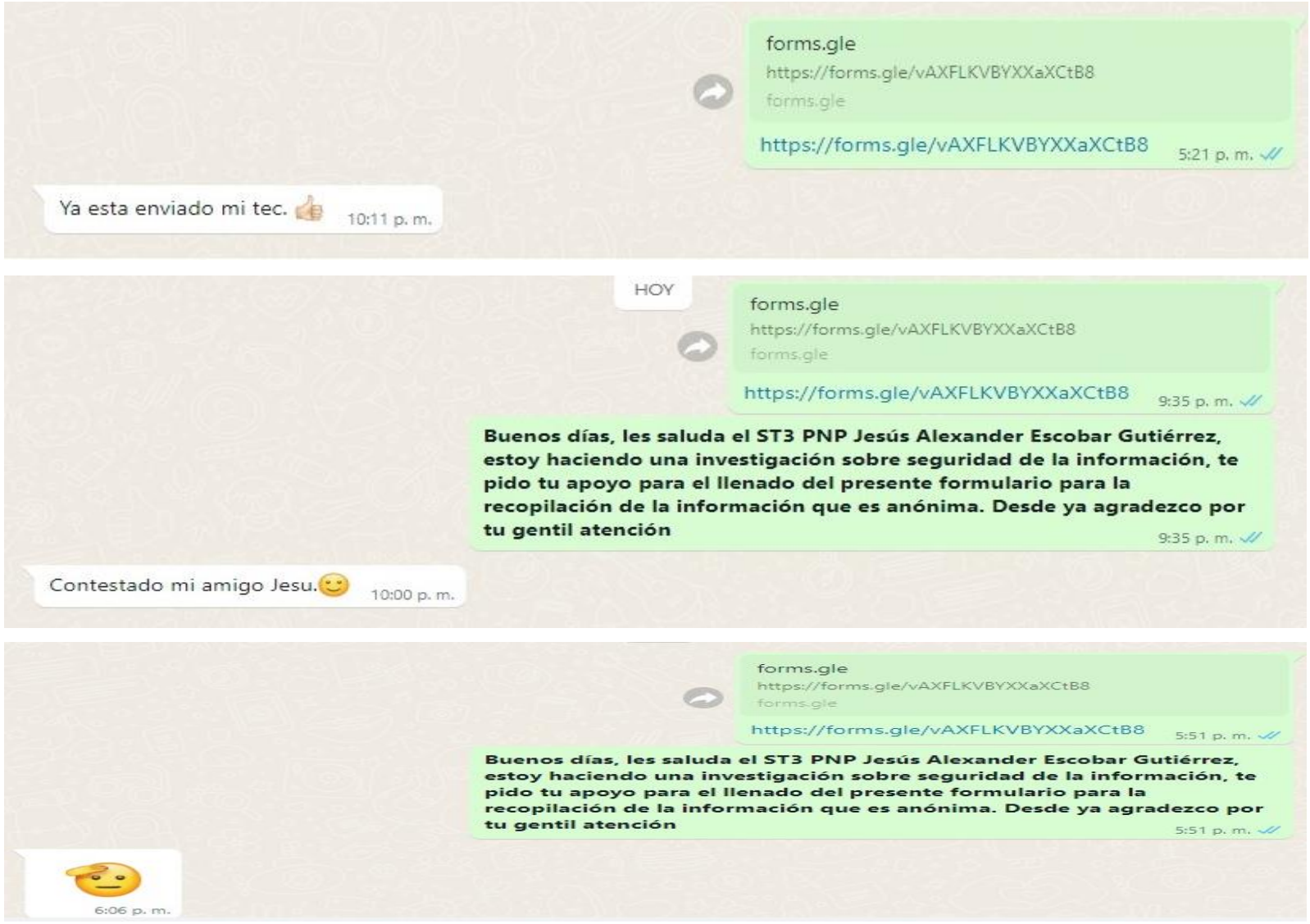
Anexo 9: Paneo fotográfico de llenado en oficinas y pedido vía WhatsApp del formulario.






Estrategia en Redes Sociales en la PNP
Policía Nacional del Perú
REDES SOCIALES
DEMOCRACIA DIGITAL


lenovo


forms.gle
https://forms.gle/vAXFLKVBYXXaXCtB8
forms.gle
https://forms.gle/vAXFLKVBYXXaXCtB8 5:21 p. m.
Ya esta enviado mi tec. 10:11 p. m.
HOY
forms.gle
https://forms.gle/vAXFLKVBYXXaXCtB8
forms.gle
https://forms.gle/vAXFLKVBYXXaXCtB8 9:35 p. m.
Buenos días, les saluda el ST3 PNP Jesús Alexander Escobar Gutiérrez, estoy haciendo una investigación sobre seguridad de la información, te pido tu apoyo para el llenado del presente formulario para la recopilación de la información que es anónima. Desde ya agradezco por tu gentil atención 9:35 p. m.
Contestado mi amigo Jesu. 10:00 p. m.
forms.gle
https://forms.gle/vAXFLKVBYXXaXCtB8
forms.gle
https://forms.gle/vAXFLKVBYXXaXCtB8 5:51 p. m.
Buenos días, les saluda el ST3 PNP Jesús Alexander Escobar Gutiérrez, estoy haciendo una investigación sobre seguridad de la información, te pido tu apoyo para el llenado del presente formulario para la recopilación de la información que es anónima. Desde ya agradezco por tu gentil atención 5:51 p. m.
6:06 p. m.

Buenos días, l...uda el ST3 PNP Jesús Alexander Escobar Gutiérrez, estoy hacien... investigación sobre seguridad de la información, te pido tu apoyo para el llenado del presente formulario para la recopilación de la información que es anónima. Desde ya agradezco por tu gentil atención 5:17 p. m.

HOY

5:18 p. m.

Implementación ISO 27001 para el Control de Delitos Informáticos en la División de Prensa DIRCII PNP, Lima, 2022

Se ha registrado tu respuesta.

Enviar otra respuesta

Este contenido no ha sido creado ni aprobado por Google. Notificar uso inadecuado · Términos del Servicio · Política de Privacidad

Google Formularios 5:24 p. m.

listo 5:24 p. m.

HOY

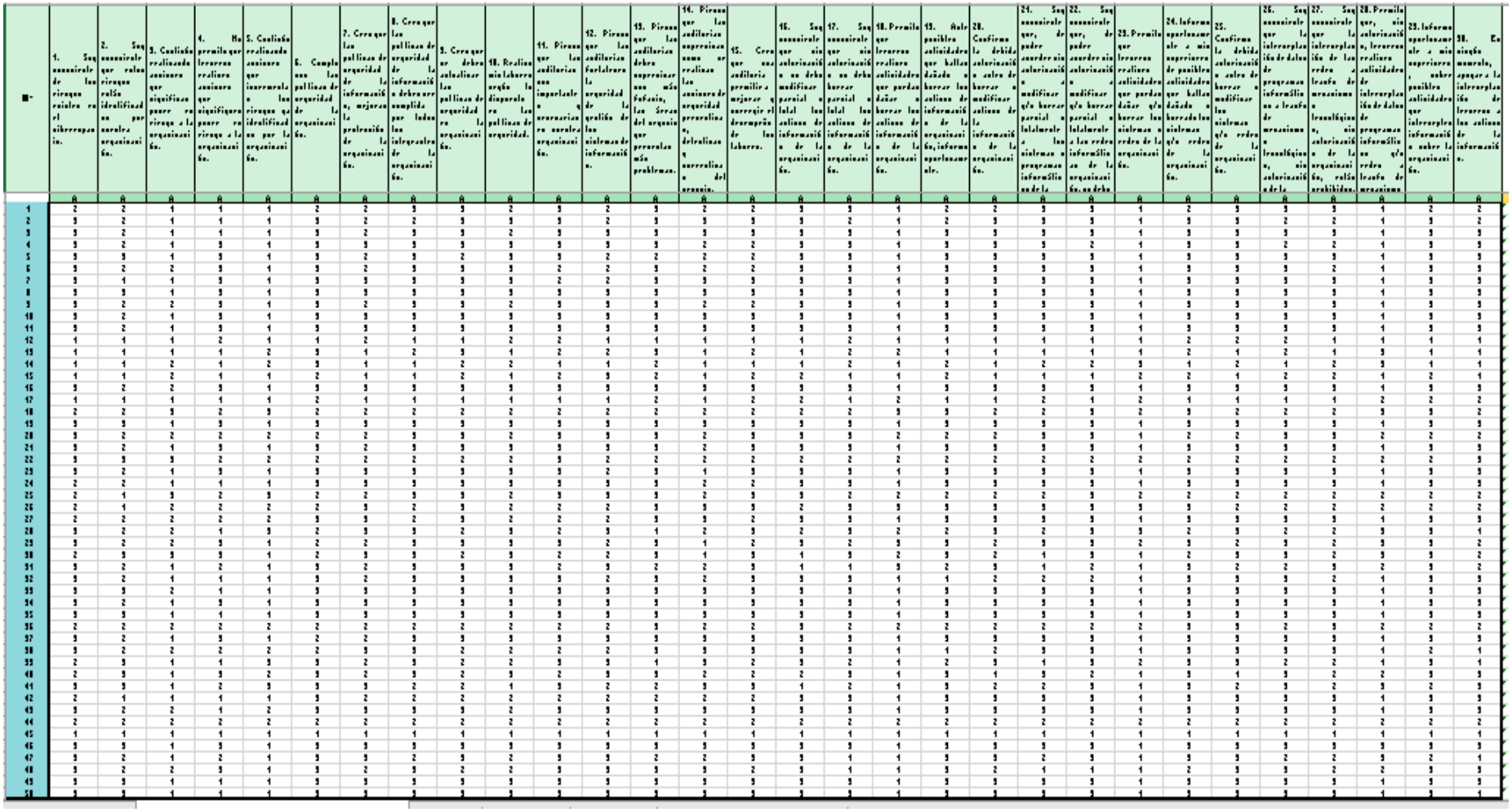
forms.gle
https://forms.gle/vAXFLKVBYXXaXCtB8
forms.gle

https://forms.gle/vAXFLKVBYXXaXCtB8 9:17 p. m.

Buenos días, les saluda el ST3 PNP Jesús Alexander Escobar Gutiérrez, estoy haciendo una investigación sobre seguridad de la información, te pido tu apoyo para el llenado del presente formulario para la recopilación de la información que es anónima. Desde ya agradezco por tu gentil atención 9:17 p. m.

Okidoki 9:18 p. m.

Anexo 10: Base de datos



Fuente: Elaboración propia (2022).

Anexo 11: Carta de Presentación por Destinatario

UNIVERSIDAD CÉSAR VALLEJO

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

Lima, 30 de junio de 2022
Carta P. 0607-2022-UCV-VA-EPG-F01/J

Coronel PNP
Vidarte Perrigo, Manuel Gustavo
Director
Dirección de Comunicación e Imagen Institucional de la Policía Nacional del Perú

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a ESCOBAR GUTIÉRREZ, JESÚS ALEXANDER; identificado con DNI N° 42234862 y con código de matrícula N° 7002617987; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

Implementación ISO 27001 para el Control de Delitos Informáticos en la División de Prensa DIRCII PNP, Lima, 2022.

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador ESCOBAR GUTIÉRREZ, JESÚS ALEXANDER asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

Dra. Estrella A. Esquiagola Aranda
Jefa
Escuela de Posgrado UCV
Filial Lima Campus Los Olivos

Somos la universidad de los que quieren salir adelante.

ucv.edu.pe

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, ACUÑA BENITES MARLON FRANK, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Implementación ISO 27001 para el Control de Delitos Informáticos en la División de Prensa DIRCII PNP, Lima, 2022", cuyo autor es ESCOBAR GUTIERREZ JESUS ALEXANDER, constato que la investigación tiene un índice de similitud de 16.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 18 de Octubre del 2022

Apellidos y Nombres del Asesor:	**Firma**
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 18-10-2022 16:25:10

Código documento Trilce: TRI - 0434996

INVESTIGA UCV