UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

ISO 27001 y gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Gil Miranda, Manuel Eleodoro (orcid.org/0000-0001-5088-7525)

ASESORES:

Mg. Poletti Gaitan, Eduardo Humberto (orcid.org/0000-0002-2143-4444)

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

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2024

DEDICATORIA

A mi hija Amira Tiaret, motor y motivo de mi progreso profesional, además de ser la brújula que orienta mi sendero personal. A mí mismo, sobre todo a aquel Manuel Gil Miranda del año 2020, por mantener la fé, desarrollar mucha paciencia, aprendí a quererme y todo fue para mejor.

AGRADECIMIENTO

Expreso mi gratitud hacia los maestros de la Universidad César Vallejo quienes brindaron apoyo, entendimiento y experiencia para el desarrollo y culminación de la Maestría. A Dios, por enseñarme que la paz, tranquilidad y el amor propio son las mayores riquezas de un ser humano con los cuales se puede ser feliz.

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, POLETTI GAITAN EDUARDO HUMBERTO, 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: "ISO 27001 y gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023", cuyo autor es GIL MIRANDA MANUEL ELEODORO, constato que la investigación tiene un índice de similitud de 11.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reppрte 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, 04 de Enero del 2024

Apellidos y Nombres del Asesor:	**Firma**
POLETTI GAITAN EDUARDO HUMBERTO **DNI:** 18073124 **ORCID:** 0000-0002-2143-4444	Firmado electrónicamente por: EPOLETTIG el 07-01-2024 17:24:57

Código documento Trilce: TRI - 0719725

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Originalidad del Autor

Yo, GIL MIRANDA MANUEL ELEODORO estudiante de la ESCUELA DE POSGRADO del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "ISO 27001 y gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

Nombres y Apellidos	Firma
GIL MIRANDA MANUEL ELEODORO **DNI:** 43692241 **ORCID:** 0000-0001-5088-7525	Firmado electrónicamente por: MGILMIR el 08-01-2024 08:42:42

Código documento Trilce: INV - 1445636

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS Y FIGURAS

RESUMEN

El objetivo de la presente investigación determinó la incidencia de la ISO 27001 en la gestión de vulnerabilidades de los activos informáticos del centro de datos de entidad pública geocientifica. El estudio fue de tipo aplicada, enfoque cuantitativo, y el diseño fue no experimental transversal descriptivo y correlacional, dónde la población era de 107 activos informáticos y la muestra de 86, por intermedio del muestreo aleatorio simple, aplicándose el instrumento Ficha de datos y como técnica el análisis documental. El instrumento fue altamente confiable, realizándose el test de confiabilidad Alfa de Cronbach obteniendo el resultado de 0.945. La muestra es mayor que 50, utilizando para normalidad de datos el método Kolmogórov-Smirnov, y sobre análisis paramétrico el coeficiente de correlación de Spearman, logrando comprobar la hipótesis y concluyendo que la ISO 27001 tiene un impacto considerable en gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad geocientifica pública, Lima 2023.

Palabras Clave: Gestión de vulnerabilidades, ISO 27001, seguridad digital, ciberseguridad, seguridad de la información.

ABSTRACT

The objective of this research determined the impact of ISO 27001 on the management of vulnerabilities of the computer assets of the data center of a public geoscientific entity. The study was of an applied type, quantitative approach, and the design was non-experimental cross-sectional descriptive and correlational, where the population was 107 computer assets and the sample were 86, through simple random sampling, applying the Data Sheet instrument and as documentary analysis technique. The instrument was highly reliable, with the Cronbach's Alpha reliability test obtaining a value of 0.945. The sample is greater than 50, using the Kolmogórov-Smirnov method for data normality, and on parametric analysis the Spearman correlation coefficient, managing to verify the hypothesis and concluding that ISO 27001 has a considerable impact on vulnerability management in computer assets. from the data center of a public geoscientific entity, Lima 2023.

Keywords: Management of vulnerabilities, ISO 27001, digital security, cybersecurity, information security

I. INTRODUCCIÓN

Las empresas u organizaciones han incorporado tecnologías y/o servicios digitales en sus actividades operativas, por lo que se hallan en fase de consumación de Transformación Digital, lo cual les permite ofrecer un excelente servicio a sus clientes. La digitalización en los procesos implica que sea primordial preservar el activo más valioso que son los datos o información, también los sistemas informáticos de posibles amenazas, en un marco total de confianza digital. Sin embargo, también existe un elevado índice de empresas que presentan exposiciones y vulnerabilidades, permitiendo que sus principales activos informáticos posean riesgo de ser infectados ya sea por software malicioso o secuestrados por algún tipo de ransomware, entre otros casos, por lo tanto, con tanta información ahora en formato digital la salvaguardia de los datos se ha transformado en un inconveniente que ninguna entidad puede permitirse ignorar.

En Colombia desde la perspectiva de Martelo (2018), señala que las organizaciones se encuentran con la necesidad de mantener sus servicios de tecnologías para garantizar a sus usuarios finales el acceso y disponibilidad, es así que la escasez de directrices de seguridad de datos es la principal dificultad identificada, lo cual ocasiona en reiteradas veces la vulneración de los datos que almacenan.

En este sentido Hernández (2019), afirma que las compañías de México, afrontan una nueva particularidad para ofertar sus servicios y por consiguiente requieren soporte especializado para la adopción de nuevas tecnologías de información, siendo un elemento clave la implantación de estándares internacionales o normas ISO que ayuden a fortalecer su seguridad como ISO 27001, que muestra el camino que deben transitar las compañías para brindar servicios seguros.

En el caso de Perú, Rodríguez (2020), hace hincapié en que se han incrementado las brechas tecnológicas que tienen las corporaciones del país y principalmente en el sector público, debido a que las entidades públicas no priorizan la mejora de sus procesos a través de la innovación tecnológica, demostrando en muchos casos el deterioro de un diseño de conectividad seguro, confiable, falta de diagramas de red de conexión e interconexión, falta de protocolos seguros.

Como estudio de investigación local, según Bustamante et al. (2021), menciona que en los municipios generan una gran cantidad de vulnerabilidades debido a la descarga y despliegue de software no autorizado, que a su vez generan riesgos de perdida de información, siendo estrictamente requerido implantar una política de gestión de vulnerabilidades técnicas.

En esta tesis se realizó la valorización y gestión de las vulnerabilidades en los activos informáticos ubicados en el Centro de Datos de una entidad pública geocientífica; siendo las vulnerabilidades aquellas debilidades en el diseño, fallas de hardware, fallas en el software, fallas a nivel de recursos humanos y/o procedimientos inclusive; otras vulnerabilidades frecuentes pueden ser: errores de configuración, errores en la gestión de recursos, validación de entrada, saltos de directorios compartidos, privilegios y/o control de accesos no definidos de manera correcta, actualización de seguridad, faltan acciones e intervenciones de seguridad.

Desde el año 2018, con la creación de la Ley de Gobierno Digital, se están implementando distintas normativas relacionadas que otorgan un marco de trabajo que se usa para la implantación, mantenimiento y progreso constante de la protección de datos. Según Artículo 115, DS N.º 029-2021-PCM. Pruebas para evaluar vulnerabilidades; el cual indica que cada 12 meses, toda entidad pública debe planificar y realizar ensayos para valorar las vulnerabilidades que se pueden identificar de los activos de información tales como: aplicaciones informáticas, plataformas informáticas, infraestructura tecnológica y redes de datos, que a su vez soportan los principales procesos de negocio, procesos estratégicos y/o de soporte.

La justificación práctica está sustentada, debido a que la gestión de vulnerabilidades permite verificar y mejorar la efectividad de las actividades preventivas que serán adoptadas, permitiendo la identificación, detección y corrección de debilidades de activos informáticos, otorgando confiabilidad y disponibilidad de datos de la entidad geocientífica pública. La justificación metodológica, es aquella que se tiene al desarrollar el instrumento que permite analizar y relacionar directamente las variables y los datos que se obtengan. Posteriormente, se encuentra incluida dentro del desarrollo de la justificación teórica, debido a su aporte al conocimiento a través de conclusiones que serán relevantes para la entidad pública geocientífica y que puedan ser parte de otros

estudios como referencia para seguir analizando y ahondando acerca del tratamiento de vulnerabilidades técnicas que se identifiquen para ser mitigados.

Luego de sostener como fundamentos la situación problemática que ha sido detallada, se plantearon los problemas generales y específicos de la presente exploración. Asimismo, el problema general fue: ¿La ISO 27001 impacta en la gestión de vulnerabilidades en activos informáticos del centro de datos de la entidad pública, Lima 2023?; Siendo problemas específicos los siguientes: ¿La ISO 27001 impacta en la identificación de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientífica, Lima 2023?;¿La ISO 27001 impacta en la detección de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientífica, Lima 2023?; ¿La ISO 27001 impacta en la corrección de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientífica, Lima 2023?.

Objetivo general fue: Establecer cómo ISO 27001 impacta en la gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica. Como objetivos específicos: Establecer cómo ISO 27001 impacta en la identificación de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientífica, Lima 2023; Determinar cómo la ISO 27001 impacta en la detección de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientífica, Lima 2023; Determinar cómo ISO 27001 impacta sobre la corrección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.

Hipótesis general fue: La ISO 27001 impacta considerablemente en la gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica. Las Hipótesis definidas fueron: La ISO 27001 impacta considerablemente en la identificación de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023; La ISO 27001 impacta considerablemente en la detección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023; La ISO 27001 impacta considerablemente en la corrección de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientífica, Lima 2023.

II. MARCO TEÓRICO

Según Díaz (2021), cita investigaciones anteriores a nivel nacional como evidencia de que este estudio analiza cómo las agencias gubernamentales peruanas han incorporado la norma ISO 27001:2014. El problema son los ataques informáticos cada vez más sofisticados. Se encuestó a una muestra de 76 servidores públicos utilizando una metodología cuantitativa y se descubrió que aproximadamente el 50% de ellos pensaba que la norma estaba incluida. A menudo las amenazas evolucionan y son más rebuscadas, este estudio enfatiza el valor de la ciberseguridad para las organizaciones.

Asimismo, según Vega et al. (2022) prioriza la seguridad como un concepto amplio de la Norma ISO 27001:2013. Se puede perder información si no se establece adecuadamente una gestión de la seguridad en los casos en que hay ataques cibernéticos o incluso durante investigaciones virtuales. El 59,1 por ciento de quienes intentaron el método Prisma lo terminaron con éxito. El análisis de qué controles cumple la información, cuáles no cumple y en definitiva qué tan segura es, nos permite determinar si la información es segura.

De acuerdo con Bustamante et al (2021), la adopción de directrices respaldado por estándares ISO prospera enormemente la gestión del aseguramiento digital cuando es necesario regular los procesos seguros e íntegros. Siendo la finalidad de la investigación evitar las deficiencias mecanisticas. Esta es una herramienta de observación y entrevista. Hay noventa trabajadores en total. El porcentaje que se obtiene es del 90%. En última instancia, esta investigación mejora eficazmente la gestión de la ciberseguridad al concentrarse en los elementos esenciales de disponibilidad, integridad y preservación.

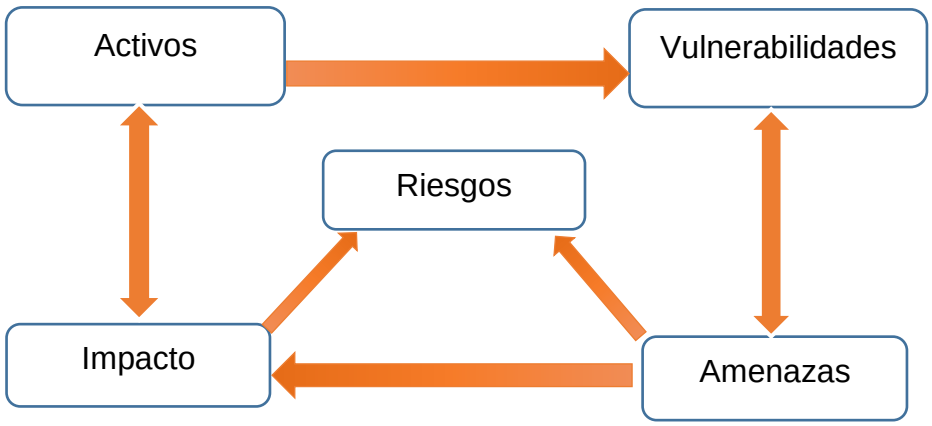
Como resultado del incremento de hackers astutos y usuarios considerados de alta exposición, Atencio (2019) afirma que existen riesgos y amenazas a la información de las instituciones. Estos factores influyen en la facilidad con la que se puede realizar la transferencia directa de datos a través de una red informática. Las metodologías empleadas fueron transversales y descriptivas. Se utilizó el registro de observación. 50 instituciones al servicio del público en general. El resultado es del 90%. Encontrar los mejores servicios de seguridad resultó ser sólo una parte de la respuesta al problema de la ciberinseguridad.

También según García et al. (2018), indica que las empresas están integrando cada vez más sistemas de información. El costo del impacto del riesgo ha aumentado por el como resultado de una deficiente gestión de la vulnerabilidad. Acertar una solución viable a una difícil gestión de TI requiere un proceso formal de diseño y valoración que garantice resolución. Tiene un enfoque cualitativo que se apoya en los procedimientos de evaluación y asocia datos utilizadas en dicho estudio. Una valoración de un suceso de una pyme de arcilla y/o cerámica utilizando el modelo da como resultado un nivel de riesgo de aproximadamente un 53 por ciento menor. Por último, pero no menos importante, se comprobó que el modelo es sencillo de usar y facilita la identificación del cuadro necesario para reducir el peligro, en la cual implementación es relevante.

Adicionalmente, Niño (2018) señala la existencia de un problema ya que las aplicaciones informáticas son vulnerables a amenazas y peligros tanto del interior como del exterior. La data se estima como un recurso importante para el funcionamiento eficiente de una estructura organizacional. 60 usuarios completan una encuesta con el fin de recolectar datos, bajo un enfoque detallado y transversal de la investigación. Se encontró que el 64 por ciento de usuarios estaban involucrados. Se ubico un alto nivel de acuerdo a la hora de establecer protocolos para aminorar la huella y asegurar la continuidad en materia de seguridad de activos vitales.

Figura 1

Relación activos, amenazas, vulnerabilidad, riesgo



Fuente: Elaborado por Manuel Gil Miranda (2023).

Por otro lado, según Rincón (2019), informa que su investigación principal se enfoca en auditoría y desarrollo de ISO 27001 en un centro de estudios universitario. Algunas de las fases metodológicas que se emplean a manera de resultado del contexto actual, la identificación de peligros, el acoger medidas de defensa y la realización de exploraciones internas y del exterior. Los hallazgos expusieron que había 28 peligros, se implementaron 51 controles de protección y hubo altas tasas de cumplimiento del 95% para las revisiones internas y externas. En última instancia, la organización pudo crear un marco más sólido para el manejo de riesgos y la ciberseguridad.

Además, los antecedentes internacionales de Mohammed & Jasim (2022) abordan los problemas del régimen de estado con la averiguación entendida de la entidad de investigación petrolera iraquí y cómo mejorar la ciberseguridad de la sociedad en su contexto. La acumulación de datos utilizó una pesquisa debido a su metodología cualitativa. El estudio examinó 321 empresas de exploración petrolera en Irak. El 64 por ciento es el resultado. A la luz de la comparación de considerar medidas para preservar la entereza de los datos corporativos, se concluye que es necesario optimizar la gobernanza de datos que registra la empresa.

Según Ferreira (2018), indica que la investigación examina la importancia de comprender e implementar en el desarrollo efectivo de la administración de seguridad. El objetivo es identificar las variables involucradas de los agentes gubernamentales que forman parte de la tecnología de la Fuerza aérea de Brasil, en la cual comprenden las prácticas de gestión de ciberseguridad. Se emplean métodos cuantitativos, exploratorios y descriptivos. La población fue de 256 empleados. El 78,3% de las personas estuvo de acuerdo con el resultado. El estudio llegó a la conclusión de que las percepciones sobre la perspicacia y acogida de destrezas de gestión segura son fundamentales.

Para Hannigan et al (2019), el objeto es optimizar la gestión en Qatar Biobank (QBB) mediante la implementación de un método de gestión que integre y complemente las normas ISO de Calidad y de Seguridad, respectivamente. Dado que se empleó una encuesta para recopilar datos, el estudio es de naturaleza cuantitativa. Se conto con 145 participantes para el estudio. En la cual se consiguió el 95 por ciento de los resultados. En resumen, la misión de la estructura se ha visto potenciada por la unificación del sistema de gestión en QBB, conjuntando las

normas anteriormente señaladas. Esto ha tenido un efecto positivo en la experiencia del usuario y en los frutos de las evaluaciones al interior.

Según Chen et al. (2022), el valor del proceder de seguridad informática de los colaboradores se incrementa. Se reunieron datos de 217 empleados de tres compañías de nacionalidad china utilizando un método de campo cuasiexperimental empleado en el estudio. Se utilizaron cuestionarios de medición del estrés. El resultado es del 58 por ciento como porcentaje. En resumen, este estudio contribuye a nuestra comprensión sobre cómo gestionar eficazmente la tensión en el marco de la ciberdefensa y el cumplimiento positivo del concepto de seguridad.

En ese sentido, según Bai (2022), el desarrollo tecnológico de big data ha creado nuevas amenazas para la seguridad informática, lo que supone un reto los profesionales de TI. El problema está en la precisión de implementar mecanismos operativos y comprobar en línea, para así poder tener confidencialidad en la información digital. El cuestionario es el método empleado y el enfoque es cuantitativo. Allí vivían 80 personas. El 64 por ciento es el resultado final. La importancia de abordar la seguridad informática para TI se destaca en la conclusión, como sugerencia hacer uso de manera integrada de plataformas informáticas y emplear la normativa de seguridad informática.

Para Zhao et al (2019), las carencias en ciberseguridad de espacios de recreación inteligentes han incluido, entre otras cosas, una forma confusa de accesibilidad, siendo una falta de gestión de accesos, datos desorganizados y una recopilación deficiente de evidencia de evaluaciones. La metodología utilizada en su estudio cuantitativo es la observación. Había 125 residentes. Las secuelas finales son del 94%. Se afirma que el tratamiento de problemas relacionados a seguridad informática en espacios recreacionales inteligentes, abordan una gestión precisa de la tendencia de las personas que se va incrementando.

En palabras de Chen et al (2021), los avances en el análisis sobre la distribución y dimensión de los aplicativos de salud, todavía existe una falta de integración entre ellos, lo que dificulta el movimiento de los registros, recopilación de información y médicos. Cuando se estudia un sistema de información de salud centralizado con directrices de privacidad y seguridad se presenta una situación

problemática. La metodología utilizada fue un enfoque cuantitativo. Tenía 365 habitantes. El 75% de los resultados son en porcentaje. Se ha destapado que la integración de registros electrónicos incrementa la prestación de servicios de salud.

Según Monev (2020), asegura que existe ausencia de métodos de evaluación de un modelo maduro de seguridad de datos. Se aconseja el uso de una metodología similar que sea útil. La metodología emplea un instrumento para comprobar el vencimiento de disposiciones y cláusulas. 140 profesionales es el total de la muestra. Da como consecuencia un porcentaje de madurez (escalado 0 a 5) del 56,6%. Da como fin una forma viable de desarrollar el análisis de madurez del sistema de seguridad basado en estándar 27002.

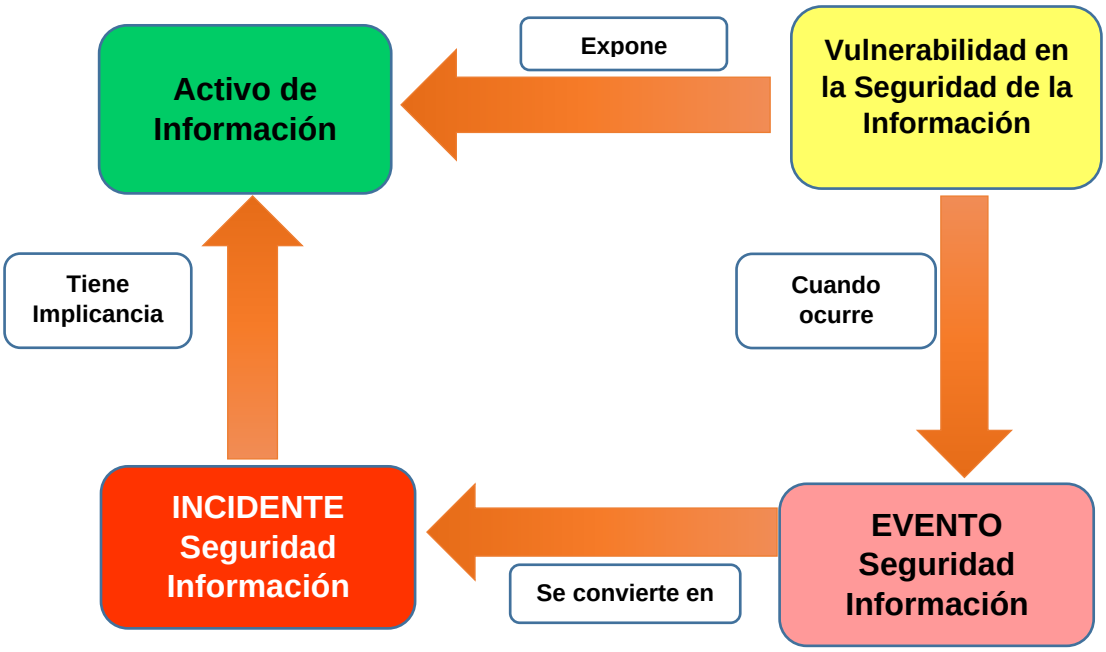
Según lo indicado por Velasco et al (2018), el sector manufacturero, la abundancia de datos y la laxa seguridad en fichas de procesos cruciales necesita identificar los peligros para la eficacia del negocio. El estudio se centra en las metodologías de gestión de riesgos (Magerit) y PDCA Deming. En Ecuador viven 105 personas, e Imptek-Chova es el principal fabricante de techos para jardín del país. Para manejar los riesgos se recomienda utilizar técnicas como el ciclo PDCA y Magerit II, y se concluye que se debe implementar un SGSI en el sector manufacturero.

Según el estudio Maingak et al. (2018) revela la problemática que existe excavando los procedimientos comerciales que la compañía requiere, por lo tanto, necesita un enfoque cuantitativo. Se emplea el proceso de observación. Hay 174 personas en la población. El 43,86 por ciento de los resultados son porcentajes. En resumen, ISO/IEC 27001 existe como instrumento muy eficiente de control y protección de la información.

Según Agustino (2018), se agrupan discrepancias sobre la salvaguardia de datos proporcionada por una entidad pública señalada y las condiciones de ISO 27001. Esa investigación es cuantitativa. Sólo 64 controles, o el 56,14 por ciento de los 114 controles de la población, fueron realmente desarrollados por la entidad gubernamental. Los hallazgos del estudio respaldan la confirmación de que la organización gubernamental bajo evaluación no procede con los requisitos necesarios según lo enmarcado en la norma en materia de seguridad.

Figura 2

Flujo de Vulnerabilidad en Seguridad Informática



Fuente: Elaborado por Manuel Gil Miranda (2023).

Asimismo, Thoyyibah (2018) aconseja que, particularmente en digitalización de procesos, la seguridad informática es fundamental para mantener viable y disponible la capacidad de una organización y su continuidad operativa ya que las deficiencias existentes utilizan enfoques prácticos para la ciberseguridad. Es correlacional en este estudio. Las encuestas se utilizan para recopilar datos. Diez personas constituyeron la población de estudio. El resultado es del 35% como porcentaje. Según los resultados del estudio, es necesario mejorar el SGSI.

También Lopes et al. (2019), concluye que el desafío fue estimar la clasificación del modelo de ciberseguridad para los sistemas y/o aplicaciones del tipo académica de una universidad en Indonesia. Método de evaluación Para realizar el estudio se utilizó la herramienta Indeks KAMI. Se empleó cuestionarios y entrevistas al personal para recopilar los datos. 577 personas participaron en el estudio. Se determina que las aplicaciones académicas del ente evaluado cumplen con requisitos de seguridad, y se concluye que para ellos se requiere documentación clara, exámenes continuos y un seguimiento estrecho.

Según lo afirmado por Kim y Kim (2021) se examina elementos que influyen en la finalidad y desarrollo de los SGSI en las empresas. Las respuestas de los

trabajadores se recopilaron utilizando un formulario virtual y el modelo TOE del estudio. Había 107 trabajadores en total. 58 por ciento como porcentaje. Los hallazgos del estudio respaldan el papel fundamental del SGSI a la hora de promover el negocio.

Para Jelovčan et al. (2022) indica que la decisión de gestionar al interno o subcontratar los servicios gestionados de seguridad informática fue un tema que este estudio intentó plantear. En la investigación se empleó el análisis jerárquico. También se recolecto información a través de una encuesta en línea. Hubo 37 profesionales en la población de estudio. 43 por ciento es el resultado como porcentaje. Se determinó que la herramienta de análisis jerárquico tuvo éxito al ayudar a las organizaciones a decidir si administrar los servicios de seguridad de la información tanto interna como externa.

También Yang & Wang (2022) el principal problema es la ciberseguridad de los estudiantes, y el SGSI para estudiantes debe actualizarse con tecnologías veraz de seguridad de datos. La estrategia es cuantitativa. Los datos de la encuesta se recopilaron utilizando la herramienta. Para ambas pruebas de seguridad, la población fue un modelo de datos académico típico. Alcanzar un porcentaje del 87 por ciento. Según los hallazgos del estudio, la tecnología blockchain puede ayudar a sistemas similares con la seguridad de los datos y adquiere una marca positiva en el SGSI de alumnos.

Figura 3

Relación entre amenaza y vulnerabilidad en un servidor de base datos

Fuente: Elaborado por Manuel Gil Miranda (2023).

Como indica Bertalanffy (1976) afirma que la teoría sistémica en su conjunto es la perspectiva principal para proporcionar el marco conceptual para comprender

sistemas complejos en diversos campos. El principio principal de la teoría es que los sistemas son entidades intrincadamente entrelazadas y mutuamente dependientes que trabajan juntas para lograr objetivos comunes. La conjetura se centra en modelos y nuevas tendencias de conocimientos que se originan de la interrelación entre los componentes del sistema en vez de examinar cada componente por separado. Se ha convertido en una técnica esencial para el pensamiento sistémico y el manejo de sistemas de alta complejidad.

Según Shannon & Weaver (1964), el enfoque de información es incluir el desarrollo de un argumento matemático riguroso que permite su uso para explicar cualquier otro tipo de datos. Crear un diseño de comunicación formal que cuantifique la indagación y la técnica de un conducto comunicativo que lo transmita hasta lograrlo. Además, posee un impacto específico acerca de la teoría de la complejidad, la informática y la ingeniería de la comunicación, este método estableció los cimientos básicos de la conjetura contemporánea. La solución comunicacional se puede representar figuradamente.

En cuanto a teoría general se ha considerado a la Seguridad informática, de acuerdo a Figueroa et al. (2018), afirma del camino de inalterabilidad es garantizar y proteger la data tanto de riesgos como amenazas. Siendo su principal meta es proteger el acceso y la privacidad de data. Esto se obtiene mediante la aplicación normativa y regla de éticas que establecen precauciones de seguridad oportunas.

La teoría específica considerada fue: Análisis de Riesgos, Estándares ISO, según Bailon (2019) la teoría específica para este estudio que han sido consideradas fue gestión de riesgos, estándares internacionales como ISO, que relaciona el análisis de peligros y amenazas cuyo objetivo es reducir posibilidad de ocurrencia de incidentes desfavorables, por medio de la exploración, evaluación, remediación y seguimiento de peligros.

Según Vela et al. (2019) habla acerca de las ISO, que son la base tecnológica y también menciona los servicios de TI, contienen aspectos como el contexto, delimitación, publico de interés, plan de comunicación, entre otros. Por lo tanto, es coherente afirmar que sumamente relevante la ejecución en entidades enfocadas en TIC’s.

Se establece que la investigación de divide en 4 categorías: planeamiento, implantación, revisión y seguimiento. Por ello, es muy crucial implementarlo en empresas orientadas a TI. El planeamiento comprender y abordar diversos elementos organizacionales, como limitar la importancia del SGSI, dividir roles y responsabilidades en ciberseguridad, así como generar una política de riesgos, revisar los protocolos y reestructurar organizacionalmente. Sin embargo, la etapa de aplicación está enfocada principalmente en actividades de análisis de vulnerabilidades y/o debilidades. Igualmente, con la ISO 27001, se obtiene un mejor control de activos en materia seguridad tecnológica. Por lo que, es constantemente necesario validar cada componente y así poder asegurar la ciberseguridad (Cardona y Restrepo, 2020). Para terminar, el seguimiento se refiere a los requisitos mínimos que deben ser acordados para innovar. Concluyendo que es primordial remediar insuficiencias y mejorar constantemente para oportuno crecimiento (Córdova, 2021).

Los análisis incluyen identificación, detección y corrección. La accesibilidad hace referencia a la capacidad de un recurso para aprobar a las personas que están acreditadas y son capaces de administrar la información. El personal designado debe recibir la capacitación necesaria para prevenir fallas físicas. La flexibilidad, por su parte, se relaciona con la capacidad de incluir información en nuevas alternativas y brindar un lugar adecuado para su almacenamiento, afirmando su defensa frente a las amenazas (Mejía, 2020).

Flores (2018), presentó una propuesta para crear almacén de datos corporativo relacionado a la investigación en Apurímac, fundamentada en metodologías científicas, por lo que su finalidad fue el análisis e identificación de las vulnerabilidades del dispositivo para así luego desarrollar tecnologías que permita solucionar los problemas corporativos. En la propuesta, basada en métodos cuantitativos, presenta los resultados numéricos de los resultados de la investigación, logra sacar conclusiones: Propuestas técnicas y económicas para la introducción de redes de datos y centros de datos debido a la necesidad de disponer de todo el equipamiento necesario para crear redes de datos mediante cables estructurados y centros de datos.

Gil y Maihuiri (2018), realizaron el análisis de Centro de procesamiento de data en lima, teniendo como finalidad conocer el contexto y a través de la

problemática proponer una solución tecnológica que permita reconducir la situación adversa, concluyendo que se encuentra en Desacuerdo, el agrado de los trabajadores de Venus Peruana S.A.C. También se concluye que más de 52 personas indican que se encuentran Muy de acuerdo y están satisfechos con la situación actual corporativa.

Esta fase investigativa está basada en estudios similares a nivel mundial y muestra el fundamento requerido del estudio, según lo siguiente: La característica de disponibilidad básica o extrema (alta disponibilidad) es un atributo de un activo informático y garantiza la continuidad operativa en un determinado plazo.

El plazo de Disponibilidad es la característica que los consumidores puedan acceder al sistema, y realizar sus actividades tales como: la publicación de nuevos trabajos, modificar trabajos actuales o recolectar trabajos anteriores, sin interrupciones. La disponibilidad y la energía son variables asociadas al centro de cómputo y comunicaciones, que son necesarios para el diseño o modificación de sus componentes electromecánicos. (Vargas, 2020).

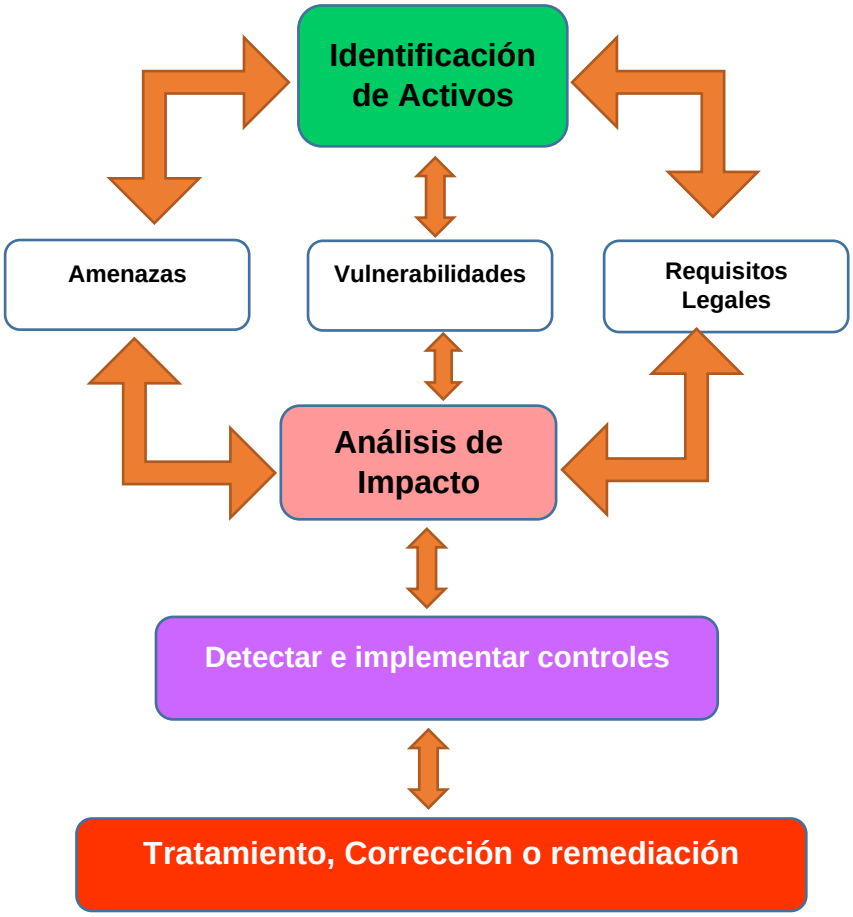
Los escenarios de riesgos de desastres son imprevisibles, por lo que es necesario tener una política de buenas prácticas en materia de redundancia, es decir que un activo tecnológico debe tener la posibilidad de seguir operando aun cuando alguno de sus componentes falle. Esto es comúnmente conocido como Tolerancia a fallas y en algunos casos como Servicio de protección contra fallas (FOS).

En esta fase se muestran los lineamientos sobre la variable, indicando lo siguiente: Según la ISO 27001, Seguridad de información, previene sobre amplio repertorio de peligros y amenazas hacia la información, si desea garantizar la continuidad operativa empresarial, así como evitar posibles daños. Del mismo modo, tiene en cuenta la existencia de hechos en una variedad de formas, incluidos aquellos que se publican o escriben en papel, se recopilan electrónicamente, se transmiten por medios electrónicos, se presentan en instantáneas o se muestran en comunicaciones. Para tener los tres pilares de la seguridad, las estadísticas, independientemente de su forma o los métodos utilizados para distribuirlas o centralizarlas (almacenarlas), siempre deben estar adecuadamente protegidas. Además, se debe utilizar, documentar y reconocer consistentemente un enfoque

de riesgo empresarial en toda la organización para que la seguridad de los registros se administre de manera efectiva. Un SGSI consiste en algo como esto.

Figura 4.

Proceso de Gestión de vulnerabilidades



Fuente: Elaborado por Manuel Gil Miranda (2023).

Clasificar vulnerabilidades mediante el Sistema de puntuación común (CVSS), es el marco de trabajo general que define los indicadores para conectar los atributos y severidad que afecten los componentes del ecosistema de seguridad TI. El organismo titular es el FIRST (Forum of Incident Response and Security), el cual cuenta con la modernización de la versión 3.0 de CVSS.

El FIRST desarrollo durante años la optimización del sistema CVSS hasta conseguir un borrador a fines de 2014, publicando la versión definitiva en junio de 2015. La versión 3.0 el sistema se aplica en nuevos entornos y remedia amenazas actuales.

El sistema de puntuación está compuesto de tres agrupaciones de indicadores: Base, Temporales y de Entorno (Environmental). Cada grupo se subdivide en subconjuntos medibles.

Conjunto Base: Abarca cualidades impliciticas de vulnerabilidades, siendo estas autónomas en tiempo y hábitat.

Temporal: Rasgos de vulnerabilidades modificables en el tiempo

Ambiental: Características de las vulnerabilidades relacionadas con el contexto del usuario.

Tabla 1

Métricas y valores CVSS según versión 2

CONJUNTO MÉTRICAS O INDICADORES	INDICADOR: (VALOR)
BASE	• Vector Acceso (AV): Valores: [L, A, N] (localizado, Contiguo, Red) • Complejidad de Acceso (AC): Valores: [H, M, L] (Alto, Medio, Bajo) • Autenticación (Au): Valores [M, S, N] (Múltiples, Único, Ninguno) • Impacto de la confidencialidad (C): Valores [N, P, C] (Ninguno, Parcial, Completo) • Impacto de Integridad (I): Valores [N, P, C] (Ninguno, Parcial, Completo) • Impacto en la disponibilidad (D): Valores [N, P, C] (Ninguno, Parcial, Completo)
TEMPORAL	• Explotabilidad (E): [U, POC, F, H, ND] (Sin probar, Prueba de concepto, Explotación funcional, Alto, No definido) • Nivel de Remediación (RL): [OF, TF, W, U, ND] (Solución oficial, Solución paliativa, Alternativa de Solución, No disponible, No determinado) • Informe de confianza (RC): Valores [UC, UR, C, ND] (No confirmado, No corroborado, Confirmado, No definido)
AMBIENTAL	• Potencial daño colateral (CDP): [N, L, LM, MH, H, ND] (Ninguno, Bajo, Bajo Medio, Medio Alto, Alto, No definido) • Distribución objetivo (TD): [N, L, M, H, ND] (Ninguno, Bajo, Medio, Alto, No definido) • Requisitos de Seguridad (CR, IR, AR): [L, M, H, ND] (Bajo, Medio, Alto, No definido)

Nota: Elaborado por Manuel Gil Miranda (2023).

Estos valores permiten determinar los criterios cualitativos de clasificación.

III. METODOLOGÍA

3.1 Tipo y Diseño de investigación

3.1.1 Tipo de investigación

Esta exploración fue en forma aplicada, toda vez que se realizaron indagaciones y la correspondiente recolección de datos, que sirvieron para sustentarlo, filtrando datos relevantes y a su vez se planteará la problemática que debe ser analizada (Cabezas, 2018).

Por lo indicado tendrá enfoque cuantitativo, toda vez que abordan datos numéricos con el objetivo de absolver las interrogantes para todos los objetivos propuestos (Cohen y Gómez, 2019).

3.1.2 Diseño de la investigación

Es de carácter no experimental, puesto que no existirá maniobra de variables, adicionalmente es correlacional toda vez que se realizará en un instante dado, según Ordoñez et al. (2018).

3.2 Variables y operacionalización

Variable independiente

ISO 27001

Definición conceptual

Velar por confidencialidad, disponibilidad e integridad de data, argumentando que implementando SGSI, permite el encargo de eventualidades, así como controlar la pertenencia de datos de la compañía, y su capacidad competitiva de dirigir y monitorear los procesos (Gil y Gil, 2017).

Definición operacional

Se aplican conceptos vinculados para administrar los activos informáticos que se manejan dentro de la entidad, para ello se analizará mediante un instrumento que mida su alcance y utilidad.

Para un SGSI, se debe tener un procedimiento de mitigación de riesgos en activos informáticos, así como establecer medidas de control. (ISOTools, 2019). Se

consideran como dimensiones de SGSI a la Dimensión 1: Confidencialidad, atributo indicativo que el activo se encuentre o no habilitado, no sea reconocida por terceros o agentes sin permiso. Dimensión 2: Integridad, indica que el activo no fue alterado o modificado indebidamente. Dimensión 3: Disponibilidad, es decía que se encuentre utilizable cuando se requiera (Córdoba, 2021).

Indicadores

Los indicadores de los activos informáticos, según las dimensiones son los atributos respecto a su confidencialidad, es decir si es de Acceso Libre, restringido o protegido, así como los atributos o características de integridad, para lo cual es necesario definir si es exacto, fiable o está completo, y por último la disponibilidad requerida del activo puede ser en un día, una semana o un mes.

Escala de medición

Es Ordinal.

Variable dependiente

Gestión de vulnerabilidades

Definición conceptual

Es la debilidad o deficiencia en un sistema o componente que puede dejar exposiciones frente a una amenaza o ataque. Las vulnerabilidades también se refieren a cualquier tipo de debilidad en un sistema informático, aplicación o modulo en sí mismo, un conjunto de procedimientos o cualquier cosa que exponga la información.

Gestión de vulnerabilidades es el uso continuo de las herramientas informáticas que permite identificar, valorar, remediar e informar sobre deficiencias técnicas. Este proceso, es de suma importancia a nivel organizacional con el objetivo de prevenir y evitar incidentes informáticos.

Definición operacional:

La base de un programa eficiente de gestión de vulnerabilidades se da a través de la evaluación de vulnerabilidades, la cual se divide en fases tales como: Identificación, Detección y Corrección de vulnerabilidades.

Indicadores:

De acuerdo con Mejía (2020), establece en los atributos que poseen las dimensiones, siendo estos los que permiten su cuantificación.

Los indicadores de gestión de vulnerabilidades, según las dimensiones son los atributos respecto a la fase de identificación, se evalúa el vector de acceso, la complejidad del accesos y/o la autenticación del activo informático; además en la fase de Detección, se valora la Explotabilidad o exposición, el nivel de remediación que se requiere y se debe remitir un reporte de confianza, para ser tratado en la fase de corrección, en la cual se procede con la remediación del daño potencial colateral, se distribuyen los objetivos y se vuelven a definir los requerimientos de seguridad (CID) del activo informático.

Escala de medición

Intervalos.

3.3 Población, muestra, muestreo, unidad de análisis

3.3.1 Población

En frases de Lepkowski (2008), teniendo determinado los activos informáticos, se pondera cada uno, mediante los discernimientos inclusivos y de exclusión, definiéndose como población a los activos informáticos del centro de datos de una entidad pública geocientifica. De lo anterior se pudo establecer el siguiente tamaño de la población:

N= 107 activos informáticos.

3.3.2 Muestra

Para calcular la cantidad de una muestra para una población conocida se tuvo que aplicar la ecuación:

$$n = \frac{N\,Z^2 S^2}{(N-1)e^2 + Z^2 S^2}$$

Dónde

n: tamaño de muestra es 86.
N: tamaño de población (107)

S: Desviación estándar

e: precisión o error (5%)

Z: nivel de confianza (95%)

3.1.3 Muestreo

Según Arias (2022), se entiende como un método que nos ayuda a manejar de manera fácil el análisis de la muestra. Esta investigación empleó una técnica probabilística aleatorio simple, que se usa normalmente en estadística, y elige una muestra significativa de una población amplia.

3.1.3 Unidad de análisis

Son los activos informáticos.

3.4 Técnicas e instrumentos de recolección de datos

Técnicas

Análisis documental permitió recopilar, ordenar y/o valorar la información de los activos informáticos.

Mejía et al. (2018) Es el equipamiento y son las formas por las que se aplica una metodología. Se diferencian los métodos de las técnicas, debido a que son la secuencia de pasos y fases, lo cual es aplicable a las ciencias.

Instrumentos de recolección de datos

Según lo observado cada dimensión genera ítems de acuerdo a las fichas de datos**.**

Según lo manifestado por Rojas (2021), el expediente de observación es un instrumento que define el comportamiento y muestra resultados. Por tanto, la recolección, proceso e interpretación fue realizado en cumplimiento del formato de seguridad y utilizando TIC´s.

3.5 Procedimientos

Se recolectaron datos de activos informáticos, cuantificando los atributos mencionados en el presente documento.

3.6 Método de análisis de datos

Los insumos que quedaron manipulados en esta pesquisa permitieron obtener la validación de la ficha de datos comprobando la confiabilidad de datos. Por lo tanto, se obtuvo el Alfa de Cronbach (Toro, 2022).

La cifra aceptada mínimamente es 0,7; siendo un valor inferior, la evidencia de que el instrumento utilizado es escasa (Toro, 2022). El enfoque cuantitativo, utiliza instrumentales de recogida de datos, determinando claridad en hipótesis concisas para los indicadores. (Wang et al., 2019).

Muestra ha sido mayor a 50, para la normalidad de datos el método a utilizar es Kolmogórov-Smirnov.

Empleamos un programa de computador estadístico especializado SPSS 25.

3.7 Aspectos éticos

Respecto a ética resaltan: Honestidad, Privacidad y/o protección de confidencialidad.

Este trabajo de investigación es propio ya que hice la recaudación, e interpretación, así como las fuentes bibliográficas utilizadas tiene el formato según la 7ma publicación de norma American Psychological Association (APA). Al mismo tiempo, fue valorado en el software especializado Turnitin generando reporte verídico sustentado en Resolución del Vicerrectorado en Investigación N° 008-2017-VI/UCV.

IV. RESULTADOS

Análisis descriptivo

Centrado en analizar eventos relevantes, presentes en aquellas estadísticas que se encuentran disponibles; así como en la reflexión de nuevos descubrimientos. Enfoque basado en interrogantes de estudio. Organizándose posteriormente y mostrando tablas describiendo los resultados.

Prueba de confiablidad del instrumento de recopilación de datos

Tabla 2

Estadística de fiabilidad: Coeficiente de Cronbach

Alfa de Cronbach	N de elementos
0.945	18

Nota: Elaborado por Manuel Gil Miranda (2023)

Las estadísticas del coeficiente alfa de Cronbach, proporciona información sobre consistencia interna de la tarjeta de datos aplicado como recopilación de datos.

Se obtuvo el cálculo del coeficiente mencionado igual a 0,945. Este valor está en el rango de 0 a 1, siendo este último el valor que indica gran consistencia entre los elementos de la ficha de datos. En este caso, un valor de 0,945 sugiere una buena consistencia interna, lo que implica que los indicadores se encuentran correlacionadas de manera positiva entre sí, y además que el instrumento usado tiene una fuerte confiabilidad, es decir que el instrumento de recopilación de datos ha permitido realzar mediciones estables y consistentes.

Número de elementos: Son los 18 indicadores del instrumento de recopilación de datos que se están evaluando para medir la consistencia interna; esto es, 9 indicadores de la variable ISO 27001 y 9 indicadores de la variable de Vulnerabilidades.

Normalidad de Variables

Tabla 3

Pruebas de normalidad de data.

	Kolmogórov-Smirnov		
	Estadístico	gl	Sig.
ISO 27001	0.375	86	0.000
Gestión de Vulnerabilidades	0.393	86	0.000

Nota: Elaborado por Manuel Gil Miranda (2023).

En el cuadro se evidencia hallazgos conseguidos en forma general al momento de realizar el test de Kolmogórov- Smirnov, fue la empleada siempre que la muestra es superior a 50. Como p-valor, es igual 0 < 0.05, refutaríamos la hipótesis nula aprobándose la alternativa, determinando que la data no es de distribución normal. Se utilizaron métodos estadísticos no paramétricos.

Dimensiones de ISO 27001: Confidencialidad, Disponibilidad e Integridad

Tabla 4

Normalidad dimensiones de Variable Independiente

	Kolmogórov-Smirnov		
	Estadístico	gl	Sig.
Confidencialidad	0.385	86	0.000
Integridad	0.374	86	0.000
Disponibilidad	0.339	86	0.000

Nota: Elaborado por Manuel Gil Miranda (2023).

Se aprecia cuales son los efectos de cada dimensión de nuestra variable independiente ISO 27001, al momento de llevarse el test de normalidad Kolmogórov, porque su población es más a 50. Como tienen un valor p = 0; siendo que p-valor es menor 0.05, entonces se objeta la suposición nula, siendo que la data posee repartición normal y se aprueba la alternativa, por lo tanto, estos aciertos no cumplen con colocación normal. Se eligió métodos no paramétricos.

Dimensiones en Gestión de Vulnerabilidades: Identificación, Detección y Corrección

Tabla 5

Normalidad dimensiones de Variable Dependiente

	Kolmogórov-Smirnov		
	Estadístico	gl	Sig.
Identificación	0.412	86	0.000
Detección	0.380	86	0.000
Corrección	0.381	86	0.000

Nota: Elaborado por Manuel Gil Miranda (2023).

Apreciamos que las reseñas obtenidas de dimensiones pertenecientes a la variable dependiente Gestión de Vulnerabilidades, al momento de llevarse a cabo la prueba de Kolmogórov, que fue la empleada, siempre que la población superas los 50. Tal es así, que las 3 dimensiones tienen un valor p igual a 0; y siendo que p-valor es inferior a 0.05, entonces se contradice la conjetura nula dónde las derivaciones poseen repartimiento normal y se aprueba la suposición alternativa, en resumen, los hallazgos incumplen con una normal distribución. Se optó por utilizar métodos estadísticos no paramétricos.

Estadística Descriptiva entre variables

Tabla 6

Cuadro Estadística Descriptiva

	Descriptivos		Estadístico	Desv. Error
ISO 27001	Media		28.1395	0.58788
	95% de intervalo de confianza para la media	Límite inferior	26.9707	
		Límite superior	29.3084	
	Media recortada al 5%		28.3966	
	Mediana		31.0000	
	Varianza		29.721	
	Desv. Desviación		5.45174	
	Mínimo		14.00	
	Máximo		38.00	
	Rango		24.00	
	Rango intercuartil		7.25	
	Asimetría		-1.053	0.260
	Curtosis		0.273	0.514
Gestión Vulnerabilidad	Media		30.3953	0.88246
	95% de intervalo de confianza para la media	Límite inferior	28.6408	
		Límite superior	32.1499	
	Media recortada al 5%		30.9832	
	Mediana		36.0000	
	Varianza		66.971	
	Desv. Desviación		8.18360	
	Mínimo		12.00	
	Máximo		36.00	
	Rango		24.00	
	Rango intercuartil		15.00	
	Asimetría		-0.918	0.260
	Curtosis		-0.938	0.514

Nota: Elaborado por Manuel Gil Miranda (2023).

La interpretación de resultados del recuento descriptivo de la Tabla número 5, para la variable independiente ISO 27001 son los siguientes:

Que la Media (Promedio): La media es 28.1395, lo que indica el valor típico. Lo que representa un nivel moderado sobre la variable. Asimismo, el error estándar es de 0.58788. Este valor indica la variabilidad esperada en la media sobre las muestras. Si el error estándar es mínimo, la estimación de la media será más precisa. Por lo que, un error estándar relativamente bajo sugiere una tasación precisa de la media. El Intervalo de Confianza al 95%: Aporta un nivel en el cual es asequible encontrar

la indudable media poblacional. En este caso, el intervalo va desde 26.9707 hasta 29.3084.

Media Recortada al 5%: La media recortada al 5% (28.3966) se calcula eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.

Mediana: La mediana es de 31.0000, que es similar e indica además que los datos distribuidos no están sesgados de manera significativa.

Varianza y Desviación Estándar: Varianza igual a 29.721 y desviación estándar es 5.45174. Ambas medidas proporcionan información sobre datos dispersos en función a la media. Se muestra que hay una moderada dispersión.

Mínimo y Máximo: El valor mínimo es 14.00 y el máximo es 38.00. Esto proporciona información sobre el rango total de la variable, que es 24.00.

Rango: Diferencia entre máximo y mínimo (38.00 - 14.00 = 24.00), mostrando la extensión total de los datos.

Rango intercuartil (IQR): Diferencia del primer y tercer cuartil (Q3 - Q1) =7.25, precisa dispersión central de los datos, excluyendo los valores extremos.

Asimetría: La asimetría es -1.053, lo que sugiere una ligera asimetría negativa. Los datos están ligeramente sesgados hacia la derecha, pero no de manera significativa.

Curtosis: La curtosis es 0.273, lo que indica una ligera curva en la distribución. La curtosis positiva sugiere colas más ligeras y una distribución más aplanada en comparación con una distribución normal.

Estos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central de la variable independiente ISO 27001 Con ello, se ha podido determinar la variabilidad y la forma de distribuir data.

Interpretar resultados de la nómina descriptiva del cuadro, de la variable Gestión de Vulnerabilidades es:

Que la Media (Promedio): La media es 30.3953, lo que indica el valor típico de variable. Representa un nivel moderado de la variable. Asimismo, el error estándar es de 0.58788. Este valor indica la variabilidad esperada en la media de las muestras. Siempre que el error estándar sea mínimo, será más precisa la estimación. En este caso, un error estándar relativamente bajo sugiere una estimación precisa de la media.

El Intervalo de Confianza al 95%: Proporciona una categoría siendo factible hallar la media en cuanto a población se refiere. En este caso, va desde 28.6408 hasta 32.1499.

Media Recortada al 5%: La media recortada al 5% (30.9832) se calcula eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.

Mediana: La mediana es de 36.0000. Indica que la colocación de datos no está sesgada de manera significativa.

Varianza y Desviación Estándar: Varianza igual a 66.971 y desviación estándar es 8.18360. Ambas medidas proporcionan información sobre distribución de data en torno a la media. En este caso, la desviación estándar muestra que hay una moderada dispersión alrededor de la media.

Mínimo y Máximo: Valor menor es 12.00 y el mayor es 36.00. Esto proporciona información sobre el rango total igual a 24.00.

Rango: Diferencia del máximo y mínimo (36.00 - 12.00 = 24.00), mostrando la extensión total de los datos.

Rango intercuartil (IQR): Diferencia entre el tercer y primer cuartil (Q3 - Q1) = 15.00, lo que indica la dispersión central de los datos, excluyendo los valores extremos.

Asimetría: La asimetría es -0.918, lo que sugiere una ligera asimetría negativa. Los datos están ligeramente sesgados hacia la derecha, pero no de manera significativa.

Curtosis: La curtosis es -0.938, lo que indica una ligera curva en la distribución. La curtosis negativa sugiere colas más ligeras y una distribución más aplanada en comparación con una distribución normal.

Estos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central de la variable dependiente Gestión de Vulnerabilidades. Con ello, se ha podido determinar la variabilidad y la forma de distribución.

Contrastación de hipótesis

Hipótesis general de investigación fue la siguiente:

Tabla 7

Cuadro de formulación de hipótesis general

Objetivo general de investigación	**Hipótesis general**
Determinar cómo ISO 27001 impacta en la gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.	La ISO 27001 impacta considerablemente en gestión de vulnerabilidades en activos informáticos del centro de datos de entidad pública geocientífica, Lima 2023.

Formulación de hipótesis estadística	
Hipótesis nula	HGo: **No existe relación significativa** de ISO 27001, en gestión de vulnerabilidades de activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.
Hipótesis alternativa	HGa: **Existe relación significativa** de ISO 27001, en la gestión de vulnerabilidades de activos informáticos del centro de datos de entidad geocientífica pública, Lima 2023.

Nota: Elaborado por Manuel Gil Miranda (2023).

Tabla 8

Prueba de Correlación entre Variables Independiente y Variable Dependiente

Correlaciones			ISO 27001	Gestión de Vulnerabilidades
Rho de Spearman	ISO 27001	Coeficiente de correlación	1.000	,872**
		Sig. (bilateral)		0.000
		N	86	86
	Gestión de Vulnerabilidades	Coeficiente de correlación	,872**	1.000
		N	86	86

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

Nota: Elaborado por Manuel Gil Miranda (2023).

Teniendo en cuenta que la data distribuida es no normal, realizamos pruebas no paramétricas, se observó correlación Directa positiva muy intensa de 0. 872 de los datos y significancia dónde el valor de $p = 0 < 0.05$, lo que demuestra una conexión sólida entre las variables analizadas. Cuando el valor de $p = 0 < 0.05$, se descarta la hipótesis general nula (HGo), y se acepta la hipótesis general alternativa (HGa).

Formulación de hipótesis específicas

La formulación de la hipótesis específica 1 de investigación fue la siguiente:

Tabla 9

Cuadro de formulación de hipótesis específica 1

Objetivo Específico 1 de investigación	**Hipótesis Específica 1 de investigación**
Determinar cómo la ISO 27001 impacta en la identificación de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.	La ISO 27001 impacta considerablemente en la identificación de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.

Formulación de hipótesis estadística específica 1	
Hipótesis nula	HE1o: **No existe relación significativa** de la ISO 27001, en la identificación de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.
Hipótesis alternativa	HE1a: **Existe relación significativa** de la ISO 27001, sobre la identificación de vulnerabilidades en activos informáticos del centro de datos de entidad geocientífica pública, Lima 2023.

Nota: Elaborado por Manuel Gil Miranda (2023).

Tabla 10

Prueba de Correlación entre ISO 27001 y dimensión Identificación

			ISO 27001	Identificación
Rho de Spearman	ISO 27001	Coeficiente de correlación	1.000	,901**
		Sig. (bilateral)		0.000
		N	86	86
	Identificación	Coeficiente de correlación	,901**	1.000
		Sig. (bilateral)	0.000	
		N	86	86

Nota: Elaborado por Manuel Gil Miranda (2023).

Se observa altamente correlacionable con valor de 0. 901 de los datos y sig. p = 0< 0.05, evidencia vínculo sólido de variables. El sig. p igual a 0 < 0.05, descartando la hipótesis específica 1 nula (HE1o), y se acepta la específica 1 alternativa (HE1a): ISO 27001 impacta considerablemente sobre la identificación de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica.

La formulación de la hipótesis específica 2 de investigación fue la siguiente:

Tabla 11

Cuadro de formulación de hipótesis específica 2

Objetivo Específico 2 de investigación	**Hipótesis Específica 2 de investigación**
Determinar cómo la ISO 27001 impacta en la detección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.	La ISO 27001 impacta considerablemente en la detección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.

Formulación de hipótesis estadística específica 2	
Hipótesis nula	HE2o: **No existe relación significativa** de la ISO 27001, en la detección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.
Hipótesis alternativa	HE2a: **Existe relación significativa** de la ISO 27001, sobre la detección de vulnerabilidades en activos informáticos del centro de datos de entidad geocientífica pública, Lima 2023.

Nota: Elaborado por Manuel Gil Miranda (2023).

Tabla 12

Prueba de Correlación entre ISO 27001 y dimensión Detección

			ISO 27001	Detección
Rho de Spearman	ISO 27001	Coeficiente de correlación	1.000	,752**
		Sig. (bilateral)		0.000
		N	86	86
	Detección	Coeficiente de correlación	,752**	1.000
		N	86	86

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

Nota: Elaborado por Manuel Gil Miranda (2023).

Valor igual a 0.752, siendo correlacional mente intenso y sig. p igual a 0 < 0.05, demostrando un vínculo sólido entre variable y dimensión analizada. El sig. p es igual a 0 < 0.05, descartando hipótesis específica 2 nula (Ho), se desestima la hipótesis específica 2 nula (HE2o), por lo tanto, se acepta la específica 2 alternativa (HE2a): ISO 27001 impacta considerablemente en la detección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica.

La formulación de la hipótesis específica 3 de investigación fue la siguiente:

Tabla 13

Cuadro de formulación de hipótesis específica 3

Objetivo Específico 3 de investigación	**Hipótesis Específica 3 de investigación**
Determinar cómo la ISO 27001 impacta en la corrección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.	La ISO 27001 impacta considerablemente en la corrección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.

Formulación de hipótesis estadística específica 3	
Hipótesis nula	HE3o: **No existe relación significativa** de la ISO 27001, en la corrección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.
Hipótesis alternativa	HE3a: **Existe relación significativa** de la ISO 27001, sobre la corrección de vulnerabilidades en activos informáticos del centro de datos de entidad geocientífica pública, Lima 2023.

Nota: Elaborado por Manuel Gil Miranda (2023).

Tabla 14

Prueba de Correlación entre ISO 27001 y dimensión Corrección

			ISO 27001	Corrección
Rho de Spearman	ISO 27001	Coeficiente de correlación	1.000	,985**
		Sig. (bilateral)		0.000
		N	86	86
	Corrección	Coeficiente de correlación	,985**	1.000
		N	86	86

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

Nota: Elaborado por Manuel Gil Miranda (2023).

Existe alta correlación de 0.985 de data y sig. p = 0 < 0.05, evidenciando sólida conexión entre con la dimensión analizada. Cuando el sig. p = 0 < 0.05, se descarta la hipótesis específica 3 nula (Ho), se desestima la hipótesis específica 3 nula (HE3o), por lo tanto, se acepta la hipótesis específica 3 alternativa (HE3a): ISO 27001 impacta considerablemente en la corrección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica**.**

V. DISCUSIÓN

Producto de las averiguaciones de este estudio, evidenciándose un ascenso notable en la dependencia existente entre dimensiones de ISO 27001 y gestión vulnerabilidades de entidad geocientífica pública. Se tiene como hipótesis principal que ISO 27001 mejora la gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad geocientífica. El resultado posee una cota de significancia $p = 0 < 0.05$, desestimando la teoría de la hipótesis nula y por el contrario se reafirma hipótesis alterna, afirmando que ISO 27001 indudablemente mejora la gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica. También se revela que ejecutar ISO 27001 de manera implícita genera el incremento de la confidencialidad, disponibilidad e integridad sobre activos en la entidad. En una etapa posterior, perceptivamente se muestra un gran interés sobre el tratamiento y atención de las vulnerabilidades, según datos arrojados. Descriptivamente, se ha realizado el estudio por intermedio de fichas de datos de un total de 107 activos informáticos.

Para la estimación inferencial, se ha utilizado Kolmogorov examinando la normalidad que poseen los datos, y se calcula que estos muestran una distribución no paramétrica. Para la etapa de contrastación, se obtuvo el valor estadístico de significancia igual 0,000, mediante Spearman, como análisis de correlación, asimismo la medida de relación es 0,901. Se ratifica descartar la teoría nula y se acepta la hipótesis disyuntiva, conllevando a determinar que ISO 27001 mejora sustancialmente identificar vulnerabilidades.

El resultado general guarda relación según lo señalado por Kapellmann & Washburn (2019), quienes determinaron que es completamente necesario aplicar de manera periódica una política de evaluación de vulnerabilidades, a fin de definir e implantar controles y/o medidas preventivas en materia de seguridad; realizar estos procedimientos significa un reto importante para cualquier entidad, y se tiene como oportunidad, que deben coexistir de manera equilibrada la transparencia de información confidencial y las medidas de protección y, siendo un comportamiento de exposición de vulnerabilidades, por lo tanto, debe considerarse un procedimiento de manejo de vulnerabilidades.

Ante esto, según Ormachea (2019), el equipamiento tecnológico obsoleto, es decir que han completado su vida útil, son el epicentro de muchas vulnerabilidades, siendo el principal riesgo informático de cualquier empresa, debe considerarse también aquellas empresas estatales, cuyas infraestructuras y/o proyectos de Centro de Datos, son tecnología de siguiente generación por lo deben estar preparados para todo tipo de escenario o contexto.

Se concuerda con Huamantingo (2021), determinando que, para la implementación de una guía de exámenes de vulnerabilidades, se cuenta con un pilar fundamental que es la gestión de vulnerabilidades digitales, además de realizar metodologías analíticas y haciendo uso de técnicas ciber defensivas, lo que a su vez contribuye en la reducción de ataques sobre las entidades de gobierno.

Adicionalmente, sería interesante complementar el sistema de calificación y/o puntuación de vulnerabilidades del presente estudio con el modelo de análisis de vulnerabilidades digitales propuesto por Huamantingo (2021), quien menciona que dicho modelo ha sido adaptado para implementarse en cualquier organización publica, con el objetivo de mitigar peligros, manteniendo de manera segura todas las aplicaciones, servicios digitales, redes y comunicaciones, entre otros.

Según el estudio realizado por Mejía (2020), con resultados similares indica que las evaluaciones muestran una notabilidad aproximadamente del 60% ejecutando ISO 27001. Previamente, la apreciación obtenida fue del 11%, sin embargo, el diagnostico posterior tuvo el resultado final con un valor del 71%. Por lo que se deduce que ISO 27001 facilita en gran medida la reducción de las amenazas sobre la forma de acceso, se tuvo media igual a 0.236 en etapa inicial, y posteriormente fue 0.347. El diseño realizado fue experimental a través de pruebas no paramétricas.

En consecuencia, se tienen cálculos conseguidos aplicando ISO 27001, por lo consiguiente se observa la creciente detección de vulnerabilidades en activos informáticos. Para calcular las conjeturas, según la prueba correlacional Spearman, alcanzando la significancia estadística bilateral de 0,000, y además la medida es 0,752. Ante esto, se admite la hipótesis alternativa y se desestima la nula, conduciéndonos a un escenario en el cual se puede afirmar que la implementar ISO 27001 incide notoriamente en la detección de vulnerabilidades.

Acorde a lo realizado por Córdova (2021), la optimización de la adaptabilidad fue por intermedio de ISO 27001, asimismo se clasificaron gran cantidad de peligros o amenazas económicas y administrativas, problemática existente de la casa de estudios superiores. Por otro lado, los colaboradores que pertenecían al área funcional de tecnología o informática, evidencio pobre conocimiento en fundamentos de seguridad (63%) o ISO 27001.

Sobre data recolectada, se ha verificado que es necesario aplicar marcos de trabajo de seguridad y/o ciberseguridad, un patrón a escala personalizada de acuerdo al proceso de negocio o activos informáticos, usualmente los especialista utilizan dos o más en simultaneo, para consolidar y elaborar una mejor propuesta alineada al contexto empresarial, en concordancia con Li, Wang, et al. (2022), que fueron capaces de desarrollar un método único para el análisis de vulnerabilidades, utilizando la métrica de severidad de Márkov.

Por otro lado Niño (2018), señala el tratamiento de riesgos como la guía propuesta en materia de seguridad, lo que nos da la posibilidad de visualizar los riesgos o amenazas, sin estar completamente de acuerdo con este pronunciamiento, sin embargo no existe congruencia toda vez que el análisis de vulnerabilidades identifica fallos o brechas de seguridad en todo el sistema, asimismo, se mide el impacto luego de la prueba de testing o penetration testing, teniendo como vehículo la explotación de la vulnerabilidad. Se confirma que no todas las organizaciones adoptan o implementan controles seguros, muchas piensan cumplir con lo indicado en la normativa, por lo que en gobierno se priorizan otros ámbitos.

En la clasificación de vulnerabilidades, Mugavero et al. (2018), guarda relación debido que en su indagación indica que son complementarios los estándares y guías de buenas prácticas; para conseguir un sistema seguro y a la vez maduro, pero que esto no se ve reflejado en todas las entidades gubernamentales debido a las diferentes realidades, en algunos casos es necesario delimitar el alcance teniendo en cuenta que su estructura organizacional es más pequeña que otras.

Para hipótesis específica respecto de la mitigación de vulnerabilidades, a través del test de Spearman, se obtuvo lo siguiente: estadística bilateral= 0,000, medida 0,985. Estos datos permiten asentir que ISO 27001 impacta claramente en la corrección de vulnerabilidades, siendo este enunciado la aceptación de la hipótesis positiva y el detrimento de la teoría nula. Acorde a la investigación concretada por Guardia (2022), que nos muestra comportamiento ascendente de 72%, en corregir vulnerabilidades interpretando ISO 27001.

Como resultado de las indagaciones, se generaron nuevos subconjuntos considerables dentro del concepto de administración y/o manejo y/o gestión, tales como una adecuada preparación y delimitación de la profundidad de análisis de las vulnerabilidades; como si se tratase de un proyecto se deben definir los servicios digitales y/o aplicativos que serán evaluados. Cabe destacar, que no todos los subconjuntos pueden ser avaluados, como son el tratamiento de eventualidades y la gestión de incidentes aislados, las cuales se diferencian en que los eventos son registros de ataques sin confirmación de ataque, mientras que un incidente es la perpetración de un ataque, que conlleva a la caída de los servicios digitales empresariales, lentitud, saturación de entorno web, y la pérdida o secuestro de datos.

Dentro de los subconjuntos o clasificaciones que emergen, es necesario hacer mención a la capacidad de elaborar la documentación respectiva que corresponde a cada una de las vulnerabilidades, así se puede formar una base de datos de conocimiento, descartando falsas eventos, por ello es importante que durante las pruebas de estrés, se realice mediante el método de la caja gris, siendo un escenario muy ágil, y simula tener los acceso de colaborador institucional, asimismo se cuenta con la técnica forzada de la negociación, que se da durante la etapa de pase a producción de un producto o servicio digital, y en la cual interactúan, los equipos de trabajo de desarrollo y pases productivos en materia de sistemas o aplicativos y el cliente final, en este caso los usuarios, se reducen los tiempos y se acuerdan aplicar de manera ligera algunos controles de seguridad en para el cumplimiento mínimo, asumiendo riesgos, gracias a las corrección o mitigación de vulnerabilidades. Por lo que es factible determinar el nivel de protección que tienen los principales sistemas informáticos o infraestructura tecnológica, ante un ciberataque de alto impacto, ciberguerras con ataques

internacionales, se toman decisiones de protección aceptando el riesgo, que pueden ser como la de aislar la red corporativa o detener los servicios digitales alojados en el centro de datos.

Es primordial que elegir la herramienta tecnológica adecuada para realizar un correcto examen de vulnerabilidades, estando conforme parcialmente con Morales et al. (2020), señalando la existencia de muchos software privados tales como Acunetix, Nessus o Shodan, sin embargo requieren el pago o crédito para hacer uso de sus bondades, por lo a nivel de gobierno central se elige una alternativa de código abierto, comúnmente conocido como software libre, dentro del cual tenemos a Owasp Zap que es de código abierto; el cual realiza un escaneo en modo escucha, y permite identificar el top diez (10) de vulnerabilidades, tal como indica Lala et al. (2021).

Se hallaron deducciones similares a lo presentado por Cueva y Ríos (2017), se revisó la ciberseguridad cuya base fueron los controles de los dominios según ISO 27001. Los efectos mostraron el cumplimiento del 43% de los controles de accesibilidad, evidenciando urgentemente intervenir para la repotenciación del ambiente. Se puede afirmar que la aplicación de algunos controles se encuentra en una fase evolutiva madura, representando un 10% del total, esto significa el cumplimiento parcial actualmente. Asimismo, se tiene que el 33% de medidas están en fase inicial para su implantación. Esta coyuntura se da en parte por las regulaciones gubernamentales peruanas, que deben cumplir entidades como EsSalud. Se identificó una gran falta en cuanto a las capacitaciones del personal de la organización, respecto a ciberseguridad, por lo cual EsSalud se encuentra en la obligación de fortalecer y concientizar a su personal. Se tiene que la ventaja de aplicar ISO 27001, incrementa el grado seguro de activos.

Producto de las observaciones realizadas se tiene como subconjunto que emerge, la implementación de controles la capa del “modelo OSI”, en el cual se encuentran incluidos la capa física, transporte, presentación, sesión y aplicación, entre otros; alineado con ISO 27001, y como recomendación se desprende que es necesario utilizar un factor adicional para la autentificación; así como contar con un procedimiento de mitigación, luego del estudio de vulnerabilidades, siendo un requerimiento determinar vectores de acceso y aquellas técnicas que se usan en

forma intrusiva, asimismo, y de ser posible proseguir con la evaluación en un laboratorio forense digital, impulsar la concientización de los usuarios.

Inferencialmente, según método de Kolmogórov-Smirnov, evaluamos normalidad de data, de distribución no paramétrica. La métrica de hipótesis utilizó Spearman, arrojando como dato de estadística bilateral 0,000, medida=0,872. De esta forma se infiere acertadamente que ISO 27001 tiene impacta de manera significativa en gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica

Se concuerda con Reis et al. (2021), quienes indican que los accesos sin autorización son el principal vector de ataque, y estos los podemos encontrar en un código no seguro de una página web, por ejemplo, y se ve expuesto cuando se publica hacia la internet, por lo que cuando se implemente el factor de doble accesibilidad, genera poca aceptación de los clientes por falta de cultura digital o habilidades digitales.

Por lo tanto, de la revisión de todos los estudios, se establece que ISO 27001 ocasiona un alto impacto sobre el tratamiento de vulnerabilidades, fortalecido la seguridad de las empresas siendo más competitivas y eficientes.

VI. CONCLUSIONES

1. El objetivo general, fue determinado a través de test Spearman, que nos muestra la medición relacional=0,872, y significancia=0.000, señalando una mejora elocuentemente y positiva entre variables, validándose de esta manera la hipótesis alternativa general (HG1), en detrimento de la nula (HG0), entendiéndose que ISO 27001 tiene un impacto sustancial sobre gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.

2. A través de pruebas de Spearman, se tiene que la relación de dimensión identificación y la ISO 27001 es de 0,901, teniendo además valor estadístico bilateral=0.000, lo que indica positividad y a su vez moderada, por lo tanto, se determinó que el objetivo específico uno cumple con la premisa que ISO 27001 enaltece positivamente la identificación de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023.

3. Corroboramos el impacto ascendente entre ISO 27001 y la detección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023. Esta conclusión se da gracias luego de realizar la evaluación de indicadores que a los resultados cuya métrica de relación es 0,752, y la significancia bilateral es 0.000, desestimando aquella teoría nula (HE20) y abrazando la suposición alterna (HE2a).

4. Finalmente, se determinó que ISO 27001 incrementa positivamente la corrección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023. La medida relacional es igual a 0,985, y la estadística bilateral tiene el valor de 0.000, se considera moderada y positiva, entonces se ha validado la suposición específica 3 alternativa (HE3a) y no se acepta la teoría específica número 3 nula (HE30).

VII. RECOMENDACIONES

1. El Oficial de Seguridad y Confianza Digital de la empresa geocientifica pública, debe auditar en forma interna y realizar seguimiento tras la ejecución de la ISO 27001, con el plan de lograr la mejora continua para el tratamiento de vulnerabilidades en activos informáticos. La asimilación de la norma citada avalará un elevado nivel de eficiencia vinculado con la defensa de activos.

2. Se recomienda al coordinador del área funcional de Redes y Comunicaciones, ejecutar un cronograma para evaluar la severidad de las vulnerabilidades y exposiciones más comunes de los activos informáticos del centro de datos. De esta forma se podrá reducir los riesgos existentes. Realizar este plan de gestión de vulnerabilidades permitiendo control efectivo y aseguramiento de data permanentemente.

3. Se recomienda al encargado funcional de Desarrollo y Mantenimiento, que establezca manuales de procedimientos de código seguro de los aplicativos de información propios de la empresa geocientífica pública para identificar vulnerabilidades que afecten la accesibilidad de la información. Esta acción permitirá lograr dinamismo y flexibilidad. Elaborar estos manuales establecerá pautas concretas y fichas de procedimiento definidos para garantizando adaptabilidad efectiva frente a cambios. Fortaleciendo una cultura organizacional que priorice la transformación digital.

4. Se recomienda al coordinador líder del Grupo de Respuesta ante Incidentes de Seguridad, planificar estrategias y desarrollar tácticas preventivas de respuesta para eventos de seguridad informática. Esto beneficia a la entidad, porque obteniendo datos en tiempo real se podrán prevenir ciberataques. Implementar planes de acción fortalecerá la seguridad informática, garantizando acceso seguro a los datos e información altamente disponible, logrando la continuidad operativa de la entidad pública geocientifica.

REFERENCIAS

Álvarez y Honorio (2018). Ciberseguridad en la actividad organizacional de la era digital. Maestro en Ingeniería de sistemas con mención en tecnologías de la información. Universidad Nacional Federico Villarreal.

Agustino, D. (2018). *Information Security Management System Analysis Menggunakan ISO 27001.* Jurnal Eksplora Informatika. https://doi.org/10.30864/eksplora.v8i1.130

Atencio, E. (2019). Diseño de un sistema de gestión de seguridad de la Información basada en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú. Universidad Nacional Daniel Alcides Carrión, Cerro de Pasco – Perú.

Arias (2022). Guía para elaborar la operacionalización de variables. Espacio I+D, Innovación más Desarrollo, 10(28). https://doi.org/10.31644/IMASD.28.2021.a02 (Original work published 2 de octubre de 2021)

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encinas, L. (2020). Ciberseguridad. CSIC

Baena, G. (2017). Metodología de investigación. ISBN ebook: 978-607-744-7481 Recuperado de http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

Bai, H. (2022). *Legal Management of Network Information Security Based on Embedded Real-Time Task Processing*. https://doi.org/10.1155/2022/2379274

Bailon, L. (2019). Gestión de riesgos en área tecnológica de empresas que exportan pesca blanca de Manta y Jaramijó. Polo del Conocimiento: Revista científico-profesional, 4(8), 165-189. https://dialnet.unirioja.es/servlet/articulo?codigo=7164331

Blázquez (2022). La ciberseguridad en gestión de activos: cómo gestionar los Riesgos.

Bertalanffy, L. (1976). Teoría General de Sistemas: Fundamentos, aplicaciones.

Fondo de Cultura Económica. https://fad.unsa.edu.pe/bancayseguros/wpcontent/uploads/sites/4/2019/03/Teoria-General-de-los-Sistemas.pdf

Bustamante, S., Valles, M. A., Cuellar, I. E., & Lévano, D. (2021*). Políticas según la ISO 27001: 2013 y su influencia en la seguridad de la información de municipalidades en Perú*. Enfoque UTE, 12(2), pp. 69- 79. https://doi.org/10.29019/enfoqueute.743

Cardona, J. & Restrepo, R. (2020). *Evaluación de implementación de ISO 27001 en empresas privadas, bajo enfoque cultural. Tecnológico de Antioquia*, Institución Universitaria. https://dspace.tdea.edu.co/handle/tdea/921

Córdova, J. (2021). *Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia*. [Tesis Maestría]. Universidad Peruana Unión. http://hdl.handle.net/20.500.12840/4789

Córdoba, J. H. (2021). Propuesta de implementación de un Sistema Gestor de Seguridad de la Información, basados en INTE/ISO/IEC 27001: 2014 en el departamento de TI para Almacenes El Rey, en el año 2021. Tecnología Vital, 1(9).

Cabezas, E., Andrade, A. y Torres, J. (2018). Introducción a metodología de la investigación científica. ISBN: 978-9942-765-44-4. Recuperado de http://repositorio.espe.edu.ec/jspui/bitstream/21000/15424/1/Introduccion%20a%20la%20Metodologia%20de%20la%20investigacion%20cientifica.pdf

Carvajal, D., Cardona, A. y Valencia, F. (2019). A proposal for the management of The information security applied to a Colombian public entity. 13(25). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672019000100068

Carrasco E. (2021). Activo: Qué es un activo, clasificación y pérdida de valor. Repositorio en 30 julio, 2022. https://www.stelorder.com/blog/activo/

Castillo, G. (2018). Modelo de optimización de recursos de un data center que

Brinda infraestructura como servicio (IAAS) de manera controlable y auditable a pymes de la Provincia del Santa. Universidad Nacional del Santa. http://repositorio.uns.edu.pe/handle/UNS/3151

Chen T. L., Huang, Y. M., & Liu, C. H. (2021). *Security Privacy and Policy for Cryptographic Based Electronic Medical Information System*. Sensors (Basel, Switzerland), 21(3), 713. https://doi.org/10.3390/s21030713

Chen, L., Xie, Z., Zhen, J., & Dong, K. (2022). The Impact of Challenge Information Security Stress on Information Security Policy Compliance: The Mediating Roles of Emotions. Psychology Research and Behavior Management, 15,1177-1191. https://doi.org/10.2147/PRBM.S359277

Cybersecurity y Infrastructure Security Agency (CISA). (2019). What is Cybersecurity. [Online] Available at: https://us-cert.cisa.gov/ncas/tips/ST04-001

Cohen, N. y Gómez, G. (2019). Metodología de la investigación, Producción de los datos y diseños. ISBN 978-987-723-190-8. Editorial Teseo. Recuperado http://biblioteca.clacso.edu.ar/clacso/se/20190823024606/Metodologia_para_que.pdf

Concepción, D., González, E., García, R. y Miño, J. (2019). Investigation methodology: Origin and construction of a doctoral tesis. 6(1). 76-87. http://scielo.iics.una.py/pdf/ucsa/v6n1/2409-8752-ucsa-6-01-76.pdf

Diaz M. (2021). El videoanálisis, evolución a las fichas de observación de clase. Recuperado el 20 de julio de 2022. https://www.codimg.com/education/blog/es/fichasobservacionclase#:~:text=Las%20fichas%20de%20observaci%C3%B3n%20son,que%20el%20videoan%C3%A1lisis%20puede%20solventar

Díaz, L. V. (2021). Percepción de la implantación de la NTP 27001:2014 basado en la documentación gubernamental del centro del Perú, año 2021. Universidad César Vallejo, Perú. https://repositorio.ucv.edu.pe/handle/20.500.12692/76216

Espinoza, M. (2021). Estudio y diseño de un data center aplicando la norma ANSI/TIA 942 para ISP AZOTEL S.A. Tesis de posgrado. http://201.159.223.180/bitstream/3317/16622/1/T-UCSG-POS-MTEL-196.pdf

Ferreira, R. S., Frogeri, R. F., Coelho, A., & Piurcosky, F. (2018). Prácticas de gestión de la seguridad de la información: Estudio de los factores que influyen en una institución de la Fuerza Aérea brasileña. *JISTEM - Revista de Sistemas de Información y Gestión de Tecnologías, 15*. https://doi.org/10.4301/S1807-1775201815005

Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2018). La seguridad Informática y la seguridad de la información. *Polo del Conocimiento, 2*(12), 145-155. https://doi.org/10.23857/pc.v2i12.420

Flores, S. (2018). Propuesta para la implementación de una red de datos para mejorar la Comunicación de las áreas del instituto de educación superior tecnológico publico todas las Artes – 2018. Universidad Nacional José María Arguedas. https://repositorio.unajma.edu.pe/bitstream/handle/123456789/548/Sandy_Tesis_Bachiler_2018.pdf?sequence=1&isAllowed=y

García, J. C., Huamani, S. C., & Lomparte, R. F. (2018). Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. *Revista Peruana De Computación Y Sistemas, 1*(1), 47–56. https://doi.org/10.15381/rpcs.v1i1.14856

Gil, V. y Gil, J. (2017). Seguridad informática organizacional: un modelo de Simulación basada en dinámica de sistemas. 22 (2). https://www.redalyc.org/pdf/849/84953103011.pdf

Gil, J. y Maihuiri, L. (2018). Implementación de un data center virtual en Cloud Computing para mejorar los servicios del departamento de ti en la empresa venus peruana S.A.C. Universidad Autónoma. http://repositorio.autonoma.edu.pe/bitstream/AUTONOMA/603/1/Gil%20Izurraga%20Jose%20Edu%2c%20y%20Maihuiri%20Vargas%2c%20Lenin%20Alex.pdf

Hannigan, L., Deyab, G., Al Thani, A., Al Marri, A., & Afifi, N. (2019). The Implementation of an Integrated Management System at Qatar Biobank. Biopreservation and Biobanking, 17(6), 506-511. https://doi.org/10.1089/bio.2019.0076

Hernández. R. y Mendoza, C. (2018). Metodología de la investigación- rutas Cuantitativa cualitativa-mixta. ISBN 1456260960. Editor McGraw-Hill Interamericana International Organization for Standardization. (2008). ISO

9001: Sistemas de gestión de la Calidad - Requisitos (4ta 2008-11-15 ed.). Ginebra, Suiza: Secretaria Central de ISO.

Hernández, F. (2019). The risks of information and communication technologies. https://www.medigraphic.com/pdfs/conamed/con-2019/con194d.pdf

Huamantingo (2021). Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021. Universidad Cesar Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/85150

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

Jara (2018). Tecnologías de la información y comunicación. Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018. Maestro en Ingeniería de sistemas con mención en tecnologías de la información. [Tesis de Maestro inédita]. Universidad Cesar Vallejo

Jelovčan, L., Mihelič, A., & Prislan, K. (2022). Outsource or not? An AHP Based Decision Model for Information Security Management. *Organizacija, 55*(2), 142-159. https://doi.org/10.2478/orga-2022-0010

Juma, G. (2017). Diseño de un data center tipo TIER I para el gobierno autónomo descentralizado municipal de Otavalo bajo la norma ANSI/TIA-942. Universidad Técnica del Norte. http://repositorio.utn.edu.ec/bitstream/123456789/6982/2/ARTICULO.pdf

Kim, Y., & Kim, B. (2021). The Effective Factors on Continuity of Corporate Information Security Management: Based on TOE Framework. *Information, 12*(11), 446. https://doi.org/10.3390/info12110446

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. *Journal of Information Systems Engineering & Management, 4*(2), 21. https://doi.org/10.29333/jisem/5888

Maingak, A. Z., Candiwan, C., & Harsono, L. D. (2018). *Information security assessment using ISO/IEC 27001:2013 standard on government institution*. Trikonomika, 17(1), 28-37. https://doi.org/10.23969/trikonomika.v17i1.1138

Martínez y Fernández (2020). Ciberdelitos. Ediciones Experiencia.

https://ebsco.bibliotecaupn.elogim.com/login.aspx?direct=true&AuthType=ip,uid&db=nlebk&AN=2712945&lang=es&site=ehostlive&ebv=EK&ppid=Pa

Martelo, R., Tovar, L. y Maza, D. (2018). Basic Logical Safety Model. Study Case: The Network Laboratory of the University of Cartagena in Colombia. 29(1). https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100003

Mejía, B. (2020). *Implementación de controles de la ISO 27002 para gestión de base de datos de registros públicos de la Zona VII en Huaraz, 2019*. Universidad Peruana de Ciencias e Informática. http://repositorio.upci.edu.pe/handle/upci/151

Mitxelena, Dal Cin y Bissell (2022) Estado de resiliencia en ciberseguridad 2021. Recuperado del 01 de mayo de 2022. https://www.accenture.com/eses/insights/security/invest-cyber-resilience

Montalván, J., Soria, C., Hopkins, A., Ascue, R. y Ajito, E. (2019). Guía de investigación.
ISBN: 978-612-4439-09-4. Primera edición digital. Recuperado de https://cdn02.pucp.education/investigacion/2016/06/12214732/guia-deinvestigacion-en-diseno.pdf

Mohammed, T. J., & Jasim, N. A. (2022). *Designing a model to protect Documented information according to the integration of some international standards (ISO 27001: 2013) (ISO 10013: 2021): A case study*. International Journal of Health Sciences, 6(S3), 10684–10697. https://doi.org/10.53730/ijhs.v6nS3.8376

Monev, V. (2020). Organisational *Information Security Maturity Assessment Based on ISO 27001 and ISO 27002*. In 2020 International Conference on Information Technologies (InfoTech) (pp. 1-5). Varna, Bulgaria. doi: 10.1109/InfoTech49733.2020.9211066.

Montaño, R. y Bustíos, J. (2020). Diseño de un data center con arquitectura Convergente para optimizar los procesos informáticos de la municipalidad distrital de José Leonardo Ortiz. Universidad Nacional Pedro Ruiz Gallo. https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/8862/Monta%c3%b1o_Guerrero_Richard_Alan_y_Bust%c3%ados_Arteaga_Jorge_Luis_Jes%c3%bas.pdf?sequence=1&isAllowed=y

Navarro, E., Jiménez, E. y Rappoport, S. (2017). Fundamentos de la

investigación y la innovación educativa. ISBN: 978-84-16602-55-1. Recuperado de https://www.unir.net/wp-content/uploads/2017/04/Investigacion_innovacion.pdf

Niño, N. (2018). Modelo de un sistema de gestión de seguridad de Información, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto nacional de estadística e informática **51** Filial Lambayeque. Universidad Nacional Pedro Ruiz Gallo, Lambayeque Perú.

Ochoa, C. (2019). Diseño y análisis en investigación. ISBN: 978-84-7867-685-9. Recuperado de https://www.aepap.org/sites/default/files/documento/archivosadjuntos/artl_2019_libro_diseno_y_analisis_de_investigacion.pdf

Ordoñez, J., Real, J., Gallardo, J., Alvarado, H., & Roby, A. (2018). Knowledge On sexual health and its relationship with sexual behavior in university students. *Anales de La Facultad de Medicina, 78*(4), 423. https://doi.org/10.15381/anales.v78i4.14264

Peñaloza (2019). Desafíos del riesgo cibernético en el sector Financiero para Colombia y américa latina. Repositorio en 29 mayo, 2022 https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-enel-sector-financiero-para-Colombia-y-America-Latina.pdf

Rodríguez, L., Cruzado, C., Mejía, C. y Alarcón, M. (2020). Application of ISO 27001 And its influence on the information security of a Peruvian private company.8(3).http://www.scielo.org.pe/scielo.php?pid=S2307-79992020000400011&script=sci_arttext

Rincón, J. (2019). *Implantación de un sistema de gestión de la seguridad de la información según la norma ISO/IEC 27001 en una entidad.* Repositorio Institucional Universitat Oberta de Catalunya. http://hdl.handle.net/10609/107386

Rojas C. (2021). Ficha de Observación. Recuperado el 27 de julio de 2022 https://milformatos.com/escolares/ficha-de-observacion/

Sánchez (2022). El 55% de las empresas no se defiende eficazmente de los ciberataques, según un estudio de Accenture. Recuperado el 30 de mayo del 2022. https://newsroom.accenture.es/es/news/mas-de-la-mitad-de-lasempresas-nose-defiende-eficazmente-de-los-ciberataques.htm

Santiago (2020). Aportes para la adecuación del marco jurídico de ciberdefensa y ciberseguridad Argentina. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1618_TatoNS.pdf

Shannon, C. E., & Weaver, W. (1964). The mathematical theory of communication. *University of Illinois Press.* https://pure.mpg.de/rest/items/item_2383164/component/file_2383163/content

Taco, R. (2019). Uso de racktables DCIM como herramienta para optimizar la gestión de los equipos que conforman el DC de una empresa eléctrica en la ciudad de Tacna, 2019. Universidad Privada De Tacna. https://repositorio.upt.edu.pe/bitstream/handle/20.500.12969/1218/Taco-CoaylaRenzo.pdf?sequence=1&isAllowed=y

Taípe Domínguez & Daniel Iván (2020). La auditoría de seguridad informática y relación en ciberseguridad del sector público año 2018. https://repositorio.unp.edu.pe/bitstream/handle/20.500.12676/2361/INFOR-TAI-DOM-2020.pdf?sequence=1&isAllowed=y

TEC (2022). Valoración de riesgo. Repositorio en 30 mayo, 2022 https://www.tec.ac.cr/valoracion-riesgo

Toro, R., Peña, M., Avendaño, B. L., Mejía, S., & Bernal, A. (2022). Análisis del Coeficiente Alfa de Cronbach según Opciones de Respuesta, Muestra y Observaciones Atípicas. *Revista Iberoamericana de Diagnóstico y Evaluación - e Avaliação Psicológica, 2*(63), 17-30. https://www.redalyc.org/articulo.oa?id=459671926003

Thoyyibah, T. (2018). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO 27001:2013 Pada Pusat Informasi dan Pangkalan Data Perguruan Tinggi X. *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informasi, 4(*2), 72-76. https://doi.org/10.24014/coreit.v4i2.6292

Turac (2020) Risks with construction project risk management - An insight into how professionals within the construction industry manage risk. Stockholm, Suecia. Recuperado 04 de junio de 2022. https://www.divaportal.org/smash/get/diva2:1445409/FULLTEXT01.pdf

Vargas, G. (2020). Virtualization of academic content in distance Learning

Environments. 61 (2). http://www.scielo.org.bo/scielo.php?pid=S1652-67762020000200009&script=sci_arttext

Vega, et al. (2020). Red de monitorización para automatizar el sistema de enfriamiento de un centro de datos. 24 (1). https://www.redalyc.org/journal/5055/505563460010/505563460010.pdf

Vela Rios, E. M. (2021). Seguridad de información basada en la norma ISO/IEC 27001: 2013 y nivel de seguridad en el centro de capacitaciones SENCICO–Ucayali 2018

Vela, Oxolon, I. A., Requejo-Mirez, M. S., Cubillas-Cochachin, C. G., Perez -Mantari, L. K., & Alfaro-Paredes, E. A. (2019). Analyzing the classification of technical standards for the management of information technology infrastructure and services. DYNA, 94(5), 484-484.

Vega, E.M., Delgado,J.R, & De los Santos, A. C. (2022). *Importancia de la gestión de seguridad de la información en instituciones educativas con ITIL e ISO 27001. Revista de investigación de Sistemas e Informática*, 5(1), 113-123.https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/view/23362/18739

Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P., & Moscoso-Zea, O. (2018). *Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry*. In 2018 International Conference on Information Systems and Computer Science (INCISCOS) (pp. 294-300). Quito, Ecuador. doi: 10.1109/INCISCOS.2018.00049

Velasco, L. (2019). Diseño de data center basado en el estándar ANSI/BICSI-002 -2014 para el funcionamiento de los servicios y aplicaciones de la Cooperativa Nuevo Milenio. Universidad Inca Garcilaso de la Vega. http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/4504/TESIS_VELASCO_LUIS.pdf?sequence=1&isAllowed=y

Wang, R., & Wang, Y. (2019). Compatible matrices of Spearman's rank correlation. Paper. *Statistics and Probability Letters, 151*(1), 67–72. https://doi.org/10.1016/j.spl.2019.03.015

Yang, M., & Wang, J. (2022). The Security of Student Information Management System Based upon Blockchain. *Journal of Electrical and Computer Engineering*, 2022. https://doi.org/10.1155/2022/8186189

ANEXOS

Anexo 1: Matriz de Operacionalización de Variables

TÍTULO: ISO 27001 y gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023

AUTOR: Gil Miranda, Manuel Eleodoro

Variables de estudio	Definición conceptual	Definición operacional	Dimensión	Indicadores	Escala de Medición
Independiente: ISO 27001	Velar por confidencialidad, disponibilidad e integridad de data, argumentando que implementando SGSI, permite el encargo de eventualidades, así como controlar la pertenencia de datos de la compañía, y su capacidad competitiva de dirigir y monitorear los procesos	Para un (SGSI) según ISO 27001, se debe tener procedimiento de mitigación de riesgos en activos de información, así como establecer medidas de control. (ISOTools, 2019).	Confidencialidad, atributo indicativo que el activo se encuentre o no habilitado, no sea reconocida por terceros o agentes sin permiso.	1. Acceso Libre 2.Restringido 3.Protegida	Ordinal 1=Muy bajo, 2=Bajo, 3=Medio, 4=Alto, 5=Muy Alto
			Integridad, indica que el activo no fue alterado o modificado indebidamente.	1.Exacto 2.Fiable 3. Completo	
			Disponibilidad, es decir que se encuentre utilizable cuando se requiera.	1.Dia 2.Semana 3. Mes	
Dependiente: Gestión de vulnerabilidades	Es la debilidad o deficiencia en un sistema o componente que puede dejar exposiciones frente a una amenaza o ataque. Las vulnerabilidades también se refieren a cualquier tipo de debilidad en un sistema informático, aplicación o modulo en sí mismo, un conjunto de	La base de un programa eficiente de gestión de vulnerabilidades se da a través de la evaluación de vulnerabilidades, la cual se divide en fases tales como: Identificación, Detección y Corrección de vulnerabilidades.	El paso de identificación implica descubrir vulnerabilidades en el entorno, a través de escaneos automatizados, prueba de penetración e incluso informes de seguridad proporcionados por fabricantes de software y hardware.	1. Vector de acceso. 2. Complejidad de acceso 3. Autenticación	Intervalo Muy Bajo 0 Bajo 0.1-3.9 Medio 4.0-6.9 Alto 7.0-8.9

TÍTULO: ISO 27001 y gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023

AUTOR: Gil Miranda, Manuel Eleodoro

Variables de estudio	Definición conceptual	Definición operacional	Dimensión	Indicadores	Escala de Medición
	procedimientos o cualquier cosa que exponga la información. Gestión de vulnerabilidades es el uso continuo de las herramientas informáticas que permite identificar, valorar, remediar e informar sobre deficiencias técnicas. Este proceso, es de suma importancia a nivel organizacional con el objetivo de prevenir y evitar incidentes informáticos.		Detectar, el daño potencial que podría causar una explotación de la vulnerabilidad y determinar con qué facilidad un atacante podría explotarla.	1. Explotabilidad 2. Nivel de Remediación 3. Reporte de confianza	Muy Alto 9.0-10.00
			Corrección, aplicación de parches de seguridad, actualizaciones de software, configuraciones mejoradas, entre otras medidas.	1. Daño potencial colateral 2. Distribución de objetivos 3. Requerimientos de confidencialidad, integridad y disponibilidad	

Matriz de Consistencia

TÍTULO: ISO 27001 y gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023

AUTOR: Gil Miranda, Manuel Eleodoro

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES
Problema principal: ¿La ISO 27001 impacta en la gestión de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientifica, Lima 2023? **Problemas específicos:** **PE1:** ¿La ISO 27001 impacta en la identificación de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientifica, Lima 2023?; **PE2:** ¿La ISO 27001 impacta en la detección de vulnerabilidades en activos informáticos del	**Objetivo principal:** Determinar cómo la ISO 27001 impacta en la gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientifica**.** **Objetivos específicos:** **OE1**: Establecer cómo ISO 27001 impacta en la identificación de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientífica, Lima 2023; **OE2:** Determinar cómo la ISO 27001 impacta en la detección de vulnerabilidades en activos informáticos del centro de	**Hipótesis principal:** La ISO 27001 impacta considerablemente en la gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientifica**.** **Hipótesis específicas:** **HE1:** La ISO 27001 impacta considerablemente en la identificación de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientifica, Lima 2023; **HE2:** La ISO 27001 impacta considerablemente en la detección de vulnerabilidades en activos informáticos del centro de	**Variable - 1:** ISO 27001

Dimensiones	Indicadores	Ítems	Niveles
Confidencialidad	Libre	1	1=Muy bajo, 2=Bajo, 3=Medio, 4=Alto, 5=Muy Alto
	Restringida	2	
	Protegida	3	
Integridad	Exactitud	4	
	fiabilidad	5	
	Completitud	6	
Disponibilidad	Hasta un día	7	
	Hasta una semana	8	
	Hasta un mes	9	

Variable - 2: Gestión de Vulnerabilidades

Dimensiones	Indicadores	Ítems	Niveles
Identificar	Vector de acceso	10	
	Complejidad de acceso	11	

TÍTULO: ISO 27001 y gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023

AUTOR: Gil Miranda, Manuel Eleodoro

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
centro de datos de la entidad pública geocientifica, Lima 2023? **PE3:** ¿La ISO 27001 impacta en la corrección de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientifica, Lima 2023?	datos de la entidad pública geocientifica, Lima 2023; **OE3:** Determinar cómo la ISO 27001 impacta en la corrección de vulnerabilidades en activos informáticos del centro de datos de la entidad pública geocientifica, Lima 2023.	datos de la entidad pública geocientifica, Lima 2023; **HE3:** La ISO 27001 impacta considerablemente en la corrección de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientifica, Lima 2023.		Autenticación	12	Muy Bajo 0 Bajo 0.1-3.9 Medio 4.0-6.9 Alto 7.0-8.9 Muy Alto 9.0-10.00
			Detectar	Explotabilidad	13	
				Nivel de Remediación	14	
				Reporte de confianza	15	
			Corregir	Daño potencial colateral	16	
				Distribución de objetivos	17	
				Requerimientos de confidencialidad, integridad y disponibilidad	18	

Anexo 2: Instrumento de recolección de datos

	Operacionalización de Variables:	V1: ISO 27001									SUBTOTAL VARIABLE INDEPENDIENTE	V2: Vulnerabilidades									SUBTOTAL VARIABLE DEPENDIENTE
		D1: Confidencialidad			D2: Integridad			D3: Disponibilidad				D1: Identificar			D2: Detectar			D3: Corregir			
		I1: Acceso Libre	I2: Acceso restringido	I3: Protegida	I4: Exactitud	I5: Fiabilidad	I6: Completitud	I7: Un día	I8: Una semana	I9: Un mes		I10: Nivel de Vector de Acceso	I11: Complejidad de Accesos	I12: Autenticación	I13: Explotabilidad	I14: Nivel de Remediación	I15: Reporte de Confianza	I16: Daño Potencial Colateral	I17: Distribución de Objetivos	I18: Requerimientos de CID	
N°	ACTIVOS INFORMATICOS	1	2	3	4	5	6	7	8	9		10	11	12	13	14	15	16	17	18	
1	Central Telefonica	3	3	1	3	2	2	1	2	2	**19**	4	2	2	3	4	1	2	1	2	**21**
2	Switches del centro datos	3	4	3	2	3	2	1	2	2	**22**	3	2	2	2	3	1	2	1	2	**18**
3	Equipo controlador de entrega de aplicaciones - Citrix	3	4	4	2	4	3	3	3	4	**30**	4	3	4	2	4	4	3	3	3	**31**
4	Firewall Empresarial	3	1	1	2	2	2	3	1	1	**16**	1	1	3	1	3	3	2	3	1	**18**
5	Sistema de Acceso Biometrico	4	3	3	3	4	3	3	4	4	**31**	5	3	2	2	4	2	3	3	4	**28**
6	Sistema contra incendio	2	2	2	3	2	1	1	1	2	**16**	1	1	2	1	3	1	1	1	1	**13**

7	Sistema de Monitoreo Ambiental	3	2	1	1	1	1	1	3	1	**14**	2	2	1	1	4	1	1	1	3	**14**
8	Sistema de Climatización - Aires Acondicionado de Precision	3	2	2	3	3	3	3	2	2	**23**	1	2	1	2	3	3	3	3	2	**20**
9	Equipo de Filtro de contenido	4	3	1	3	4	2	1	3	1	**22**	2	2	2	2	3	2	2	1	3	**17**
10	Equipo Administrador de Ancho de Banda	3	4	2	2	4	4	2	4	2	**27**	1	1	1	1	2	1	4	2	4	**15**
11	Equipo de Firewall de aplicaciones - WAF	5	4	2	3	3	4	5	5	5	**36**	3	4	3	5	4	3	4	5	5	**36**
12	Acumulador de Energia - UPS	3	2	3	3	2	4	1	4	2	**24**	3	1	1	2	3	2	4	1	4	**19**
13	Equipo anti denegacion de Servicios - Anti Ddos	3	3	1	2	2	3	2	3	3	**22**	3	2	1	3	3	3	3	2	3	**23**
14	Servidor de archivos	4	4	5	3	3	4	5	5	5	**38**	3	4	5	2	5	2	4	5	5	**35**
15	Servidor de base de datos de mineria	4	3	3	2	1	1	1	3	2	**20**	1	2	1	4	5	1	1	1	3	**18**
16	Servidor de base de datos de core administrativo	3	3	1	3	1	3	2	3	4	**23**	3	1	2	3	5	2	3	2	3	**25**
17	Servidor de base de datos de geologia	4	4	1	2	1	2	1	1	2	**18**	1	1	1	1	5	4	2	1	1	**18**
18	Servidor de base de datos espacial	4	3	1	2	2	2	2	1	2	**19**	2	2	1	2	3	2	2	2	1	**18**

19	Servidor de aplicaciones de mineria	4	5	1	1	5	3	3	3	3	**28**	2	3	3	1	2	2	3	3	3	**22**
20	Servidor de aplicaciones de geologia	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
21	Servidor de aplicaciones administrativas	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
22	Servidor de correo	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
23	Servidor de Directorio Activo	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
24	Servidor de Intranet	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
25	Servidor de Laserfiche	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
26	Servidor de METADATOS	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
27	Servidor de BIBLIOTECA	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
28	Servidor de REPOSITORIO	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
29	Servidor de Revistas Seriadas	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
30	Servidor FTP	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
31	Servidor SFTP	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
32	Servidor Licencias Autocad	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
33	Servidor Licencias CITRIX	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
34	Servidor Licencias GIS	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
35	Servidor NTP	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**

36	Servidor de Petitorio Online	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
37	Servidor de DHCP	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
38	Servidor DNS	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
39	Servidor PIDE	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
40	Servidor de aplicaciones CITRIX	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
41	Servidor de VDI CITRIX	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
42	Servidor de Telefonia VOZ IP	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
43	Servidor ECATASTRO	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
44	Servidor Padron Minero	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
45	Servidor SIGA PATROMONIO	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
46	Servidor Sistema de Colas	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
47	Servidor Portal Web	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
48	Servidor de Federación de cuentas	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
49	Servidor GEOCATMIN	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
50	Servidor SIDEMCAT	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
51	Servidor SUBVersion	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
52	Servidor SESUITE	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
53	Servidor de tramite documentario	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**

54	Servidor de convocatorias CAS	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
55	Servidor ANTISPAM	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
56	Servidor ANTIVIRUS	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
57	Servidor Contact Center	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
58	Sistema de Almacenamiento HPE 3PAR	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
59	Sistema de Almacenamiento HUAWEI	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
60	Servidor de Impresoras	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
61	Servidor de Inventario de Equipos	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
62	Servidor de Tarificador de llamadas	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
63	Servidor de Backup Dataprotector	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
64	Servidor de Backup Veeam	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
65	Servidor de VMWAR VCENTER	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
66	Servidor WSUS	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
67	Servidor Proxy reverso	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
68	Servidor de firma digital	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**

69	Servidor de de Adm. De Filtro de Contenido	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
70	Servidor SIEM	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
71	Servidor de agente de Firewall	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
72	Servidor de Analisis de Vulnerabilidades	5	2	1	4	4	5	3	4	3	**31**	3	4	3	5	5	4	5	3	4	**35**
73	Cintas Magneticas	2	2	2	3	2	1	1	1	2	**16**	1	1	2	1	3	1	1	1	1	**13**
74	PDUS	3	2	1	1	1	1	1	3	1	**14**	2	2	1	1	4	1	1	1	3	**14**
75	Gabinete de Servidores	3	2	2	3	3	3	3	2	2	**23**	1	2	1	2	3	3	3	3	2	**20**
76	Gabinete de Comunicaciones	4	3	1	3	4	2	1	3	1	**22**	2	2	2	2	3	2	2	1	3	**17**
77	Tablero de Dsitribucion Electrica	3	4	2	2	4	4	2	4	2	**27**	1	1	1	1	2	1	4	2	4	**15**
78	Transformador de aislamiento	5	4	2	3	3	4	5	5	5	**36**	3	4	3	5	4	3	4	5	5	**36**
79	Pozos a tierra	3	2	3	3	2	4	1	4	2	**24**	3	1	1	2	3	2	4	1	4	**19**
80	CCTV	3	3	1	2	2	3	2	3	3	**22**	3	2	1	3	3	3	3	2	3	**23**
81	Sensores de Humedad	4	4	5	3	3	4	5	5	5	**38**	3	4	5	2	5	2	4	5	5	**35**
82	Sensores de aniego	4	3	3	2	1	1	1	3	2	**20**	1	2	1	4	5	1	1	1	3	**18**
83	Sensores de Humo	3	3	1	3	1	3	2	3	4	**23**	3	1	2	3	5	2	3	2	3	**25**
84	Sensores de temperatura	4	4	1	2	1	2	1	1	2	**18**	1	1	1	1	5	4	2	1	1	**18**
85	Sensor de intrusión	4	3	1	2	2	2	2	1	2	**19**	2	2	1	2	3	2	2	2	1	**18**
86	Puerta Cortafuego	3	4	2	2	4	4	2	4	2	**27**	1	1	1	1	2	1	4	2	4	**15**

Anexo 3: Evaluación por Juicio de Expertos

CARTA DE PRESENTACIÓN

Señor:

MARLON FRANK ACUÑA BENITES

Presente

Asunto: **VALIDACION DE INSTRUMENTOS A TRAVES DE JUICIO DE EXPERTO.**

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa Académico de Maestría en Ingeniería de Sistemas con Mención en Tecnologías de la Información de la Escuela de Posgrado de la Universidad Cesar Vallejo, en la sede Lima Norte Periodo 202302, requiero validar los instrumentos con los cuales se recogerá información necesaria para poder desarrollar mi investigación y con la que sustentaré mis competencias investigativas en la experiencia curricular de diseño y desarrollo del trabajo de investigación.

Las variables que tiene mi tesis son: **ISO 27001 y Gestión de vulnerabilidades,** siendo imprescindible contar con la aprobación de docentes expertos para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación que le hago llegar contiene:

- Carta de presentación.
- Formato de validación
- Certificado de validez de contenido de los instrumentos.

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,

Firma
Manuel Eleodoro Gil Miranda
DNI: 43692241

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento FICHA DE DATOS, y así poder medir las variables ISO 27001 y Gestión de vulnerabilidades. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Marlon Frank Acuña Benites	
Grado profesional:	Maestría ( )	Doctor (**X**)
Área de formación académica:	Clínica ( ) Educativa ( )	Social () Organizacional ( )
Áreas de experiencia profesional:	Educación	
Institución donde labora:	Universidad Cesar Vallejo Sede Lima Norte	
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (**x**)	
Experiencia en Investigación: (si corresponde)		

2. Propósito de la evaluación

Validar el contenido del instrumento, por juicio de expertos

Dimensiones del instrumento:

Variable del Instrumento: **ISO 27001**

Dimensión	Indicadores	Detalle
D1. Confidencialidad	1. Acceso Libre 2.Restringido 3.Protegida	Hace referencia a que la información no esté disponible, no se lea o no sea conocida por terceros o agentes no autorizadas.
D2. Integridad	1.Exacto 2.Fiable 3. Completo	Se indica que la información es veraz, y no ha sido manipulada, alterada o modificada indebidamente por personas no autorizadas.
D3. Disponibilidad	1.Un Dia 2.Una Semana 3. Un Mes	Consiste en que la información se encuentre disponible cuando se requiera.

Escala	Definición	Métrica de los activos Informáticos
Ordinal	Los activos tienen sus atributos, que se diferencian en el estado, en vocablos de seguridad, hace referencia a los niveles de los subestados, confidencialidad, disponibilidad e integridad.	1=Muy bajo, 2=Bajo, 3=Medio, 4=Alto, 5=Muy Alto

Variable del Instrumento: **Gestión de vulnerabilidades**

Dimension	Indicadores	Detalle
D1. Identificar	1. Vector de acceso. 2. Complejidad de acceso 3. Autenticación	El paso de identificación implica descubrir vulnerabilidades en el entorno, a través de escaneos automatizados, prueba de penetración e incluso informes de seguridad proporcionados por fabricantes de software y hardware.
D2. Detectar	1. Explotabilidad 2. Nivel de Remediación 3. Reporte de confianza	Daño potencial que puede causar una explotación de la vulnerabilidad y determinar con qué facilidad un atacante podría explotarla.
D3. Corregir	1. Daño potencial colateral 2. Distribución de objetivos 3. Requerimientos de C, I, D	Aplicación de parches de seguridad, actualizaciones de software, configuraciones mejoradas, entre otras medidas.

Escala	Definición	Métricas de la Gestión de Vulnerabilidades
Intervalo	Evaluar la gravedad de una vulnerabilidad, se utiliza el estándar del sector **"CVSS - Common Vulnerability Scoring System"**. Se determina una puntuación global de 0 a 10 a partir de las métricas de puntuación base.	Muy Bajo: 0 Bajo: [0.1- 3.9] Medio: [4.0 - 6.9] Alto: [7.0 - 8.9] Muy Alto: [9.0 - 10.00]

CERTIFICADO DE VALIDEZ CONTENIDO DEL INSTRUMENTO

- Primera dimensión: **CONFIDENCIALIDAD**
- Objetivos de la Dimensión: Determinar el valor del activo informático y clasificar si su acceso puede ser libre, restringida, o protegida.

Indicadores de las tres Dimensiones	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	
Acceso Libre				x				x				x	
Acceso Restringido				x				x				x	
Acceso Protegido				x				x				x	

- Segunda dimensión: **INTEGRIDAD**
- Objetivos de la Dimensión: Determinar si los datos mantienen su exactitud, fiabilidad y completitud.

Indicadores de las tres Dimensiones	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	
Exactitud				x				x				x	
Fiabilidad				x				x				x	
Completitud				x				x				x	

- Tercera dimensión: **DISPONIBILIDAD**
- Objetivos de la Dimensión: Identificar si el activo informático puede estar disponible por un día, hasta por una semana, o hasta por un mes.

Indicadores de las tres Dimensiones	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	
Un día				X				X				X	
Una semana				X				X				X	
Un mes				X				X				X	

- Cuarta dimensión: **IDENTIFICAR**
- Objetivos de la Dimensión: Evaluación de los activos informáticos, documentación, Vector de acceso, Complejidad de acceso, Autenticación

Indicadores	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	
Vector de acceso				X				X				X	
Complejidad de acceso				X				X				X	
Autenticación				X				X				X	

- Quinta dimensión: **DETECTAR**
- Objetivos de la Dimensión: Analís, monitoreo, Explotabilidad, Nivel de Remediación, Reporte de confianza

Indicadores	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	
Explotabilidad				X				X				X	
Nivel de remediación				X				X				X	
Reporte de Confianza				X				X				X	

- Sexta dimensión: **CORREGIR**
- Objetivos de la Dimensión: Reparar completamente una vulnerabilidad, Remediar, Mitigar, Aceptar, Daño potencial colateral, Distribución de objetivos, Requerimientos de confidencialidad, integridad y disponibilidad

Indicadores	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel	
Daño potencial colateral				X				X				X	
Distribución de objetivos				X				X				X	
Requerimientos de CID				X				X				X	

CERTIFICADO DE VALIDEZ CONTENIDO DEL INSTRUMENTO

Observaciones (precisar si hay suficiencia): _____

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

Apellidos y nombres del juez evaluador: MARLON ACUÑA BENITES

DNI: 42097456

Especialidad del validador: Ing. De Sistemas /Investigador

10 de diciembre del 2023

[1]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2]**Coherencia:** El ítem corresponde al concepto teórico formulado.
[3]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

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

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Anexo 4: Propuesta de Formato de Política de Gestión de Vulnerabilidades

Entidad Publica Geocientifica	**Política de Gestión Vulnerabilidades (SGSI)**	**Fecha:**
Clasificación: Público	**Código:**	**Versión:**

1. INTRODUCCIÓN

El objetivo de crear la política de gestión de vulnerabilidades para la Entidad Publica Geocientifica, es establecer los compromisos y el marco general (legal y regulatorio) para gestionar los riesgos asociados a la seguridad de la información durante la prestación de los servicios ofrecidos a fin identificar las vulnerabilidades y amenazas para los activos de información.

2. DEFINICIONES

Activos de información: Todo aquello que es o contiene información que es de valor para la Entidad Publica Geocientifica. Por ejemplo: documentos digitales o físicos, servicios, aplicaciones, equipos, entre otros activos que la organización valora y protege de cualquier vulnerabilidad que amenaza con la divulgación, indisponibilidad y pérdida de integridad de la información.

Amenazas: Evento que puede afectar adversamente la operación de las empresas y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.

Riesgos: Las amenazas de ataques y las vulnerabilidades de la tecnología. Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de los activos de información.

Vulnerabilidad: Debilidad de un sistema de información que se encuentra en riesgo la seguridad de la información.

3. ALCANCE

Los activos de información involucrados en la prestación de los servicios ofrecidos por la Entidad Publica Geocientifica.

4. OBJETIVOS

a) Definir y formalizar una política alineada a los marcos legales (contrato entre la Entidad Publica Geocientifica y sus clientes y proveedores), que ayudarán a la empresa a mitigar los riesgos de seguridad de la información en la relación a las amenazas, vulnerabilidades y riesgos de los activos de información.

b) Establecer compromisos con la finalidad de monitorear y prevenir las amenazas, identificar y remediar las vulnerabilidades, así como establecer los riesgos sobre los activos de información involucrados en la prestación de los servicios ofrecidos por la Entidad Publica Geocientifica.

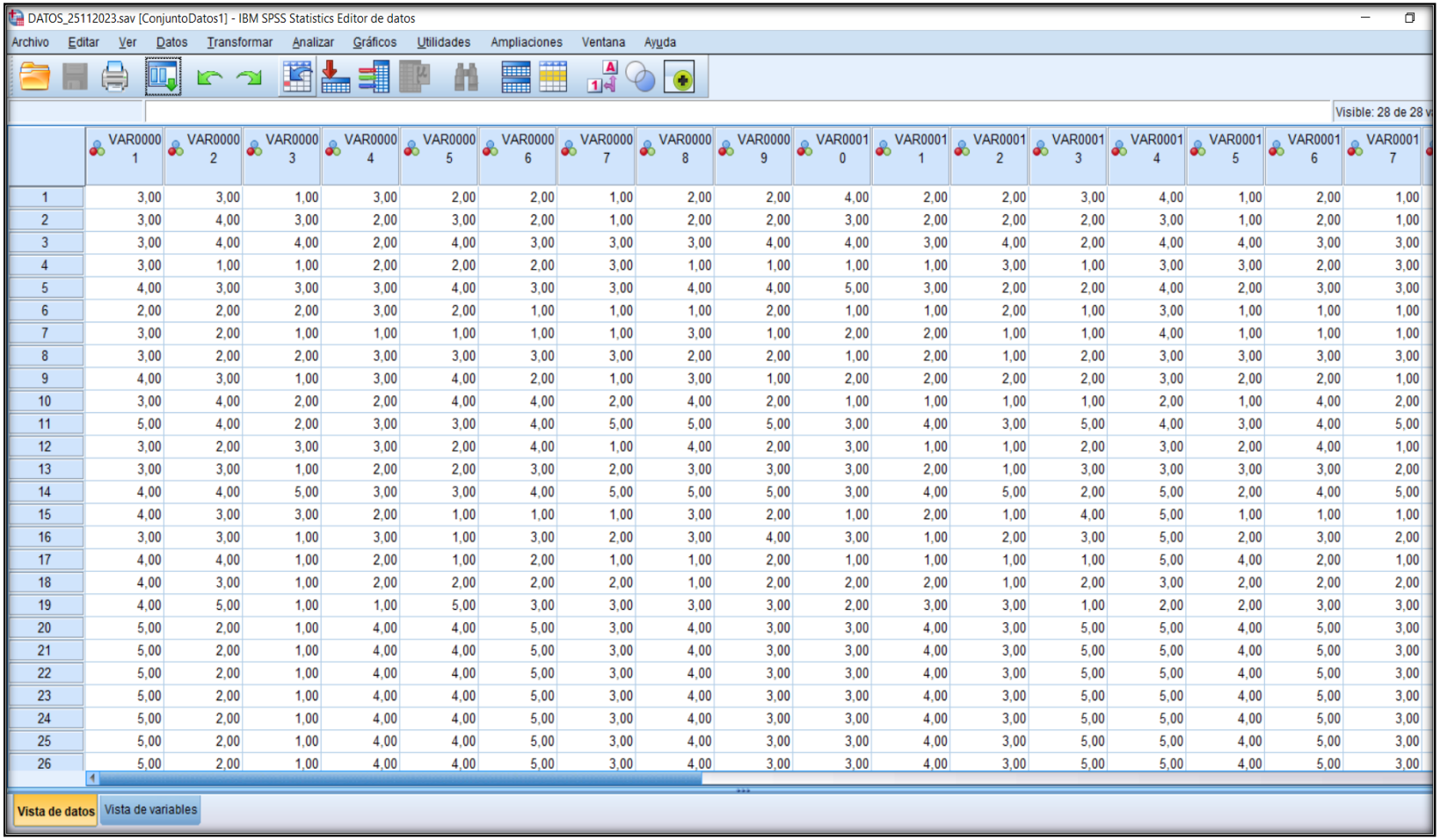
5. POLÍTICA DE GESTIÓN DE AMENAZAS, VULNERABILIDADES Y RIESGOS

El CSIRT realiza la mitigación de los riesgos de seguridad de la información asociados a los activos de información durante la prestación de los servicios ofrecidos por la Entidad Publica Geocientifica, a fin prevenir daños sobre los activos de información.

Para la ejecución adecuada en materia de seguridad de la información, el CSIRT asume los siguientes compromisos:

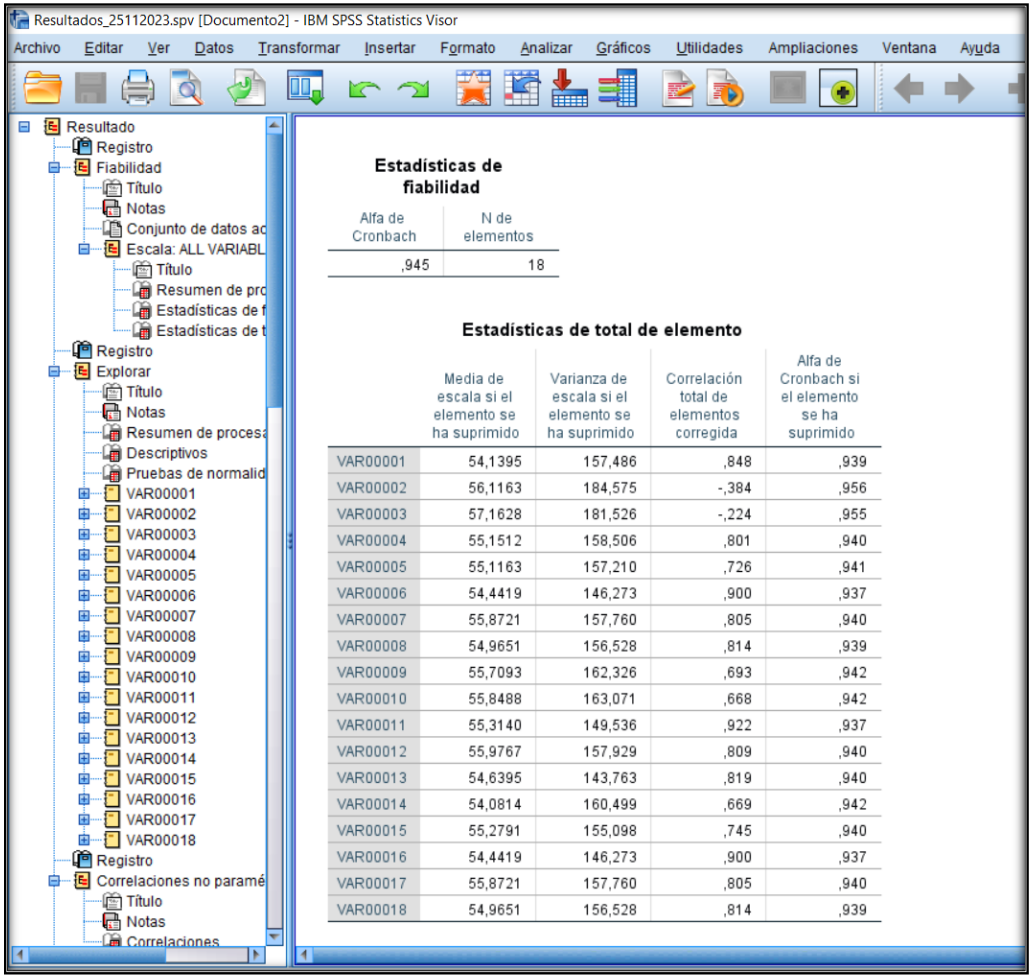
1. Difundir la política de gestión de amenazas, vulnerabilidades y riesgos.
2. Identificar, evaluar y controlar permanente los riesgos, amenazas y vulnerabilidades que puedan afectar la prestación de los servicios ofrecidos.
3. Elaborar planes de seguridad de la información para la prevención de riesgos, amenazas y vulnerabilidades.
4. Asegurar que el personal no deba explotar los puntos vulnerables o las deficiencias en la seguridad en los activos de información, para dañar, eliminar y/o modificar los programas o la información.
5. Asegurar que todos los programas conectados a internet deben estar sujetos a una verificación automática de riesgo, esto se lleva a cabo a través de programa para identificación de vulnerabilidades.
6. Capacitar al personal para identificar información que puede ser un riesgo y asegurar una respuesta adecuada ante una amenaza.
7. Asegurar que la administración de las redes cuente con protocolos de seguridad para la detección de intrusos durante la prestación de los servicios ofrecidos.
8. Concientizar para la no divulgación de información sobre las vulnerabilidades de los activos de información a personas no autorizadas.
9. Reportar cualquier daño o pérdida de los activos de información a la CSIRT.
10. Asegurar que el proveedor del CSIRT que maneja información sobre los activos de información, comunique la ocurrencia de incidentes que no permitan una prestación del servicio de forma adecuada.
11. Llevar periódicamente una revisión externa e independiente de los controles de los activos de información.
12. Documentar todas las excepciones que se hayan aprobado al cumplimiento de la presente política.

Anexo 5: Evidencias de Base de datos en SPSS



	VAR00001	VAR00002	VAR00003	VAR00004	VAR00005	VAR00006	VAR00007	VAR00008	VAR00009	VAR00010	VAR00011	VAR00012	VAR00013	VAR00014	VAR00015	VAR00016	VAR00017
1	3,00	3,00	1,00	3,00	2,00	2,00	1,00	2,00	2,00	4,00	2,00	2,00	3,00	4,00	1,00	2,00	1,00
2	3,00	4,00	3,00	2,00	3,00	2,00	1,00	2,00	2,00	3,00	2,00	2,00	2,00	3,00	1,00	2,00	1,00
3	3,00	4,00	4,00	2,00	4,00	3,00	3,00	3,00	4,00	4,00	3,00	4,00	2,00	4,00	4,00	3,00	3,00
4	3,00	1,00	1,00	2,00	2,00	2,00	3,00	1,00	1,00	1,00	1,00	3,00	1,00	3,00	3,00	2,00	3,00
5	4,00	3,00	3,00	3,00	4,00	3,00	3,00	4,00	4,00	5,00	3,00	2,00	2,00	4,00	2,00	3,00	3,00
6	2,00	2,00	2,00	3,00	2,00	1,00	1,00	1,00	2,00	1,00	1,00	2,00	1,00	3,00	1,00	1,00	1,00
7	3,00	2,00	1,00	1,00	1,00	1,00	1,00	3,00	1,00	2,00	2,00	1,00	1,00	4,00	1,00	1,00	1,00
8	3,00	2,00	2,00	3,00	3,00	3,00	3,00	2,00	2,00	1,00	2,00	1,00	2,00	3,00	3,00	3,00	3,00
9	4,00	3,00	1,00	3,00	4,00	2,00	1,00	3,00	1,00	2,00	2,00	2,00	2,00	3,00	2,00	2,00	1,00
10	3,00	4,00	2,00	2,00	4,00	4,00	2,00	4,00	2,00	1,00	1,00	1,00	1,00	2,00	1,00	4,00	2,00
11	5,00	4,00	2,00	3,00	3,00	4,00	5,00	5,00	5,00	3,00	4,00	3,00	5,00	4,00	3,00	4,00	5,00
12	3,00	2,00	3,00	3,00	2,00	4,00	1,00	4,00	2,00	3,00	1,00	1,00	2,00	3,00	2,00	4,00	1,00
13	3,00	3,00	1,00	2,00	2,00	3,00	2,00	3,00	3,00	3,00	2,00	1,00	3,00	3,00	3,00	3,00	2,00
14	4,00	4,00	5,00	3,00	3,00	4,00	5,00	5,00	5,00	3,00	4,00	5,00	2,00	5,00	2,00	4,00	5,00
15	4,00	3,00	3,00	2,00	1,00	1,00	1,00	3,00	2,00	1,00	2,00	1,00	4,00	5,00	1,00	1,00	1,00
16	3,00	3,00	1,00	3,00	1,00	3,00	2,00	3,00	4,00	3,00	1,00	2,00	3,00	5,00	2,00	3,00	2,00
17	4,00	4,00	1,00	2,00	1,00	2,00	1,00	1,00	2,00	1,00	1,00	1,00	1,00	5,00	4,00	2,00	1,00
18	4,00	3,00	1,00	2,00	2,00	2,00	2,00	1,00	2,00	2,00	2,00	1,00	2,00	3,00	2,00	2,00	2,00
19	4,00	5,00	1,00	1,00	5,00	3,00	3,00	3,00	3,00	2,00	3,00	3,00	1,00	2,00	2,00	3,00	3,00
20	5,00	2,00	1,00	4,00	4,00	5,00	3,00	4,00	3,00	3,00	4,00	3,00	5,00	5,00	4,00	5,00	3,00
21	5,00	2,00	1,00	4,00	4,00	5,00	3,00	4,00	3,00	3,00	4,00	3,00	5,00	5,00	4,00	5,00	3,00
22	5,00	2,00	1,00	4,00	4,00	5,00	3,00	4,00	3,00	3,00	4,00	3,00	5,00	5,00	4,00	5,00	3,00
23	5,00	2,00	1,00	4,00	4,00	5,00	3,00	4,00	3,00	3,00	4,00	3,00	5,00	5,00	4,00	5,00	3,00
24	5,00	2,00	1,00	4,00	4,00	5,00	3,00	4,00	3,00	3,00	4,00	3,00	5,00	5,00	4,00	5,00	3,00
25	5,00	2,00	1,00	4,00	4,00	5,00	3,00	4,00	3,00	3,00	4,00	3,00	5,00	5,00	4,00	5,00	3,00
26	5,00	2,00	1,00	4,00	4,00	5,00	3,00	4,00	3,00	3,00	4,00	3,00	5,00	5,00	4,00	5,00	3,00

Anexo 6: Evidencias de cálculo de estadísticas de fiabilidad en programa SPSS



Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,945	18

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
VAR00001	54,1395	157,486	,848	,939
VAR00002	56,1163	184,575	-,384	,956
VAR00003	57,1628	181,526	-,224	,955
VAR00004	55,1512	158,506	,801	,940
VAR00005	55,1163	157,210	,726	,941
VAR00006	54,4419	146,273	,900	,937
VAR00007	55,8721	157,760	,805	,940
VAR00008	54,9651	156,528	,814	,939
VAR00009	55,7093	162,326	,693	,942
VAR00010	55,8488	163,071	,668	,942
VAR00011	55,3140	149,536	,922	,937
VAR00012	55,9767	157,929	,809	,940
VAR00013	54,6395	143,763	,819	,940
VAR00014	54,0814	160,499	,669	,942
VAR00015	55,2791	155,098	,745	,940
VAR00016	54,4419	146,273	,900	,937
VAR00017	55,8721	157,760	,805	,940
VAR00018	54,9651	156,528	,814	,939

Anexo 7: **Propuesta de Cronograma de actividades de gestión de vulnerabilidades**

N°	Gestión de Vulnerabilidades	Primer Semestre		Segundo Semestre	
		Inicio	Fin	Inicio	Fin
1	Equipamiento de Infraestructura del Centro de Datos	Mes 2	Mes 5	Mes 9	Mes 12
2	Análisis de código de seguro de aplicativos informáticos o sistemas de información	Mes 1	Mes 5	Mes 8	Mes 12
3	Actualización de parches de Seguridad de sistemas operativos	Mes 1	Mes 5	Mes 8	Mes 12
4	Sistemas de telecomunicaciones y telefonía	Mes 2	Mes 5	Mes 9	Mes 12
5	Equipos de Seguridad Perimetral	Mes 1	Mes 5	Mes 8	Mes 11

Anexo 8: Distribución Estadística de severidad CVSS a lo largo del tiempo

La elección de BAJO, MEDIO y ALTO es basada en la puntuación CVSS V2 Base.