UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS:

Propuesta de plan de seguridad informática para mejorar el nivel de seguridad de la información, dirección de salud "Virgen de Cocharcas", provincia de Chincheros, 2024

Para optar el título profesional de:
INGENIERO DE SISTEMAS

PRESENTADO POR:
Bach. Marco Antonio HUARACA HUARHUACHI

ASESOR:
Dr. Efraín Elías PORRAS FLORES

AYACUCHO - PERÚ

2026

DEDICATORIA

A mis padres: Magdalena y Silvano con profundo agradecimiento, cuya influencia y apoyo han sido fundamentales en mi vida. A mi querido hijo, Luis Antonell, mi gran inspiración y mi mayor motivación para alcanzar mis metas.

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a la Universidad Nacional de "San Cristóbal de Huamanga" por ser el pilar fundamental en mi camino hacia la formación profesional. A todos los distinguidos maestros de la Escuela Profesional de Ingeniería de Sistemas, les agradezco por compartir sus vastos conocimientos y experiencias, no solo en el ámbito académico, sino también en el desarrollo personal y profesional. Su dedicación y apoyo han sido el motor que impulsó mi crecimiento y aprendizaje, y por ello siempre estaré agradecido.

Con gran estima, expreso mi más profundo agradecimiento al Dr. Efraín Elías Porras Flores por su destacada gestión y orientación en la realización de este trabajo de investigación. Su constante apoyo y valiosas enseñanzas fueron cruciales para guiar cada etapa de este proyecto hasta su conclusión. Agradezco sinceramente su dedicación y compromiso, los cuales han sido fundamentales en mi desarrollo académico y profesional.

RESUMEN

La Dirección de Salud “Virgen de Cocharcas” de la provincia de Chincheros carecía de un plan formal de seguridad informática, enfrentando incidentes que comprometían la confidencialidad, integridad y disponibilidad de la información institucional. El objetivo fue desarrollar una propuesta de plan de seguridad informática basada en la norma ISO/IEC 27002:2022 para mejorar el nivel de seguridad de la información. Se empleó un diseño preexperimental con mediciones pretest y postest en una población censal de 60 trabajadores, utilizando un cuestionario tipo Likert de 30 ítems validado por juicio de expertos (V de Aiken = 0.97) con confiabilidad alta (alfa de Cronbach = 0.906). El plan implementó 12 controles de la norma ISO/IEC 27002:2022 distribuidos en cuatro dominios: organización, personas, objetos físicos y tecnología. Los resultados evidenciaron una mejora significativa: la prueba t de Student mostró una diferencia de medias de 26.95 puntos (t = 15.46, p = 0.000) con tamaño de efecto grande (d de Cohen = 1.996). La concienciación en seguridad presentó el mayor impacto (r = –0.860), seguida por políticas y procedimientos (r = –0.798), controles de seguridad (r = –0.460) y norma de seguridad (r = –0.313). Se concluye que la propuesta mejora significativamente el nivel de seguridad de la información, siendo la concienciación del personal el componente más efectivo.

Palabras clave: Seguridad informática, plan de seguridad informática, políticas de seguridad, controles de seguridad, norma ISO/IEC 27002:2022.

ABSTRACT

The Health Directorate “Virgen de Cocharcas” in the province of Chincheros lacked a formal cybersecurity plan, facing incidents that compromised the confidentiality, integrity, and availability of institutional information. The objective was to develop a cybersecurity plan proposal based on the ISO/IEC 27002:2022 standard to improve the level of information security. A pre-experimental design with pretest and posttest measurements was employed with a census population of 60 workers, using a 30-item Likert-type questionnaire validated by expert judgment (Aiken’s V = 0.97) with high reliability (Cronbach’s alpha = 0.906). The plan implemented 12 controls from the ISO/IEC 27002:2022 standard distributed across four domains: organization, people, physical objects, and technology. Results showed a significant improvement: the paired t-test revealed a mean difference of 26.95 points (t = 15.46, p = 0.000) with a large effect size (Cohen’s d = 1.996). Security awareness showed the greatest impact (r = –0.860), followed by policies and procedures (r = –0.798), security controls (r = –0.460), and the security standard (r = –0.313). It is concluded that the proposal significantly improves the level of information security, with staff awareness being the most effective component.

Keywords: Cybersecurity, information security plan, security policies, security controls, ISO/IEC 27002:2022 standard

INDIICE

Lista de tablas

Lista de figuras

I. INTRODUCCIÓN

1.1. Planteamiento del problema

La Dirección de Salud Virgen de Cocharcas enfrenta desafíos críticos en materia de seguridad informática. Como entidad responsable de 48 establecimientos de salud en la provincia de Chincheros, esta institución gestiona información sensible relacionada con atenciones médicas, administración, logística y datos del personal asistencial y administrativo.

Desde enero de 2023, se han reportado incidentes de seguridad que afectaron temporalmente los sistemas administrativos y de coordinación para el seguimiento de programas presupuestales y estrategias de salud. Estos incidentes impactaron la capacidad operativa de la sede central y de los cuatro establecimientos de salud principales de su jurisdicción (Hospital Chincheros, Centro de Salud Uripa, Centro de Salud Huaccana y Centro de Salud Ocobamba), los cuales concentran del 50 % del flujo de datos sensibles vinculados a la gestión y monitoreo de servicios asistenciales.

Entre las causas identificadas figura que la falta de mantenimiento preventivo de equipos ha ocasionado varias interrupciones no programadas del servidor principal en el último semestre, afectando directamente la disponibilidad de información crítica. Asimismo, el desconocimiento del personal sobre protocolos de seguridad ha derivado en prácticas como compartir credenciales de acceso y utilizar dispositivos no autorizados, comprometiendo la confidencialidad de datos protegidos por ley.

Las vulnerabilidades identificadas representan un riesgo directo para la continuidad asistencial, pudiendo ocasionar retrasos en la atención médica, errores en la administración de tratamientos y exposición indebida de información sensible de pacientes. Según el Reporte de Ciberseguridad en el Sector Salud 2023 del MINSA, las brechas de seguridad en establecimientos de salud (como la DISA Virgen de Cocharcas) pueden incrementar los tiempos de respuesta ante emergencias hasta en un 40%.

Frente a este escenario, se propone desarrollar una propuesta de plan basado en la norma ISO 27002:2022, que incluirá la identificación de controles de seguridad adecuados, el diseño de políticas y procedimientos de seguridad, y fomentar una cultura de concienciación entre el personal. Con esta propuesta, se abordarán las amenazas cibernéticas emergentes y se mitigarán los riesgos asociados a la seguridad informática.

1.2. Formulación del problema

1.2.1. Problema general

¿Cómo es el plan de seguridad informática que mejora el nivel de seguridad de la información en la Dirección de Salud Virgen de Cocharcas en la provincia de Chincheros, 2024?

1.2.2. Problemas específicos

a. ¿Cómo es la norma de seguridad que mejora el nivel de seguridad de la información?
b. ¿Cómo son los controles de seguridad que mejora el nivel de seguridad de la información?
c. ¿Cómo son las políticas y procedimientos de seguridad que mejora el nivel de seguridad de la información?
d. ¿Cómo es la concienciación en seguridad que mejora el nivel de seguridad de la información?

1.3. Formulación de los objetivos

1.3.1. Objetivo general

Desarrollar una propuesta de plan de seguridad informática que mejora el nivel de seguridad de la información en la Dirección de Salud Virgen de Cocharcas en la provincia de Chincheros, 2024.

1.3.2. Objetivos específicos

a. Identificar la norma de seguridad que mejora el nivel de seguridad de la información.
b. Identificar los controles de seguridad que mejora el nivel de seguridad de la información.
c. Diseñar las políticas y procedimientos de seguridad que mejora el nivel de seguridad de la información.
d. Diseñar la concienciación en seguridad que mejora el nivel de seguridad de la información.

1.4. Justificación de la investigación

1.4.1. Justificación teórica

Este estudio se fundamenta en el modelo de gestión de riesgos de la norma ISO 27002:2022, particularmente en su enfoque actualizado de controles organizativos, personales, físicos y tecnológicos. A pesar de la existencia de investigaciones sobre

seguridad informática en el sector público peruano (Vílchez Guevara, 2023) Y (Rumiche Huamani, 2021), existe un vacío significativo en la adaptación de estos estándares a instituciones de salud en entornos rurales con recursos limitados. La presente investigación busca generar conocimiento aplicado que vincule los principios teóricos de la seguridad de la información con las características operativas de establecimientos de salud en regiones andinas.

1.4.2. Justificación practica

Esta investigación propone un plan de seguridad informática adaptable a las circunstancias particulares de la Dirección de Salud “Virgen de Cocharcas”, basado en controles prioritarios de la norma ISO 27002:2022 que responden a los riesgos más críticos identificados. Presenta un marco metodológico robusto y un conjunto de herramientas prácticas que otras instituciones de salud pueden adaptar según sus necesidades específicas y recursos disponibles.

La implementación del plan de seguridad informática generará mejoras como: reducir la cantidad de incidentes relacionados con accesos no autorizados, errores humanos y pérdida de datos. Asimismo, optimizar los tiempos de respuesta y recuperación ante fallos del sistema, gracias a la implementación de respaldos automáticos y protocolos de atención de incidentes. El cumplimiento de los controles básicos establecidos por la norma ISO 27002:2022. Para los coordinadores de programas y estrategias de salud, esto se traducirá en una mayor disponibilidad y confiabilidad de los sistemas informáticos utilizados para el seguimiento de indicadores, la gestión de información de establecimientos y la coordinación con el personal asistencial, reduciendo errores en la consolidación de datos y facilitando la toma de decisiones.

El personal administrativo, por su parte, se beneficiará con procesos más eficientes y seguros en áreas clave como la gestión de recursos humanos, la planificación presupuestal y los procesos logísticos, lo cual fortalecerá la capacidad operativa de la institución. En conjunto, estos beneficios fortalecerán la capacidad institucional para garantizar el soporte necesario al personal asistencial, lo que indirectamente se traduce en mejores condiciones para una atención de calidad en los establecimientos de salud.

Este estudio se alinea con la Ley N.° 29733 de Protección de Datos Personales, la Directiva Administrativa N.° 294-MINSA/2020/OGTI sobre el uso de tecnologías de la información en el sector salud, y la Resolución Ministerial N.° 214-2018/MINSA relativa

a la gestión de historias clínicas. Dado que la DISA “Virgen de Cocharcas” gestiona información sensible relacionada con estrategias de salud, seguimiento de programas presupuestales y coordinación con los establecimientos de salud de su jurisdicción, el plan propuesto contribuirá directamente al cumplimiento normativo, fortaleciendo los mecanismos de seguridad informática necesarios para garantizar una gestión institucional eficiente, segura y alineada con el marco legal vigente.

1.4.3. Justificación metodológica

En cuanto a la justificación metodológica, la elección de la norma ISO/IEC 27002:2022 como marco de referencia se basa en su reconocimiento internacional y su enfoque práctico y estructurado para la gestión de la seguridad de la información. El uso de esta norma como guía metodológica permitirá llevar a cabo un análisis detallado de los propósitos y directrices establecidos en la misma, así como establecer e implementar adecuadamente controles básicos de seguridad informática y desarrollar políticas claras y actualizadas de seguridad de la información. Además, de utilizar técnicas estadísticas y herramientas de procesamiento y análisis de datos para evaluar la eficacia de la propuesta de plan de seguridad informática.

1.5. Delimitación de la investigación

Delimitación temporal: La investigación analiza la situación de la seguridad de la información en la Dirección de Salud “Virgen de Cocharcas” durante el año 2024, comprendiendo las mediciones pretest y postest realizadas antes y después de la aplicación de la propuesta de plan de seguridad informática.

Delimitación espacial: El estudio se circunscribe a la sede central de la Dirección de Salud “Virgen de Cocharcas”, ubicada en la provincia de Chincheros, departamento de Apurímac, Perú, institución responsable de la coordinación de 48 establecimientos de salud de su jurisdicción.

Delimitación temática: La investigación se enfoca exclusivamente en la seguridad de la información desde la perspectiva de la norma ISO/IEC 27002:2022, abordando cuatro dimensiones específicas: norma de seguridad, controles de seguridad, políticas y procedimientos de seguridad, y concienciación en seguridad. No se incluyen aspectos relacionados con la seguridad física de las personas, la seguridad patrimonial ni la evaluación de riesgos clínicos.

Delimitación social: Las unidades de análisis comprenden los 60 trabajadores de la

DISA “Virgen de Cocharcas” (38 del área administrativa y 22 de las coordinaciones de salud), así como 52 activos informáticos.

1.6. Limitaciones de la investigación

El alcance temporal de esta investigación implica un enfoque selectivo en los controles de seguridad más relevantes para el contexto de la DISA, priorizando aquellos de mayor impacto y factibilidad de implementación. Esta aproximación permite desarrollar un modelo de intervención efectiva, concentrándose en soluciones de alta prioridad que generen impacto significativo. La falta de acceso a ciertos datos o información detallada podría restringir la capacidad de realizar un análisis completo de la seguridad informática. Es importante considerar que, al restringirnos a investigar una institución de salud, los resultados obtenidos pueden no ser representativos o aplicables a otras instituciones de diferentes sectores.

II. MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales

Moya (2023), ante la ausencia de un plan formal de seguridad de la información y la falta de roles definidos en la Unidad de Tecnologías de la Información de la Empresa Pública Municipal de Agua Potable y Alcantarillado de Ambato (Ecuador), se propuso diseñar un plan de seguridad informática basado en la norma ISO/IEC 27001:2013 y la metodología MAGERIT. El estudio empleó un enfoque cualitativo, analizando políticas, procesos y controles existentes para establecer una línea base de seguridad, complementado con métodos estadísticos para verificar la hipótesis y medir el impacto del proyecto. Los resultados incluyeron la elaboración del plan, la definición de una política de seguridad, la asignación de roles y responsabilidades, y la evidencia de un impacto positivo en la protección de los activos de información. Se concluyó que la implementación del plan mejoró la seguridad de la información de la empresa, destacando la necesidad de fomentar una cultura de seguridad y realizar evaluaciones periódicas para mantener la eficacia de los controles.

Delgado Ojeda (2024), identificando que la empresa Airmaxtelecom Soluciones Tecnológicas S.A. (Ecuador) carecía de un sistema de gestión estructurado para la seguridad de la información, tuvo como propósito diseñar un SGSI basado en las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022. La metodología fue de tipo aplicada con enfoque mixto, empleando entrevistas, encuestas y análisis documental para diagnosticar vulnerabilidades y evaluar los riesgos existentes en la infraestructura

tecnológica. Los resultados evidenciaron múltiples vulnerabilidades en los controles de acceso, la gestión de incidentes y la protección de datos, y se propuso un conjunto de 93 controles alineados con la versión actualizada de la norma. Se concluyó que la adopción de la ISO/IEC 27002:2022, con sus cuatro temas reorganizados (organización, personas, objetos físicos y tecnología), resulta más práctica y eficaz para empresas del sector tecnológico, facilitando la implementación y el seguimiento de los controles de seguridad.

De La Torre Yamberla (2024), ante la limitada disponibilidad de los servicios tecnológicos y la inexistencia de controles formales de seguridad en la Cooperativa de Ahorro y Crédito Imbacoop Ltda. (Ecuador), se propuso desarrollar un plan de SGSI aplicando el estándar ISO/IEC 27001 para fortalecer la disponibilidad de los servicios. Utilizó una metodología de investigación aplicada con diseño preexperimental, realizando un diagnóstico inicial de la situación de seguridad, evaluación de riesgos mediante MAGERIT y diseño de controles específicos para el contexto financiero cooperativo. Los resultados mostraron una mejora significativa en los indicadores de disponibilidad de los servicios críticos y una reducción de los tiempos de interrupción no planificada. Se concluyó que la implementación del SGSI basado en ISO 27001 es viable y necesaria para las cooperativas de ahorro y crédito, contribuyendo a garantizar la continuidad operativa y la confianza de los socios en los servicios financieros digitales.

Carrillo García (2023), ante el creciente número de incidentes de seguridad en operaciones financieras digitales y la falta de análisis formalizados de seguridad en una empresa dedicada a transacciones interbancarias en Ecuador, se propuso realizar un análisis integral de seguridad de la información aplicando la norma ISO/IEC 27001. La investigación adoptó un enfoque cuantitativo-descriptivo, evaluando los controles existentes mediante auditorías internas, encuestas al personal técnico y revisión documental de los procesos transaccionales. Los resultados revelaron deficiencias críticas en la gestión de accesos privilegiados, la monitorización de eventos y la respuesta ante incidentes, identificando brechas que podrían comprometer la integridad de las transacciones. Se concluyó que la aplicación de la norma ISO 27001 permite una evaluación sistemática de los riesgos en entornos financieros de alta criticidad, y que la implementación de los controles recomendados reduce significativamente la exposición a amenazas internas y externas.

Fuel Rodríguez (2024), considerando la necesidad de cumplir con la Ley Orgánica de

Protección de Datos Personales y la ausencia de un marco integrado de seguridad y privacidad en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega (Ecuador), se propuso implementar un sistema de protección de datos personales integrando los estándares ISO/IEC 27001:2022, ISO/IEC 27002:2022 e ISO/IEC 27701:2019 con el SGSI institucional. La metodología empleada fue de investigación aplicada, combinando el análisis de brechas (gap analysis) con la evaluación de riesgos de privacidad y la adecuación de los controles existentes a los nuevos requisitos normativos. Los resultados demostraron que la integración de los tres estándares ISO permitió una cobertura más completa de los requisitos legales y regulatorios, mejorando tanto la gestión de la seguridad como la protección de datos personales de los socios. Se concluyó que la convergencia entre ISO 27001, ISO 27002 e ISO 27701 constituye un enfoque eficiente para organizaciones financieras que deben cumplir simultáneamente con obligaciones de seguridad de la información y protección de datos personales.

2.1.2. Antecedentes nacionales

Vílchez (2023), ante la inexistencia de un plan de seguridad informática que protegiera de manera integral los activos tecnológicos de la Municipalidad Distrital de San Juan Bautista, se propuso elaborar un plan de seguridad informática conforme a la norma ISO/IEC 27002:2013. El estudio adoptó un enfoque cuantitativo con diseño descriptivo simple, tomando como muestra 680 activos informáticos y utilizando checklists, encuestas, entrevistas y fichas de observación para la recopilación de datos. Los resultados revelaron un nivel de riesgo bajo en los activos informáticos evaluados, pero con oportunidades de mejora en los controles preventivos y la capacitación del personal. Se concluyó que la implementación de un plan basado en ISO/IEC 27002:2013 contribuye significativamente al fortalecimiento de la seguridad informática en instituciones públicas, siendo replicable en entidades similares del sector gubernamental.

Abad y Cruz (2022), identificando deficiencias en la confidencialidad, integridad y disponibilidad de la información en la Unidad de Gestión Educativa Local (UGEL) Utcubamba, se propusieron mejorar la seguridad informática mediante la aplicación de la norma ISO/IEC 27002:2013. La investigación fue de tipo aplicada con diseño preexperimental, empleando una muestra de 18 empleados y cuestionarios como instrumento de recolección de datos, realizando mediciones pre y post intervención. Los resultados evidenciaron un incremento significativo en la seguridad informática: la confidencialidad mejoró de 2.95 a 59.00%, la integridad de 3.09 a 61.80% y la

disponibilidad de 3.25 a 65.00%. Se concluyó que la implementación de la norma ISO/IEC 27002:2013 fortaleció efectivamente los tres pilares de la seguridad de la información en la UGEL Utcubamba, recalcando la utilidad de este estándar en instituciones educativas públicas y la importancia de evaluaciones regulares para mitigar riesgos.

Rumiche (2021), ante la ausencia de una política interna de seguridad, la inexistencia de controles permanentes y el desconocimiento generalizado de estándares de seguridad en la Corte Superior de Justicia de Lima, se propuso identificar los riesgos y vulnerabilidades en los sistemas informáticos de la institución para fundamentar la necesidad de un plan de seguridad informática. El estudio empleó un enfoque descriptivo-diagnóstico, utilizando encuestas aplicadas al personal técnico y administrativo para recopilar información sobre fallos recurrentes y la situación real de la seguridad informática. Los resultados destacaron la ausencia total de una política interna de seguridad, la falta de controles permanentes de acceso y el desconocimiento de la norma ISO 27002:2013 por parte del personal. Se concluyó que es imperativo implementar un plan de seguridad informática que aborde políticas y estrategias específicas para mitigar los riesgos identificados y establecer una cultura de seguridad informática en la institución judicial.

Merino (2021), ante la insatisfacción del personal con las medidas de seguridad existentes y la ausencia de un plan formal de protección de la información en RANSA Comercial S.A. (Piura), se propuso investigar e implementar un plan de seguridad informática basado en la norma ISO/IEC 27001. La metodología fue cuantitativa y descriptiva, comprendiendo el análisis de la situación actual de seguridad, el diseño e implementación del plan, la evaluación de la satisfacción de los empleados y el análisis de la necesidad de una nueva propuesta. Los resultados indicaron que el 60% de los trabajadores encuestados manifestó insatisfacción con el sistema de seguridad vigente y el 80% consideró necesario un nuevo plan; tras la implementación, se registró una mejora en los indicadores de seguridad de la información. Se concluyó que la implementación de planes de seguridad informática basados en ISO 27001 es fundamental para las organizaciones del sector privado, siendo indispensable la participación activa de todos los empleados y la realización de evaluaciones regulares para la detección y reducción de riesgos.

Huallpa (2020), ante la alta exposición a riesgos de seguridad de la información y la insuficiencia de controles formales en la Dirección de Tecnologías de Información (DTI)

de la Universidad Nacional Micaela Bastidas de Apurímac (UNAMBA), se propuso mejorar la seguridad de la información mediante la implementación de un SGSI basado en la norma ISO/IEC 27001:2013. La investigación fue de tipo aplicada con diseño preexperimental y nivel explicativo, empleando el Método Deming (PDCA) y la Metodología MAGERIT III para el análisis y tratamiento de riesgos. Los resultados revelaron una reducción del 75% en los riesgos de seguridad identificados, un incremento del 41.23% en los controles de seguridad implementados y una mejora sustancial en el nivel de capacitación del personal en materia de seguridad. Se concluyó que la implementación del SGSI basado en ISO/IEC 27001:2013 mejoró significativamente la seguridad de la información en la DTI de la UNAMBA, enfatizando la importancia de instaurar una cultura de seguridad institucional y la aplicación del ciclo de mejora continua.

2.2. MARCO CONCEPTUAL

2.2.1. Plan de seguridad informática

De acuerdo con Radu Constantinescu (2006) Un plan de seguridad informática es un documento estratégico y completo que establece las políticas, objetivos y lineamientos que una organización adopta para proteger su información y sistemas tecnológicos. Este tipo de plan no solo aborda los aspectos técnicos, sino también los procedimientos y responsabilidades necesarias para mantener seguros los activos digitales. Entre sus componentes más importantes se encuentran los requisitos específicos de seguridad, los controles implementados y los mecanismos utilizados para asegurar la integridad de los datos, la confidencialidad de la información sensible y la disponibilidad de los servicios. Además, el plan contempla medidas para garantizar la continuidad operativa de la organización en situaciones de crisis o interrupciones imprevistas.

Según Bhaskar & Kapoor (2013) un plan de seguridad informática es el punto de partida para proteger los activos tecnológicos de una organización, ya que establece las políticas, objetivos y lineamientos a seguir. Sin embargo, su implementación no es un evento aislado, sino que da paso a la gestión de la seguridad informática, entendida como el conjunto de procesos permanentes que respaldan la estructura y los sistemas organizacionales frente a amenazas internas o externas, intencionales o accidentales. El objetivo central de esta gestión es preservar la confidencialidad, integridad y disponibilidad de la información. Además, se vincula directamente con la gestión de riesgos, al permitir identificar vulnerabilidades, aplicar controles y evaluar resultados

Para La Organización Internacional de Normalización (ISO), (2022) un compendio documentado que engloba políticas, procedimientos y prácticas predefinidas, destinado a gestionar de manera efectiva los riesgos inherentes a la seguridad de la información dentro de una institución. Este plan debe ser elaborado de manera que se adapte de manera precisa al entorno y las necesidades específicas de la organización en cuestión, considerando además las obligaciones legales y normativas que le son aplicables. De esta forma, se garantiza que el plan no solo sea pertinente y efectivo, sino también que cumpla con los estándares y regulaciones vigentes en materia de seguridad de la información.

2.2.2. Norma internacional ISO/IEC 27002

Altaos Group (2017) menciona que la norma ISO 27001 consta de 10 capítulos y un anexo que detalla 14 dominios de seguridad. Para complementarla, se desarrolló la ISO 27002, un estándar internacional para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La última versión de la norma es la ISO 27002:2022.

La ISO 27002 proporciona un conjunto detallado de prácticas que complementan los puntos clave de la ISO 27001. Estos estándares abordan tanto la ciberseguridad como la protección de la información en diversas situaciones, como posibles desastres que puedan destruir los datos de una empresa. Además, ofrece recomendaciones de mejores prácticas en la gestión de la seguridad de la información para todos los interesados y responsables.

2.2.3. Norma internacional ISO/IEC 27002:2022

Viteri Peñafiel (2022) resalta que la nueva versión de la norma ISO 27001:2022 mantiene en su mayoría la estructura y las cláusulas principales de la edición anterior, con algunos ajustes menores en los controles. La novedad más importante es la incorporación del ANEXO A, que presenta la norma ISO 27002:2022.
Esta actualización se centra en un enfoque combinado de prevención y detección en seguridad de la información, detallando 83 controles específicos. Aunque el número total de controles ha disminuido de 114 a 93, esto se debe a una reorganización y consolidación de los controles existentes, junto con la incorporación de 11 nuevos controles.

Viteri Peñafiel (2022) la ISO 27002:2022 destaca por su enfoque en los aspectos organizativos y del talento humano, reconociendo al individuo como el eslabón más

débil en la seguridad de la información. También aborda aspectos como la tipología de controles (preventivos, detectivos o correctivos) y su impacto en la confidencialidad, integridad o disponibilidad de la información. Además, incorpora conceptos reconocidos de ciberseguridad del marco del Instituto Nacional de Estándares y Tecnología (NIST), considera las capacidades operativas de la organización y subraya la importancia del análisis de riesgos, particularmente en áreas clave como gobernanza, resiliencia, defensa y protección. Los nuevos controles se centran principalmente en ciberseguridad y en fortalecer la resiliencia organizacional, tratando temas como la seguridad de la información en entornos de nube y la vigilancia de la seguridad física en las empresas.

Tabla 1

Temas ISO-27002:2022

TEMAS ISO 27002:2022	CONTROLES
A.5 Organización	37
A.6 Personas	8
A.7 Objetos físicos	14
A.8 Tecnología	34
Total, controles	**93**

Fuente: Viteri Peñafiel (2022)

A. Organización

Este aspecto aborda la manera en que una empresa estructura y formula directrices para resguardar su información crucial. Implica la creación de políticas de seguridad, la asignación de responsabilidades definidas y garantizar que todos los miembros comprendan cómo manejar la información de forma segura. (ISO/IEC 27002, 2022).

Tabla 2

Tema organización ISO-27002:2022

ORGANIZACION		
27002:2022	**CONTROL**	**TIPO DE CONTROL**
5.1	Políticas para la seguridad de la información	Preventivo
5.2	Roles y responsabilidades de seguridad de la información	Preventivo
5.3	Segregación de deberes	Preventivo
5.4	Responsabilidades de gestión (la dirección)	Preventivo
5.5	Contacto con las autoridades	P. Correctivo
5.6	Contacto con grupos de interés especial	P. Correctivo
5.7	Inteligencia de amenazas	P. Detectivo
5.8	Seguridad de la información en la gestión de proyectos	Preventivo
5.9	Inventario de información y otros activos asociados	Preventivo

5.10	Uso aceptable de información y otros activos asociados	Preventivo
5.11	Retorno de los activos	Preventivo
5.12	Clasificación de información	Preventivo
5.13	Etiquetado de información	Preventivo
5.14	Transferencia de información	Preventivo
5.15	Control de acceso	Preventivo
5.16	Gestión de identidad	Preventivo
5.17	Información de autenticación	Preventivo
5.18	Derechos de acceso	Preventivo
5.19	S. Inf. en las relaciones con los proveedores	Preventivo
5.20	Abordar la SI dentro de los acuerdos de proveedores	Preventivo
5.21	Gestión de la SI en la cadena de suministro de las TIC	Preventivo
5.22	Monitoreo, revisión y gestión de cambios de servicios de proveedores	Preventivo
5.23	S. Inf. para el uso de servicios en la nube	Preventivo
5.24	Gestión de incidentes de SI Planificación y preparación	Correctivo
5.25	Evaluación y decisión sobre eventos de SI	Detectivo
5.26	Respuesta a incidentes de seguridad de la información	Correctivo
5.27	Aprender de los incidentes de SI	Preventivo
5.28	Recopilación de evidencia	D. Correctivo
5.29	Seguridad de la información durante eventos disruptivos	Preventivo
5.30	Preparación para las TIC para la continuidad del negocio	P. Correctivo
5.31	Requisitos legales, legales, regulatorios y contractuales	Preventivo
5.32	Derechos de propiedad intelectual	Preventivo
5.33	Protección de registros	Preventivo
5.34	Privacidad y protección de PII	Preventivo
5.35	Revisión independiente de la seguridad de la información	P. Correctivo
5.36	Cumplimiento de las políticas, reglas y estándares para la SI	Preventivo
5.37	Procedimientos operativos documentados	Preventivo

Fuente: Viteri Peñafiel (2022)

B. Personas

En este contexto se discute la relevancia del factor humano en la protección de la información, reconociendo que el personal es un componente fundamental en la seguridad de los datos corporativos. Se refiere a cómo la empresa selecciona y capacita a su personal, garantizando que todos comprendan la importancia de salvaguardar la información y sepan cómo actuar ante cualquier eventualidad. (ISO/IEC 27002, 2022).

Tabla 3

Tema personas ISO-27002:2022

PERSONAS		
27002:2022	**CONTROL**	**TIPO DE CONTROL**
6.1	Selección	Preventivo
6.2	Términos y condiciones de empleo	Preventivo
6.3	Conciencia de seguridad, educación y capacitación de la información	Preventivo
6.4	Proceso Disciplinario	P. Correctivo
6.5	Responsabilidades después de la terminación o cambio de empleo	Preventivo
6.6	Acuerdos de confidencialidad o no divulgación	Preventivo
6.7	Trabajo remoto	Preventivo
6.8	Informes de eventos de seguridad de la información	Detectivo

Fuente: Viteri Peñafiel (2022)

C. Objetos físicos

Este tema se enfoca en resguardar elementos físicos, como instalaciones y dispositivos, con el fin de prevenir el deterioro o la pérdida física de información relevante. Incluye medidas como el mantenimiento de la seguridad en los lugares y la protección de los equipos contra daños o hurtos. (ISO/IEC 27002, 2022).

Tabla 4

Tema objetos físicos ISO-27002:2022

OBJETOS FISICOS		
27002:2022	**CONTROL**	**TIPO DE CONTROL**
7.1	Perímetros de seguridad física	Preventivo
7.2	Entrada física	Preventivo
7.3	Asegurar oficinas, habitaciones e instalaciones	Preventivo
7.4	Monitoreo de seguridad física	Detectivo
7.5	Protección contra amenazas físicas y ambientales	Preventivo
7.6	Trabajando en áreas seguras	Preventivo
7.7	Descripción de la pantalla y pantalla clara	Preventivo
7.8	Manejo de equipos y protección	Preventivo
7.9	Seguridad de activos fuera de las instalaciones	Preventivo
7.10	Medios de almacenamiento	Preventivo
7.11	Soporte de servicios públicos	Preventivo Detectivo
7.12	Cableado de seguridad	Preventivo
7.13	Mantenimiento de equipo	Preventivo
7.14	Eliminación o reutilización segura del equipo	Preventivo

Fuente: Viteri Peñafiel (2022)

D. Tecnología

En este ámbito se explora cómo la tecnología puede contribuir a la protección integral de la información empresarial. Se enfoca en la implementación de medidas tecnológicas, como el uso de contraseñas robustas, la instalación de software antivirus actualizado y la realización regular de copias de seguridad automatizadas, con el fin de mitigar los riesgos asociados a posibles fallos técnicos y a las diversas amenazas provenientes del ciberespacio. Estas herramientas no solo buscan mantener la confidencialidad, integridad y disponibilidad de los datos, sino también fortalecer la resiliencia de la organización ante posibles incidentes de seguridad. (ISO/IEC 27002, 2022).

Tabla 5

Tema tecnología ISO-27002:2022

	TECNOLOGIA	
27002:2022	**CONTROL**	**TIPO DE CONTROL**
8.1	Dispositivos de punto final del usuario	Preventivo
8.2	Derechos de acceso privilegiados	Preventivo
8.3	Restricción de acceso a la información	Preventivo
8.4	Acceso al código fuente	Preventivo
8.5	Autenticación segura	Preventivo
8.6	Gestión de capacidad	P. Detectivo
8.7	Protección contra malware	P. D. Correctivo
8.8	Gestión de vulnerabilidades técnicas	Preventivo
8.9	Gestión de configuración	Preventivo
8.10	Eliminación de información	Preventivo
8.11	Enmascaramiento de datos	Preventivo
8.12	Prevención de fugas de datos	Preventivo
8.13	Copia de seguridad de la información	Correctivo
8.14	Redundancia de instalaciones de procesamiento de información	Preventivo
8.15	Registro	Detectivo
8.16	Actividades de monitoreo	D. Correctivo
8.17	Sincronización de reloj	Detectivo
8.18	Uso de programas de utilidad privilegiados	Preventivo
8.19	Instalación de software en sistemas operativos	Preventivo
8.20	Seguridad de las redes	P. Detectivo
8.21	Seguridad de los servicios de red	Preventivo
8.22	Segregación de redes	Preventivo
8.23	Filtrado web	Preventivo
8.24	Uso de la criptografía	Preventivo
8.25	Ciclo de vida de desarrollo seguro	Preventivo
8.26	Requisitos de seguridad de la aplicación	Preventivo
8.27	Principios de arquitectura e ingeniería de sistema seguro	Preventivo
8.28	Codificación segura	Preventivo
8.29	Pruebas de seguridad en desarrollo y aceptación	Preventivo
8.30	Desarrollo subcontratado	Preventivo Detectivo
8.31	Separación de entornos de desarrollo, prueba y producción	Preventivo
8.32	Gestión del cambio	Preventivo
8.33	Información de prueba	Preventivo

8.34	Protección de sistemas de información durante las pruebas de auditoría	Preventivo

Fuente: Viteri Peñafiel (2022)

2.2.4. Controles de seguridad

Para Taylor, Alexander, Finch, & Sutton (2020) los controles de seguridad, conforme a la norma ISO 27002, son acciones y medidas específicas implementadas dentro de una organización para mitigar los riesgos de seguridad de la información identificados. Estos controles, que pueden abarcar políticas, procesos, tecnologías y prácticas organizativas, tienen como objetivo principal proteger la confidencialidad, integridad y disponibilidad de los activos de información de la organización. Su implementación se orienta a cumplir con los requisitos establecidos en la norma ISO/IEC 27002:2022, abarcando áreas como la gestión de accesos, protección de datos, gestión de riesgos, seguridad de la red, continuidad del negocio y gestión de incidentes, entre otros aspectos relevantes para la seguridad de la información en la organización.

McCumber (2002), describe los controles de seguridad informática como medidas de protección que resguardan un sistema de computadoras contra posibles ataques o daños. Clasifica estos controles en tres grupos principales: preventivos, que evitan ataques; de detección, que identifican y alertan sobre intrusiones en curso; y correctivos, que reducen los daños causados por un ataque. Destaca la necesidad de combinar estos tipos de controles para garantizar una protección efectiva. Asimismo, subraya la importancia de adaptar estas medidas a las necesidades particulares de cada organización, considerando factores como el tipo de información manejada, los riesgos enfrentados y los recursos disponibles.

2.2.5. Políticas de seguridad

Según Velásquez Henao (2016) las políticas de seguridad son un conjunto de reglas y pautas creadas por una organización para proteger su información. Estas políticas explican qué se debe hacer para mantener la información segura, quién es responsable de hacerlo y cómo se debe llevar a cabo. Su objetivo es garantizar que la información esté protegida contra accesos no autorizados, cambios no deseados y esté disponible cuando sea necesario. Además, estas políticas también indican las medidas específicas que se deben tomar para reducir los riesgos de seguridad y cumplir con las leyes y regulaciones aplicables.

Para los autores Murray, Ulmer, & Ranade (2007), las políticas de seguridad

informática son directrices oficiales que establecen las reglas para el uso de sistemas y datos dentro de una organización, según los expertos. Estas políticas son esenciales para gestionar el riesgo en seguridad informática, ya que ayudan a identificar y evaluar riesgos, implementar medidas de seguridad adecuadas, cumplir con las leyes y fomentar una cultura de seguridad. Se recomienda que estas políticas sean desarrolladas en colaboración con todas las partes interesadas, incluyendo la gerencia, usuarios y equipos de informática y seguridad. Además, es crucial revisar y actualizar regularmente estas políticas para adaptarse a los cambios en las amenazas y las necesidades de la organización.

2.2.6. Concienciación en seguridad

Para Khan (2024) la concienciación en seguridad informática implica educar y sensibilizar de forma continua a los empleados de una empresa sobre los peligros en línea y cómo adoptar prácticas seguras al usar la tecnología. Su objetivo es establecer una cultura organizacional donde todos entiendan su rol en proteger la información y los recursos digitales. Esto incluye temas como identificar correos electrónicos fraudulentos, crear contraseñas sólidas, proteger datos sensibles, navegar de manera segura en Internet y reportar incidentes de seguridad.

Por otra parte, Mauwa (2007), resalta que la concienciación del personal en materia de seguridad informática es un componente esencial para fortalecer la defensa de cualquier organización. Cuando los empleados están bien informados y sensibilizados, se convierten en un recurso clave para prevenir incidentes y responder de manera adecuada ante posibles amenazas. Por ello, los programas de concienciación no deben verse como simples talleres ocasionales, sino como una estrategia continua e integrada dentro del plan global de seguridad de la información. A pesar de su importancia, muchas organizaciones aún muestran un nivel bajo de implementación o compromiso real con estos programas. Esto se debe, en parte, a que los enfoques utilizados no siempre se ajustan a las necesidades específicas de cada institución, ni logran involucrar realmente al personal.

2.2.7. Seguridad de la información

Para INDECOPI (2014) La seguridad de la información comprende salvaguardar los datos en términos de confidencialidad, integridad y disponibilidad. Esto implica asegurar que solo el personal autorizado acceda a la información, que los datos permanezcan precisos y sin alteraciones no autorizadas, y que estén disponibles cuando se necesiten. Además, puede abordar aspectos adicionales como la

autenticidad, evitando la negación de acciones, y la confiabilidad, asegurando la coherencia de los datos.

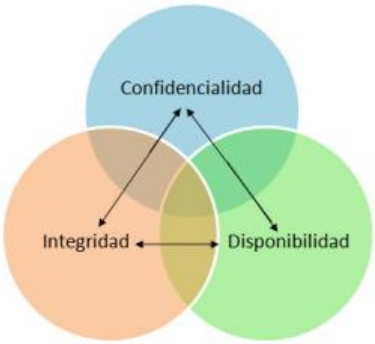
Según Fitzgerald (2007) la seguridad de la información implica una serie de medidas tanto proactivas como reactivas, adoptadas por individuos, organizaciones y sistemas tecnológicos, con el fin de proteger y preservar la integridad, confidencialidad y autenticidad de los datos. Este enfoque integral busca asegurar que la información esté resguardada de posibles amenazas y riesgos, tanto internos como externos. Es esencial distinguir entre seguridad de la información y seguridad informática, ya que mientras la primera abarca la protección global de los datos, la segunda se centra específicamente en la protección de los sistemas y redes informáticas.

2.2.8. Propiedades fundamentales de la seguridad de la información

Las propiedades fundamentales de la seguridad se definen como un principio básico que comprende tres características clave: confidencialidad, integridad y disponibilidad. Según esta tríada, la seguridad de la información debe asegurar la privacidad de los datos, su exactitud y su accesibilidad en todo momento para ser efectiva. (Whitman & Mattord, 2009).

Figura 1

Triada de la seguridad de la información



Fuente: Elaboracion Propia

A. Confidencialidad

Según Roa Buendía (2013) la confidencialidad garantiza que solo personas o sistemas autorizados puedan acceder a la información. Se logra mediante tres mecanismos principales: autenticación, que verifica la identidad para evitar accesos no autorizados; autorización, que asigna niveles de acceso como lectura o modificación; y cifrado, que convierte la información en un formato ilegible para quienes no tienen la autorización,

protegiéndola contra accesos no autorizados.

B. Integridad

Para Vega Briceño (2021) la integridad se enfoca en evitar alteraciones no permitidas o no deseadas en los datos, tanto evitando cambios o eliminaciones no autorizados como revirtiendo cambios aceptados, pero no deseados. En sistemas operativos y aplicaciones, se emplean métodos para supervisar la integridad, como permisos de archivo y funciones de reversión de cambios. Mantener la integridad es esencial, especialmente en datos críticos como registros médicos, donde cambios inapropiados podrían tener consecuencias graves, como errores en las prescripciones o incluso riesgos para la vida del paciente.

C. Disponibilidad

La disponibilidad se trata de poder acceder a nuestros datos cuando los necesitamos. La falta de disponibilidad puede ser causada por diversas interrupciones en la cadena de comunicaciones que nos permite acceder a nuestros datos, como la pérdida de energía, fallos en el sistema operativo o la aplicación, ataques a la red de datos, entre otros. Estos problemas suelen ser el resultado de ataques avanzados de denegación de servicio u otras fallas que impiden a los usuarios acceder a su información (Vega Briceño, 2021).

2.3. MARCO REFERENCIAL

2.3.1. Dirección de Salud

Una DISA (Dirección de Salud) en Perú es una entidad administrativa que depende del Ministerio de Salud y tiene la tarea de gestionar y coordinar los servicios de salud en ciertas áreas específicas dentro de una región. Estas direcciones son responsables de poner en práctica y vigilar las políticas de salud pública en su zona, ajustando y ejecutando programas nacionales y regionales para atender las necesidades de las personas en su área de influencia. (Direccion de Salud Virgen de Cocharcas - Chincheros, 2022).

La DISA se enfoca en planificar, organizar y controlar los servicios de salud para asegurar que la atención médica sea accesible y de calidad en hospitales, centros de salud y otros establecimientos. Trabajan en estrecha colaboración con la DIRESA (Direccione Regional de Salud), que tienen un ámbito de acción más amplio y abarcan toda una región. La estructura de una DISA generalmente incluye una dirección

general y varias unidades que se encargan de áreas específicas como la promoción de la salud, el control de enfermedades y la atención primaria.

Su rol es clave para la descentralización de la administración de la salud en Perú, permitiendo una respuesta más rápida y adecuada a las necesidades locales, y ayudando a implementar las políticas de salud pública de manera más efectiva en las áreas específicas que supervisan.

2.3.2. Seguridad Informática

Según Steinberg (2022) la seguridad informática se centra en proteger todos los aspectos de la información digital, desde archivos personales en dispositivos computacionales hasta datos confidenciales en amplias bases de datos empresariales, contra cualquier amenaza que pueda comprometer su integridad o su adecuado funcionamiento. Esto incluye la protección contra virus, intrusiones de hackers, robo de datos, errores humanos, desastres naturales y cualquier otro peligro potencial en el entorno digital (pág. 7).

Scolnik (2016) enfatiza que la seguridad informática se basa en tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Estos pilares garantizan que solo individuos autorizados accedan a la información, que los datos permanezcan sin alteraciones o daños, y que la información esté disponible cuando sea necesaria. Además, el autor destaca la importancia de las acciones preventivas, de detección y de respuesta ante posibles ataques cibernéticos que puedan comprometer estos principios. (pág. 7)

Es crucial comprender que la seguridad informática no se restringe únicamente a los dispositivos computacionales, ya que abarca una amplia gama de aspectos en diferentes áreas de la vida. Por lo tanto, es igualmente importante familiarizarse con otros conceptos relacionados (Roa Buendía, 2013).

A. Seguridad física

Según Roa Buendía (2013) la seguridad física abarca la protección de todos los elementos relacionados con los equipos informáticos, incluyendo ordenadores de propósito general, servidores especializados y equipamiento de red. En este sentido, las principales amenazas son los desastres naturales, como incendios o inundaciones, que pueden afectar la operatividad de los servidores. Por ello, se recomienda contar

con un segundo lugar para garantizar la continuidad de las operaciones. Además, se debe considerar la protección contra robos mediante medidas de seguridad como vigilancia y controles de acceso. Por último, para mitigar fallos de suministro como cortes de energía o conexión, es esencial contar con respaldos como baterías o grupos electrógenos, asegurando así la disponibilidad de los servicios incluso en situaciones adversas.

B. Seguridad lógica

Para Roa Buendía (2013) la seguridad lógica se centra en proteger las aplicaciones informáticas, con amenazas como virus, pérdida de datos y ataques a servidores. Para contrarrestar estos riesgos, se recomienda eliminar programas no deseados, realizar pruebas exhaustivas de aplicaciones y mantener copias de seguridad. Los servidores son especialmente vulnerables y requieren una instalación mínima de software para reducir el riesgo de ataques. Además, la seguridad se puede abordar desde una perspectiva activa y pasiva, siendo esta última la recuperación tras un ataque, como la utilización de baterías para cortes de energía, mientras que la activa busca prevenir ataques mediante medidas de protección detalladas previamente.

2.3.3. Norma Internacional de seguridad

La Norma Internacional de Seguridad se refiere a un conjunto de estándares y directrices globales que establecen prácticas de seguridad consistentes y eficaces en diversos campos, como la tecnología de la información, la gestión de riesgos y la protección de datos. Estas normas son desarrolladas por organizaciones internacionales de normalización, como la Organización Internacional de Normalización (ISO). Abordan aspectos específicos de seguridad, como la seguridad de la información (por ejemplo, ISO 27001), la seguridad alimentaria (por ejemplo, ISO 22000) y la seguridad laboral (por ejemplo, ISO 45001). Adoptar normas internacionales de seguridad ayuda a las organizaciones y a los países a establecer un marco común de buenas prácticas y a mejorar la protección de personas, activos y datos contra amenazas y riesgos (ISO Tools, 2020).

2.3.4. Grupo de normas ISO/IEC 27000

La ISO/IEC (2018) describe al Grupo de normas ISO/IEC 27000 como un conjunto de estándares internacionales que se centran en la seguridad de la información. Estas normas son el resultado de la colaboración entre la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Su objetivo principal es establecer un marco completo para la gestión de la seguridad de la

información en las organizaciones, proporcionando directrices para su establecimiento, implementación, mantenimiento y mejora continua.

Este grupo de normas incluye estándares como ISO/IEC 27001, que define los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), así como normas complementarias como ISO/IEC 27002, que ofrece orientación específica sobre la implementación de controles de seguridad de la información. Estas normas desempeñan un papel crucial en la protección de los activos de información de una organización y en la gestión eficaz de los riesgos relacionados con la seguridad cibernética.

2.3.5. Sistema de gestión de seguridad de la información

Un Sistema de Gestión de la Seguridad de la Información, o SGSI, es un conjunto de políticas, procedimientos, procesos y controles que una organización implementa para gestionar y proteger la seguridad de la información de manera efectiva. Este sistema ayuda a identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información, y establece medidas para prevenir, mitigar y responder a incidentes de seguridad (ISO/IEC, 2018).

2.3.6. Ciclo de vida de un proyecto de seguridad informática

Según Joyanes Aguilar (2010) el ciclo de vida de un proyecto de seguridad informática abarca una secuencia de fases y acciones desde su concepción hasta su conclusión, adoptando un método sistemático y ordenado. Involucra el diagnostico, planificación, implementación, evaluación de medidas de seguridad, con el fin de resguardar los sistemas de información contra riesgos y amenazas., este ciclo resulta fundamental para asegurar la efectividad y adaptabilidad de las estrategias de seguridad en un entorno tecnológico que evoluciona constantemente.

A. Diagnostico

Se considerar como una fase inicial donde se realiza un análisis exhaustivo de la situación actual de la seguridad informática en la organización. Aquí se identifican vulnerabilidades, riesgos y puntos débiles en el sistema de seguridad existente. (Joyanes Aguilar, 2010).

B. Planificación

Luego del diagnóstico, se procede a la elaboración de un plan detallado de seguridad

informática. En esta etapa se establecen objetivos claros, se definen estrategias, se determinan los recursos necesarios y se desarrolla un plan de acción para abordar las deficiencias identificadas anteriormente. (Joyanes Aguilar, 2010).

C. Implementación

Una vez que se ha diseñado el plan de seguridad, se pasa a la etapa de implementación, donde se ejecutan las acciones y medidas planificadas. Esto implica la instalación de sistemas, la configuración de herramientas de seguridad, la aplicación de políticas y procedimientos, entre otros aspectos que garanticen la implementación adecuada. (Joyanes Aguilar, 2010).

D. Evaluación

Después de la implementación, se lleva a cabo una evaluación exhaustiva de las medidas de seguridad implementadas. Se realizan pruebas de penetración, auditorías de seguridad y revisiones periódicas para verificar la eficacia de las medidas y detectar posibles vulnerabilidades. (Joyanes Aguilar, 2010).

2.3.7. Técnicas estadísticas

Hernández Sampieri (2014) define a las técnicas estadísticas como métodos usados para analizar datos de una investigación, facilitar su comprensión y responder preguntas o verificar hipótesis. Incluyen procedimientos descriptivos para resumir información, métodos inferenciales para generalizar resultados y pruebas paramétricas o no paramétricas empleadas según las características de los datos.

Las pruebas paramétricas son métodos de análisis de datos que solo se pueden usar si se cumplen ciertas condiciones importantes. La regla principal es que los datos de la población que se está estudiando deben seguir una distribución normal. También es necesario que la información se haya medido usando una escala con valores bien definidos. (Hernández Sampieri, 2014).

Las pruebas no paramétricas son un conjunto de métodos que permiten analizar datos sin necesidad de asumir que siguen un tipo específico de distribución, como la normal. Es decir, se pueden utilizar incluso cuando no se conoce cómo están distribuidos los datos en la población de donde provienen. (Hernández Sampieri, 2014).

Los métodos no paramétricos ofrecen ventajas frente a los paramétricos porque

permiten analizar datos sin exigir una escala estricta, funcionando con información nominal, ordinal, de intervalo o razón y requiriendo menos supuestos. También resultan apropiados cuando se desconoce la distribución poblacional. No obstante, su desventaja principal es que pueden perder parte de la información aprovechable mediante técnicas paramétricas más precisas. (Arias Gomez, Villasís Keever, & Miranda Novales, 2016).

A. Prueba de normalidad

La prueba de normalidad es un análisis estadístico preliminar que se realiza para verificar si la distribución poblacional de la variable dependiente se asemeja a una distribución normal, lo cual es un requisito crucial para poder utilizar las pruebas estadísticas paramétricas (como la t de Student) o en su defecto las pruebas no paramétricas (como la de Wilcoxon). Esta verificación es indispensable antes de proceder con el análisis estadístico inferencial para garantizar la validez de los resultados. (Hernández Sampieri, 2014).

B. Prueba T Student

Diseñada para evaluar si dos grupos específicos difieren de manera significativa en sus medias con respecto a una variable. Se utiliza cuando la variable de comparación posee un nivel de medición por intervalos o razón. La hipótesis de investigación establece que existe una diferencia notable entre los grupos, mientras que la hipótesis nula postula que no hay una diferencia significativa entre ellos. (Hernández Sampieri, 2014).

C. Prueba de Wilcoxon

Es un test no paramétrico diseñado para la comparación de dos muestras relacionadas o asociadas, como mediciones tomadas antes" y después en el mismo grupo. Se emplea para contrastar dos mediciones de rangos o medianas, con el fin de determinar si la diferencia entre ellas es estadísticamente significativa. (Goss-Sampson, 2018).

D. Análisis factorial

Una técnica estadística multivariante fundamentalmente usada para reducir dimensiones al identificar estructuras subyacentes o factores comunes en un gran conjunto de variables cuantitativas, con el fin de evaluar la dimensionalidad y la validez de constructo de los instrumentos de medición. Esta técnica se divide en dos tipos

principales: el Análisis Factorial Exploratorio (AFE), que busca descubrir las dimensiones emergentes, y el Análisis Factorial Confirmatorio (AFC), que verifica una estructura factorial previamente explorada o teórica. (Méndez, 2024).

2.4. MARCO LEGAL

2.4.1. Ley Nº 29733

La Ley N° 29733 de Protección de Datos Personales en Perú (2011), controla cómo se usan los datos personales. Se aplica a cualquier persona u organización, pública o privada, que maneje datos en el país, ya sea de manera electrónica o en papel. Establece reglas como obtener permiso, usar la información con honestidad y protegerla. Reconoce los derechos sobre datos personales, como verlos, corregirlos, borrarlos o negarlos a que los usen. También dice qué responsabilidades tienen quienes manejan datos, como mantenerlos seguros y confidenciales. Se crearon el Registro Nacional de Protección de Datos Personales y la Autoridad Nacional de Protección de Datos Personales. Si alguien no cumple la ley, puede recibir multas u otras sanciones.

2.4.2. Ley Nº 30096

La Ley N° 30096 (2013), también conocida como Ley de Delitos Informáticos, busca prevenir, investigar y castigar los delitos que afectan los sistemas y datos informáticos, así como otros aspectos legales relevantes; la normativa destaca la tipificación de diversos delitos vinculados con la seguridad de la información, como el acceso no autorizado a sistemas informáticos, el robo de datos, el fraude en línea y la interceptación de comunicaciones, además de establecer la obligación de proteger los datos personales y la confidencialidad de la información. Se requiere la implementación de medidas de seguridad para proteger los sistemas y datos, y se establecen procedimientos para investigar y sancionar los delitos informáticos. La ley enfatiza en la proporcionalidad de las medidas de seguridad, promueve la adopción de acciones preventivas y establece la responsabilidad de las personas jurídicas por los delitos cometidos por sus representantes o empleados. Aunque la Ley N° 30096 es importante para proteger la seguridad de la información en el Perú, se sugiere complementarla con medidas adicionales, como la sensibilización de los usuarios, la implementación de buenas prácticas en seguridad informática y la colaboración entre el sector público y privado.

2.4.3. Decreto supremo Nº 003-2018-PCM

El Decreto Supremo N° 003-2018-PCM, emitido por el Gobierno de Perú,

complementa la Ley N° 29733 sobre protección de datos personales. Publicado el 10 de enero de 2018, entra en vigor al día siguiente. Su objetivo principal es fortalecer el marco legal para la protección de datos en el país. El decreto establece la designación de la Autoridad Nacional de Protección de Datos Personales (ANPDP) y define sus funciones, que incluyen supervisión y fiscalización para garantizar el cumplimiento de la ley. Además, regula el funcionamiento del Registro Nacional de Protección de Datos Personales (RNPD), creado conforme a la Ley N° 29733. (Gobierno del Perú, 2018).

2.4.4. Directiva Nº 005-2019-MINSA

La Directiva N° 005-2019-MINSA, promulgada por el Ministerio de Salud del Perú, establece un marco regulatorio crucial para la gestión de la seguridad de la información en las entidades del sector salud. Esta directiva, con su enfoque integral, busca proteger la confidencialidad, integridad y disponibilidad de los datos sensibles que manejan estas instituciones. En sus diez capítulos, la directiva detalla los principios rectores que guían la gestión de la seguridad de la información, tales como la responsabilidad, la proporcionalidad y la gestión de riesgos. Asimismo, establece lineamientos específicos para la implementación de controles de seguridad, incluyendo la clasificación de activos de información, el control de accesos, la protección contra malware, la gestión de incidentes y la continuidad del negocio. (Ministerio de Salud, 2019).

2.5. Hipótesis

2.5.1. Hipótesis general

La propuesta de plan de seguridad informática mejora el nivel de seguridad de la información en la Dirección de Salud Virgen de Cocharcas en la provincia de Chincheros, 2024.

2.5.2. Hipótesis especificas

a. La propuesta de una norma de seguridad mejora el nivel de seguridad de la información.
b. La propuesta de controles de seguridad mejora el nivel de seguridad de la información.
c. La propuesta de políticas y procedimientos de seguridad mejora el nivel de seguridad de la información.
d. La propuesta de concienciación en seguridad mejora el nivel de seguridad de la información.

2.6. Variables

2.6.1. Definición conceptual de la variable

Plan de seguridad informático (X)

Conjunto de normas para proteger la información: integridad, confidencialidad y disponibilidad. Basado en estándares de seguridad.

Dimensiones de la variable X

X1: Norma de seguridad informática

Marco de seguridad para gestionar riesgos y garantizar la seguridad de sistemas y datos.

a. **Cumplimiento de Normas Internacional:** Nivel de adherencia a estándares internacionales.
b. **Actualización Regular:** Frecuencia de revisión y actualización de las normas de seguridad para mantenerlas alineadas con las mejores prácticas y cambios regulatorios.
c. **Implementación de Políticas:** Grado de implementación de políticas específicas de seguridad dentro de la organización.

X2: Controles de seguridad

Son las medidas y herramientas utilizadas para prevenir, detectar y responder a incidentes de seguridad que puedan comprometer la información o los sistemas informáticos.

a. **Tipos de Controles:** Clasificación de los controles en preventivos, detectivos y correctivos.
b. **Eficacia de los Controles:** Medición del impacto de los controles implementados en la reducción de incidentes de seguridad.
c. **Frecuencia de Evaluación:** Regularidad con la que se revisan y actualizan los controles de seguridad para adaptarse a nuevas amenazas.

X3: Políticas y procedimientos de seguridad

Son los lineamientos y pasos definidos que deben seguirse para garantizar la correcta gestión y protección de la información en una organización.

a. **Existencia de Documentación:** Presencia de manuales y documentos que detallan las políticas y procedimientos.
b. **Cumplimiento y Adherencia:** Nivel de cumplimiento de las políticas por parte

del personal.

c. **Capacitación y Formación:** Frecuencia y calidad de la formación que reciben los empleados sobre las políticas de seguridad.

X4: Concienciación en seguridad

Es el grado de conocimiento y sensibilización del personal respecto a los riesgos de seguridad y las prácticas necesarias para proteger la información.

a. **Capacitación Regular:** Frecuencia con la que se realizan programas de capacitación en seguridad.
b. **Conocimiento del Personal:** Nivel de comprensión y conocimiento del personal sobre los riesgos y medidas de seguridad.
c. **Participación en Simulacros:** Participación del personal en simulacros y ejercicios de seguridad.

Nivel de seguridad de la información (Y)

Es el grado de protección que poseen los datos y sistemas informáticos de una organización frente a amenazas y riesgos de seguridad. Incluye medidas de prevención, detección y respuesta para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

Dimensiones de la variable Y

Y1: Confidencialidad de la información

Es la garantía de que la información sensible y privada está protegida contra acceso no autorizado o divulgación a personas no autorizadas.

Y2: Integridad de la información

Es la propiedad de que la información se mantenga exacta, completa y sin alteraciones no autorizadas, asegurando su fiabilidad y consistencia a lo largo del tiempo y durante su manipulación.

Y3: Disponibilidad de la información

Es la posibilidad de alcanzar la información y los recursos informáticos en el momento adecuado, garantizando su disponibilidad para los usuarios autorizados sin retrasos ni interrupciones.

2.6.2. Definición operacional de la variable

Plan de seguridad informático (X)

La variable Plan de Seguridad Informático se operacionaliza como el conjunto de indicadores cuantitativos que miden el nivel de implementación y eficacia de las acciones de seguridad informática en la DISA, a través de cuatro dimensiones: norma de seguridad informática, controles de seguridad, políticas y procedimientos de seguridad, y concienciación en seguridad. Se utiliza un cuestionario tipo Likert de 5 puntos (1 = Totalmente en desacuerdo, 2 = En desacuerdo, 3 = Ni de acuerdo ni en desacuerdo, 4 = De acuerdo, 5 = Totalmente de acuerdo) con 24 ítems distribuidos en las cuatro dimensiones, aplicado al personal de la DISA.

Dimensiones e indicadores operacionales de la variable X

X1: Norma de seguridad informática

Se operacionaliza mediante el cumplimiento de normas internacionales, la actualización regular y la implementación de políticas.

X2: Controles de seguridad

Se operacionaliza mediante los tipos de controles, su eficacia y la frecuencia de evaluación.

X3: Políticas y procedimientos de seguridad

Se operacionaliza mediante la existencia de documentación, el cumplimiento y adherencia, y la capacitación y formación.

X4: Concienciación en seguridad

Se operacionaliza mediante la capacitación regular, el conocimiento del personal y la participación en simulacros.

Nivel de seguridad de la información (Y)

Dimensiones e indicadores operacionales de la variable Y

Y1: Confidencialidad de la Información

Se mide por: accesos no autorizados, capacitación del personal, políticas de seguridad de la información distribuidas y leídas, equipos con software antivirus actualizado, gestión de contraseñas.

Y2: Integridad de la Información

Se mide por: controles de acceso y auditoría, copias de seguridad y recuperación, tiempo promedio de detección y respuesta ante alteraciones, firmas digitales, modificaciones no autorizadas a los datos.

Y3: Disponibilidad de la Información

Se mide por: tiempo de recuperación del servicio, sistemas críticos, sistemas de respaldo (UPS) y redundancia, mantenimiento preventivo, monitoreo y alerta de fallos.

2.6.3. Operacionalización de variables

Tabla 6

Matriz de operacionalización de la variable Y: Nivel de seguridad de la información

VARIABLE	DIMENSIÓN	INDICADOR	ÍTEM	TIPO DE DATO / INSTRUMENTO
Y: Nivel de Seguridad de la Información	**Y1:** Confidencialidad de la Información	Accesos no autorizados	1. ¿Cree que la DISA toma medidas efectivas para evitar accesos no autorizados a la información?	Ordinal / Cuestionario tipo Likert
			2. ¿Considera que se llevan a cabo revisiones suficientes para detectar accesos no autorizados a la información en la DISA?	
		Capacitación al Personal	3. ¿Está de acuerdo en que las capacitaciones sobre protección de la información son necesarias para el personal de la DISA?	
			4. ¿Cree que sería útil que la DISA implemente un programa de capacitación regular sobre seguridad información?	
		Políticas de	5. ¿Está de acuerdo	

		Seguridad de la Información distribuidas y leídas	en que es importante que el personal de la DISA reciba y lea las políticas de seguridad de la información?
			6. ¿Cree que la DISA debería implementar políticas claras sobre la seguridad de la información y asegurar su difusión al personal?
		Equipos con software antivirus actualizado	7. ¿Considera que es esencial que todos los equipos de la DISA tengan software antivirus actualizado?
			8. ¿Cree que el software antivirus instalado en los equipos de la DISA es adecuado para protegerlos contra amenazas de seguridad?
		Gestión de Contraseñas	9. ¿Cree que la gestión y protección de las contraseñas en la DISA es adecuada y segura?
			10. ¿Está de acuerdo en que es importante implementar procedimientos claros para el cambio regular de contraseñas en la DISA?
	Y2: Integridad de la	Controles de acceso y	11. ¿Está de acuerdo en que el control de

	Información	auditoría	acceso a la información en la DISA es efectivo para prevenir accesos no autorizados?
			12. ¿Cree que la DISA debería implementar auditorías periódicas para detectar accesos no autorizados?
		Copias de seguridad y recuperación	13. ¿Está de acuerdo en que la DISA realiza copias de seguridad de la información de manera regular y segura?
			14. ¿Cree que la DISA está preparada para recuperar la información de manera efectiva en caso de pérdida o daño de los datos?
		Tiempo promedio de detección y respuesta ante alteraciones	15. ¿Cree que la DISA detecta rápidamente los cambios no autorizados en la información?
			16. ¿Está de acuerdo en que la DISA responde de manera oportuna cuando se identifican problemas o alteraciones en la información?
		Firmas	17. ¿Está de acuerdo

		digitales	en que la firma digital es una herramienta importante para garantizar la autenticidad de los documentos en la DISA?
			18. ¿Considera necesario implementar el uso de firmas digitales en los procesos clave de la DISA?
		Modificaciones no autorizadas a los datos	19. ¿Cree que la DISA toma las medidas necesarias para evitar modificaciones no autorizadas en los datos?
			20. ¿Está de acuerdo en que se deberían implementar mejores medidas para detectar cambios no autorizados en los datos de la DISA?
	Y3: Disponibilidad de la Información	Tiempo de Recuperación del Servicio	21. ¿Está de acuerdo en que la DISA restaura rápidamente los servicios tras una interrupción?
			22. ¿Cree que la comunicación sobre interrupciones del servicio en la DISA es oportuna y clara para el personal?
		Sistemas Críticos	23. ¿Está de acuerdo en que los sistemas

		críticos de la DISA están disponibles la mayor parte del tiempo y funcionan sin problemas?
		24. ¿Cree que la DISA debería implementar medidas adicionales para garantizar la operación continua de los sistemas críticos?
	Sistemas de respaldo (UPS) y redundancia	25. ¿Está de acuerdo en que los UPS instalados en la DISA son efectivos para prevenir interrupciones durante cortes de energía?
		26. ¿Considera necesario implementar sistemas redundantes para asegurar el funcionamiento continuo en caso de fallas del servidor principal de la DISA?
	Mantenimiento preventivo	27. ¿Está de acuerdo en que el mantenimiento regular de los equipos de la DISA es efectivo para prevenir fallas?
		28. ¿Cree que se deberían realizar revisiones más

		frecuentes para evitar problemas en los equipos de la DISA?
	Monitoreo y alerta de fallos	29. ¿Está de acuerdo en que la DISA monitorea adecuadamente el estado de los equipos para prevenir fallos?
		30. ¿Cree que sería útil recibir alertas automáticas cuando hay problemas con los equipos de la DISA?

Nota. Elaboración propia.

III. MATERIAL Y MÉTODOS

3.1. Tipo y nivel de investigación

3.1.1. Tipo de investigación

De acuerdo con Jaime Miranda (2015), “Los estudios experimentales, conocidos también como estudios de intervención, se distinguen porque el investigador controla y cambia de manera deliberada lo que desea evaluar, ya sea un tratamiento, una actividad o una condición particular”. La investigación tesis es experimental porque aplica una intervención y evalúa su efecto comparando resultados pre y post test.

Hernández Sampieri (2014), describe la investigación prospectiva como “la manera de prever lo que podría suceder en el futuro, usando mediciones que han sido planeadas con cuidado para recopilar información de forma ordenada y entender lo que podría pasar”. La investigación es prospectiva porque se recopilan datos planificados para prever y entender futuros riesgos en la seguridad informática a lo largo del tiempo.

Para Hernández Sampieri (2014), la investigación longitudinal " Un estudio longitudinal analiza cómo cambian ciertas características o situaciones a lo largo del tiempo. Para lograrlo, se recoge información en distintos momentos, lo que permite seguir el proceso y entender mejor cómo evoluciona el fenómeno que se está investigando.". La investigación es longitudinal porque recopila datos antes y después de la propuesta de plan de seguridad.

Ruiz Olabuénaga (2012), la investigación analítica se “define como un enfoque que implica la manipulación de una o más variables para examinar cómo afectan a otra variable”. La investigación se considera analítica porque la variable independiente plan de seguridad y dependiente nivel de seguridad de la información, son variables analíticas, que tienen una relación de independencia y dependencia.

3.1.2. Nivel de investigación

Hernández Sampieri (2014), menciona que "La investigación aplicativa busca resolver problemas concretos mediante propuestas y programas que aplican conocimientos teóricos y metodológicos para mejorar procesos o situaciones específicas en la realidad”. El nivel de Investigación es aplicativo, porque se propone un plan de seguridad para mejorar el nivel de seguridad de la información, mediante la norma ISO/IEC 27002.

3.2. Métodos

El método empleado en la presente investigación es el método científico en su vertiente hipotético-deductiva, que parte de hipótesis formuladas a partir de teorías generales sobre seguridad de la información y la norma ISO/IEC 27002:2022, para contrastarlas empíricamente mediante la comparación de mediciones pretest y postest (Hernández-Sampieri et al., 2014). Este método permite evaluar si la propuesta de plan de seguridad informática produce una mejora significativa en el nivel de seguridad de la información en la DISA “Virgen de Cocharcas”.

Complementariamente, se emplea el método analítico, que consiste en la descomposición de la variable independiente (plan de seguridad informática) en sus cuatro dimensiones constitutivas —norma de seguridad, controles de seguridad, políticas y procedimientos de seguridad, y concienciación en seguridad— para su estudio detallado e independiente (Arias, 2012). Asimismo, la variable dependiente (nivel de seguridad de la información) se analiza a través de sus tres dimensiones: confidencialidad, integridad y disponibilidad.

El método estadístico descriptivo e inferencial constituye la herramienta central de análisis: la estadística descriptiva permite la organización y resumen de los datos mediante frecuencias absolutas y relativas, mientras que la estadística inferencial —prueba t de Student para muestras emparejadas y prueba de rangos con signo de Wilcoxon— posibilita la contrastación de las hipótesis formuladas, determinando si las diferencias observadas entre las mediciones pretest y postest son estadísticamente significativas (Triola, 2013).

3.3. Diseño de la investigación

Según Hernández Sampieri (2014), “El diseño pre - experimental llamado preprueba y posprueba con un solo grupo consiste en medir primero a un mismo grupo, luego aplicarles una intervención o tratamiento y, finalmente, volver a evaluarlos para ver si hubo cambios. Su mayor desventaja es que no incluye un grupo de control con el cual comparar los resultados obtenidos”. En el diseño pre experimental, específicamente el modelo preprueba–posprueba con un solo grupo, la investigación evalúa el efecto de la propuesta de plan de seguridad informática en el nivel de seguridad de la información. Este diseño contempla una medición antes de la intervención, la aplicación del plan de seguridad y una medición posterior, sin la inclusión de un grupo de control. Siendo los procedimientos del diseño los siguientes:

a. Se debe operacionalizar la variable nivel se seguridad para construir el instrumento cuestionario.
b. Se debe determinar la validez y confiabilidad del instrumento cuestionario.
c. Se debe aplicar el instrumento cuestionario a los empleados de la Dirección de Salud Virgen de Cocharcas; para obtener la medición inicial de los datos relacionadas al nivel de seguridad.
d. Se debe aplicar la intervención, correspondiente a la propuesta de plan de seguridad de la información.
e. Se debe aplicar nuevamente el cuestionario para obtener la medición final del nivel de seguridad.
f. Se debe realizar el análisis comparativo de los resultados obtenidos en los cuestionarios, procesar los datos y determinar el efecto de la intervención.

3.4. Población y muestra

3.4.1. Población

Según Hernández-Sampieri (2014), la población es el conjunto de todos los casos que concuerdan con determinadas especificaciones; es decir, abarca la totalidad de elementos o unidades de análisis que comparten características comunes, sobre los cuales se pretende generalizar los resultados de la investigación.

En la presente investigación, la población está conformada por **60 trabajadores** que laboran en la Dirección de Salud Virgen de Cocharcas de la provincia de Chincheros, distribuidos en dos áreas funcionales: 38 trabajadores del área administrativa y 22 trabajadores de las coordinaciones de salud.

Tabla 7

Distribución de la población de estudio

Área	N.° de trabajadores	Porcentaje
Área administrativa	38	63.3%
Coordinaciones de salud	22	36.7%
Total	**60**	**100.0%**

Nota. Elaboración propia a partir del CAP institucional de la DISA Virgen de Cocharcas, 2024.

Adicionalmente, se identificó la población de activos informáticos de la DISA Virgen de Cocharcas, con el objetivo de contextualizar el entorno tecnológico institucional y sustentar la propuesta del plan de seguridad informática. Esta inclusión no implica una evaluación técnica individualizada, sino una caracterización referencial orientada a determinar la criticidad, uso y relevancia operativa de los recursos tecnológicos.

Tabla 8

Inventario categorizado de activos informáticos de la DISA Virgen de Cocharcas

Activo informático	Tipo	Descripción / Uso
Servidor	Hardware	Aloja las bases de datos locales del SIGA y SIAF para la gestión financiera, logística y administrativa.
Computadoras	Hardware	Equipos utilizados para realizar actividades de gestión administrativa, operativa y de coordinación.
Equipos de red	Red	Permiten la conectividad entre las estaciones de trabajo y el acceso a Internet y a sistemas web.
UPS	Hardware	Dispositivos que aseguran la continuidad eléctrica ante cortes de energía, protegiendo los equipos críticos.
Impresoras	Hardware	Equipos para imprimir documentos administrativos, informes, reportes y formatos oficiales.
Antivirus	Software	Soluciones de seguridad instaladas en las computadoras para prevenir infecciones por malware.
Sistemas críticos	Software	Aplicativos instalados localmente para el registro y gestión de procesos financieros y logísticos.

Nota. Elaboración propia.

3.4.2. Muestra

Muestra de trabajadores (censo)

Hernández-Sampieri (2014) señala que cuando la población es pequeña y accesible en su totalidad, resulta pertinente realizar un estudio censal, que consiste en incluir a todos los elementos de la población como unidades de análisis. Esta metodología

garantiza una representación completa y exhaustiva del universo poblacional, eliminando el error muestral y proporcionando resultados más precisos y generalizables.

Dado que la población de estudio comprende únicamente 60 trabajadores, cifra que permite su abordaje integral, se optó por un censo poblacional (N = n = 60). En consecuencia, no se aplicó fórmula de cálculo muestral, ya que la totalidad del personal administrativo (38) y de las coordinaciones de salud (22) fue incluida en el estudio.

Muestra de activos informáticos

Para los activos informáticos, se seleccionó una muestra no probabilística de 52 activos de un total de 163 identificados, utilizando criterios de selección basados en: (1) nivel de criticidad, considerando activos que impactan directamente sobre la confidencialidad, integridad y disponibilidad de la información institucional; (2) valor operativo y estratégico, tomando en cuenta su aporte al cumplimiento de los objetivos funcionales de la DISA; (3) exposición a riesgos, priorizando activos con mayor vulnerabilidad frente a amenazas internas o externas; y (4) tipo de información procesada, privilegiando activos asociados al tratamiento de datos sensibles, como los sistemas financieros y administrativos.

Tabla 9

Distribución de activos informáticos: población y muestra seleccionada

Tipo de activo	Cantidad total	Muestra seleccionada	Criterio de selección
Servidor	1	1	Criticidad alta; aloja sistemas SIGA y SIAF.
Computadoras	58	20	Muestreo estratificado según áreas de mayor flujo de información.
Equipos de red	17	5	Exposición a riesgos por conectividad externa.
UPS	20	5	Asociados a activos críticos (servidor y equipos de red).
Impresoras	20	8	Ubicadas en áreas críticas con alto volumen de impresión.
Antivirus	40	10	Instalados en equipos de mayor uso y exposición.

Sistemas críticos	7	3	Manejo de datos financieros y administrativos sensibles.
Total	**163**	**52**	

Nota. Elaboración propia.

La muestra de activos informáticos no fue determinada mediante fórmula estadística, dado que el universo es reducido, finito y completamente identificado. La información recopilada a partir de estos activos sirvió como base referencial para orientar las recomendaciones del plan de seguridad informática, en coherencia con la infraestructura tecnológica disponible en la institución.

3.5. Muestreo

El muestreo constituye el procedimiento mediante el cual se seleccionan las unidades de análisis que conformarán la muestra de estudio (Hernández-Sampieri, 2014). En la presente investigación se emplearon dos estrategias de muestreo diferenciadas según la naturaleza de las unidades de análisis:

Muestreo para trabajadores: censo

Al tratarse de una población finita y pequeña (N = 60), se aplicó un censo poblacional, que implica la inclusión de todos los elementos de la población como sujetos de estudio. Según Arias (2012), el censo es recomendable cuando la población es accesible en su totalidad y su tamaño no justifica la aplicación de técnicas de muestreo probabilístico. En este caso, la totalidad de los 60 trabajadores de la DISA Virgen de Cocharcas fue considerada como unidad de análisis, por lo que no se requirió técnica de muestreo.

Muestreo para activos informáticos: no probabilístico intencional

Para la selección de activos informáticos se empleó un muestreo no probabilístico de tipo intencional o por juicio, que consiste en la selección deliberada de los elementos que, a criterio del investigador, resultan más representativos y relevantes para los fines del estudio (Hernández-Sampieri, 2014). La selección se fundamentó en cuatro criterios técnicos: nivel de criticidad, valor del activo, exposición a riesgos y tipo de información procesada o almacenada.

Esta estrategia se justifica porque el universo de activos informáticos es reducido (163 unidades), completamente identificado y heterogéneo en cuanto a su función y criticidad, lo que hace pertinente una selección dirigida en lugar de un muestreo

aleatorio. Los 52 activos seleccionados representan los elementos de mayor relevancia para la caracterización del entorno tecnológico y la formulación del plan de seguridad informática propuesto.

3.6. Técnicas e instrumentos

3.6.1. Técnicas

Según Aguilar Villanueva (2015) la encuesta, es una técnica de investigación, posibilita recabar datos de un grupo de individuos, conocidos como encuestados o informantes, mediante una serie de preguntas estructuradas que se aplican de manera organizada y planificada. Se emplea la técnica de encuesta para recopilar información sobre las variables relacionadas con el plan de seguridad informática y el nivel de seguridad de la información.

Fase pre experimental: En esta fase se evaluará el efecto del plan de seguridad informática propuesto en la mejora del nivel de seguridad de la información. Para ello, se realizará una medición inicial antes de aplicar la intervención y una medición final después de su implementación, lo que permitirá comparar los resultados y determinar el cambio producido.

3.6.2. Instrumentos

Según Hernández Sampieri (2014), el cuestionario estructurado es un formulario con preguntas ya preparadas que se hacen a un grupo de personas de manera organizada. Las preguntas pueden ser de opción múltiple, de opinión o para responder libremente. En este estudio, se usará un cuestionario estructurado para recolectar información sobre cómo el personal percibe el nivel de seguridad y entiende el plan de seguridad informática. Las respuestas se registrarán en el cuestionario en un único momento del estudio.

3.7. Validez y confiabilidad de instrumentos

3.7.1. Validez

Según Hernández Sampieri (2014), la validez de un instrumento de medición se refiere a su capacidad para medir con precisión la cualidad específica que se intenta evaluar. En esencia, indica qué tan acertadamente el instrumento captura la variable bajo estudio. Para asegurar que las herramientas utilizadas para recoger datos en esta investigación sean efectivas, se empleó un método conocido como juicio de expertos. En el Anexo 2, se presenta la prueba de validez de contenido, y en el Anexo 3 se encuentran los resultados que proporcionaron los jueces, así como el cálculo de la V

de Aiken.

Esto significa que la validez de contenido del instrumento ha sido confirmada, lo que indica que las preguntas son adecuadas y relevantes para el estudio. En este contexto, un valor de 1 en la evaluación de los expertos señala que el ítem es altamente apropiado para medir los aspectos relacionados con la seguridad de la información.

3.7.2. Confiabilidad

De acuerdo con Hernández Sampieri (2014), La confiabilidad de un instrumento se relaciona con su capacidad para proporcionar resultados consistentes cada vez que se evalúa el mismo aspecto o fenómeno en diferentes momentos o situaciones. Para garantizar la confiabilidad del instrumento de recolección de datos, se aplicará el coeficiente de alfa de Cronbach. Este coeficiente evalúa qué tan bien se correlacionan las preguntas entre sí, lo que permite determinar si el instrumento está midiendo de manera consistente los aspectos relacionados con la seguridad de la información.
El análisis se llevó a cabo utilizando los datos obtenidos de las respuestas del cuestionario (Ver anexo 4). Se obtuvo un coeficiente de alfa de Cronbach igual a 0.906 (Ver anexo 5) lo que indica una muy buena confiabilidad del instrumento. Esto significa que las preguntas del cuestionario son coherentes y que los resultados obtenidos serán más confiables.

3.8. Técnicas de procesamiento de datos

3.8.1. Descripción de procedimientos

Para mejorar el nivel de seguridad de la información en la Dirección de Salud (DISA) "Virgen de Cocharcas", se propone un plan de seguridad informática basado en la norma internacional ISO/IEC 27002:2022. La elección de esta norma se justifica porque, a diferencia de la ISO/IEC 27001 -que exige un sistema de gestión completo y una certificación formal-, la ISO/IEC 27002:2022 se enfoca en proporcionar recomendaciones prácticas sobre controles específicos de seguridad de la información, sin los requisitos de auditoría y certificación, lo que permite que la DISA pueda adoptar y adaptar estos controles de manera directa y viable.

La propuesta del plan de seguridad se estructura en cuatro fases, alineadas con el ciclo de vida de un proyecto de seguridad informática (Joyanes Aguilar, 2010): diagnóstico, planificación, implementación y evaluación.

A. Fase de diagnóstico

En esta fase inicial se examinó exhaustivamente el entorno institucional, recopilando información sobre el estado actual de los equipos informáticos -incluyendo aspectos de software, hardware y seguridad de los entornos de almacenamiento-, así como el nivel de conciencia de los empleados en materia de seguridad de la información, mediante la aplicación de un cuestionario (ver Anexo 4).

En relación con el aspecto estructural -ubicación de centros de datos, servidores, switches y exposición de las redes-, se identificaron problemas como la exposición no deseada de equipos, la desorganización del cableado y su falta de estructura, incluyendo la disposición caótica de cables sin orden discernible y el uso de cinta adhesiva para fijarlos a paredes y pisos, lo cual no se ajusta a los estándares de instalación y podría afectar el funcionamiento y seguridad de la red.

Tabla 10

Fase de diagnóstico

Actividad	Stakeholders	Acciones a realizar	Logros esperados
Revisión inicial de la situación actual de la DISA "VC"	Unidad de Estadística e Informática	Evaluar el entorno laboral y recopilar información a través de un cuestionario.	Se identificaron debilidades significativas: falta de controles de acceso, desconocimiento de prácticas de seguridad y ausencia de políticas formales.
Evaluación de normas de seguridad informática	Unidad de Estadística e Informática	Elegir la norma más conveniente y actualizada acorde a las necesidades de la institución.	Se determinó que la ISO/IEC 27002:2022 es la norma más adecuada para estructurar el plan de seguridad de la información.

Nota. Elaboración propia.

B. Fase de planificación

Completado el diagnóstico, se procedió a diseñar la propuesta del plan de seguridad de la información, incluyendo una revisión proyectada de los sistemas y equipos actuales con recomendaciones específicas para mejorar la infraestructura informática.

Entre las recomendaciones se planteó la posible sustitución de equipos con fallas críticas y la adquisición de Sistemas de Alimentación Ininterrumpida (UPS) para preservar la integridad de los datos ante cortes eléctricos.

El plan se formuló en alineación con la norma ISO/IEC 27002:2022, seleccionando 12 controles distribuidos en los cuatro dominios de la norma, según las necesidades específicas de la DISA "VC":

Dominio organización

Políticas para la seguridad de la información. Establece directrices claras de seguridad, crea un marco para la capacitación del personal y asegura que las políticas estén distribuidas y sean leídas por todos los empleados.

Seguridad de la información en la gestión de relaciones. Protege la información durante las interacciones con terceros (proveedores, otras entidades), estableciendo requisitos claros de seguridad y permitiendo gestionar y auditar el acceso que terceros tienen a la información.

Transferencia de información. Garantiza que los datos se trasladen de manera segura, previniendo modificaciones no autorizadas durante el proceso y restringiendo el acceso solo al personal autorizado.

Dominio personas

Conciencia de seguridad, educación y capacitación. Asegura que el personal esté capacitado en prácticas de seguridad y conozca los riesgos, promoviendo la comprensión de las políticas de seguridad establecidas.

Trabajo remoto. Gestiona de manera segura el acceso a la información cuando los trabajadores operan fuera de las instalaciones, protegiendo contra accesos no autorizados y promoviendo el uso de contraseñas seguras.

Informes de eventos de seguridad de la información. Proporciona un sistema de reporte de eventos de seguridad, facilitando el seguimiento de accesos, la detección de actividades inusuales y la gestión rápida de incidentes.

Dominio seguridad física

Asegurar oficinas, habitaciones e instalaciones. Establece protecciones físicas rigurosas en las áreas donde se maneja información sensible, limitando el acceso a personal autorizado.

Protección contra amenazas físicas y ambientales. Implementa medidas preventivas ante riesgos ambientales (incendios, fallos de energía), fortaleciendo la infraestructura física y minimizando interrupciones en la disponibilidad de servicios

esenciales.

Eliminación o reutilización segura del equipo. Facilita la gestión segura del equipo al final de su vida útil, garantizando la eliminación de datos residuales y la desinfección exhaustiva antes del desecho o reutilización.

Dominio tecnología

Protección contra malware. Mantiene actualizado el software antivirus para asegurar la confidencialidad de la información, minimizando accesos no autorizados o pérdida de datos.

Copia de seguridad de la información. Asegura la integridad y disponibilidad de la información mediante respaldos periódicos, apoyando la estabilidad operativa y el tiempo de recuperación del servicio.

Actividades de monitoreo. Detecta actividades sospechosas y accesos no autorizados de forma temprana, manteniendo vigilancia continua sobre los sistemas críticos y la infraestructura de datos.

Tabla 11

Fase de planificación

Actividad	Stakeholders	Acciones a realizar	Logros esperados
Programación, cronograma y recursos	Unidad de Estadística e Informática	Establecer cronograma tentativo, identificar recursos necesarios y definir logística para la implementación futura.	Organización del cronograma y planificación de recursos para cumplir estándares de seguridad.
Revisión de infraestructura y diagnóstico de controles	Unidad de Estadística e Informática	Evaluar el estado actual de la infraestructura y detectar posibles fallas en equipos y controles de seguridad.	Diagnóstico de la infraestructura y evaluación inicial de controles, con recomendaciones para mejorar.
Socialización de la propuesta de seguridad	Dirección, Unidad de Estadística e Informática	Presentar el plan propuesto a directivos y áreas clave, detallando su	Aprobación preliminar del plan y respaldo de los directivos para

		alineación con ISO/IEC 27002:2022.	continuar con la siguiente fase.
Planificación de capacitación y sensibilización	Unidad de Estadística e Informática, Recursos Humanos	Diseñar un programa de capacitación en seguridad de la información y establecer un plan de sensibilización del personal.	Plan de capacitación establecido, con enfoque en sensibilizar al personal sobre la importancia de la seguridad.

Nota. Elaboración propia.

C. Fase de implementación

En esta fase se ejecutaron las acciones y medidas planificadas. Se elaboró un plan de mantenimiento para los equipos informáticos (ver Anexo 6), se instalaron cámaras de seguridad en puntos clave, se trasladaron equipos críticos (switches) a lugares más seguros con puertas con llave, se instalaron sistemas biométricos de acceso y se crearon contraseñas seguras para los sistemas.

Asimismo, se brindó capacitación al personal sobre el manejo correcto de la información institucional, la identificación de correos electrónicos sospechosos y la importancia de proteger la confidencialidad de los datos. A continuación, se detallan las acciones implementadas por dominio:

Dominio Organización

Políticas para la seguridad de la información: se diseñaron documentos normativos con directrices claras, se distribuyeron electrónica y físicamente a todos los trabajadores, y se organizaron sesiones de capacitación periódicas sobre su contenido.

Seguridad de la información en la gestión de relaciones: se elaboró un registro de servicios tercerizados, se actualizaron contratos con cláusulas de seguridad, se configuraron sistemas de registro de acceso (logs), se asignaron roles y permisos específicos, y se implementaron auditorías mensuales.

Transferencia de información: se implementó cifrado de base de datos y VPN para proteger datos en tránsito, protocolos seguros (SFTP, HTTPS) para transferencias de archivos, y autenticación robusta con gestión de permisos de acceso.

Dominio personas

Conciencia de seguridad, educación y capacitación: se desarrolló un programa integral de formación (presencial y virtual), con capacitaciones regulares y obligatorias,

y evaluaciones de conocimiento tras cada sesión.

Trabajo remoto: se está implementando VPN con autenticación de dos factores (2FA), se establecieron políticas claras de acceso remoto y se monitorean y registran todos los accesos remotos.

Informes de eventos de seguridad: se propuso implementar una herramienta SIEM de código abierto (Wazuh, OSSEC o Graylog), se establecieron procedimientos de reporte de incidentes y seguimiento desde la detección hasta la resolución.

Dominio seguridad física

Asegurar oficinas e instalaciones: se instalaron lectores biométricos en la entrada principal y áreas sensibles, cámaras CCTV en puntos clave, y registros electrónicos de entradas y salidas con carnets de visitante.

Protección contra amenazas físicas y ambientales: se priorizó la implementación de UPS en áreas críticas y se desarrolló un Plan de Respuesta ante Emergencias con copias de seguridad periódicas y simulacros regulares.

Eliminación o reutilización segura del equipo: se implementó eliminación segura de datos en discos duros al final de la vida útil y procedimientos de inspección y limpieza para equipos destinados a reciclaje o reutilización.

Dominio tecnología

Protección contra malware: se instaló antivirus en todos los equipos con actualizaciones automáticas, se realizan escaneos periódicos y se capacita al personal en identificación de amenazas.

Copia de seguridad: se realizan respaldos periódicos (diarios o semanales según criticidad), se almacenan localmente en servidores internos y se realizan pruebas regulares de recuperación.

Actividades de monitoreo: se propuso implementar SIEM, se establecieron procedimientos de reporte y seguimiento de incidentes desde la detección hasta la resolución con identificación de causas raíz.

Tabla 12

Fase de implementación

Actividad	Stakeholders	Acciones a realizar	Logros esperados
Definición general de controles de seguridad	Unidad de Estadística e Informática	Diseño de controles básicos en tecnología, personas,	Bases establecidas para la implementación de controles mínimos en

		organización y seguridad física.	todas las áreas.
Elaboración de políticas de seguridad	Dirección, Unidad de Estadística e Informática	Elaboración de documentos normativos y difusión mediante reuniones, correos y capacitaciones.	Políticas claras distribuidas a todo el personal, promoviendo su entendimiento y aplicación.
Mantenimiento preventivo de equipos	Unidad de Estadística e Informática	Elaboración de cronograma de mantenimiento preventivo y uso de herramientas de diagnóstico.	Equipos funcionando en óptimas condiciones, reduciendo fallos y garantizando continuidad.
Capacitación en uso seguro de la información	Unidad de Estadística e Informática, Recursos Humanos	Capacitación sobre riesgos comunes y buenas prácticas, usando materiales audiovisuales accesibles.	Aumento de la conciencia del personal sobre riesgos de seguridad para prevenir incidentes.
Actividades complementarias	Dirección, Área Administrativa, Área de Informática	Implementación de controles físicos, monitoreo, protección, respaldos y eliminación segura de datos.	Mitigación de riesgos físicos, control de acceso, recuperación de datos y protección al final del ciclo de vida.

Nota. Elaboración propia.

D. Fase de evaluación

En esta fase se revisó el avance de la propuesta del plan informático para mejorar el nivel de seguridad de la información, evaluando su efecto real y verificando que los controles aplicados se alineen con las necesidades de seguridad de la DISA "VC". Se implementaron 12 de los 93 controles de la norma ISO/IEC 27002:2022, con el uso de recursos tecnológicos, humanos, materiales y logísticos.

Tabla 13

Controles ISO/IEC 27002:2022 seleccionados para la DISA "VC"

Dominio / Tema	**Controles**
Organización	Políticas para la seguridad de la información

	Seguridad de la información en la gestión de relaciones
	Transferencia de información
Personas	Conciencia de seguridad, educación y capacitación de la información
	Trabajo remoto
	Informes de eventos de seguridad de la información
Objetos físicos	Asegurar oficinas, habitaciones e instalaciones
	Protección contra amenazas físicas y ambientales
	Eliminación o reutilización segura del equipo
Tecnología	Protección contra malware
	Copia de seguridad de la información
	Actividades de monitoreo

Nota. Elaboración propia.

Asimismo, se verificó que los controles estén alineados con las necesidades de la DISA "VC" y se evaluó su viabilidad considerando recursos, costos y compatibilidad con los sistemas. Se aseguró que las políticas y procedimientos propuestos cubran las áreas críticas, se analizó si el plan contempla métodos apropiados para aumentar la conciencia en seguridad informática, y se definieron las etapas para la implementación estableciendo recursos, presupuesto y prioridades.

Tabla 14

Fase de evaluación

Actividad	**Stakeholders**	**Acciones a realizar**	**Logros esperados**
Evaluación de los controles propuestos	Unidad de Estadística e Informática	Revisar si los controles definidos cumplen con los objetivos de seguridad identificados en el diagnóstico.	Controles alineados con los objetivos y ajustes definidos para una correcta implementación.
Validación de políticas y procedimientos	Unidad de Estadística e Informática	Revisión de las políticas de seguridad propuestas para garantizar que cubran las áreas críticas y sean claras.	Políticas adecuadas y aprobadas, aplicadas en la fase de implementación.

Análisis de recursos necesarios	Unidad de Estadística e Informática	Identificación de recursos humanos, tecnológicos y logísticos requeridos, priorizando necesidades críticas.	Recursos definidos y estructurados en un plan para una implementación ordenada.

Nota. Elaboración propia.

3.8.2. Técnicas de análisis de datos

Para el procesamiento de los datos, se aplicaron pruebas de normalidad para determinar el comportamiento de los datos; posteriormente, se empleó la prueba de Wilcoxon para contrastar las hipótesis específicas y la prueba *t* de Student para la hipótesis general. Este procedimiento permitió seleccionar el análisis más adecuado según la distribución de cada variable.

3.8.3. Diseño estadístico

La investigación empleó un diseño preexperimental con mediciones antes y después del plan propuesto. La selección de las pruebas estadísticas se estableció según el supuesto de normalidad, evaluado mediante Kolmogorov-Smirnov.

Para la hipótesis general, la variable presentó distribución normal ($p = 0.200$), por lo que se aplicó la prueba *t* de Student para muestras emparejadas, técnica paramétrica adecuada para comparar medias cuando se cumple la normalidad. El análisis se centró en contrastar las puntuaciones promedio del plan de seguridad informática antes y después de su implementación.

En el caso de las hipótesis específicas, las variables mostraron distribución no normal en el postest ($p < 0.05$). Ante ello, se empleó la prueba de rangos con signo de Wilcoxon, alternativa no paramétrica equivalente a la *t* para muestras relacionadas.

3.8.4. Análisis e interpretación de datos

Para analizar e interpretar los datos obtenidos a través de los cuestionarios aplicados a los trabajadores de la Dirección de Salud Virgen de Cocharcas, se empleó un enfoque descriptivo e inferencial-comparativo. Las respuestas del cuestionario, basado en una escala de Likert, se analizaron utilizando frecuencias para identificar los cambios en la percepción antes y después del plan propuesto.

El análisis se centró en las cuatro dimensiones clave identificadas mediante el Análisis Factorial Exploratorio (AFE): concienciación en seguridad, controles de seguridad, políticas y procedimientos de seguridad, y norma de seguridad. Para cada dimensión, se compararon los puntajes obtenidos y se evaluó el efecto percibido por los trabajadores tras la propuesta.

Los resultados del análisis proporcionaron una visión clara del impacto esperado del plan de seguridad informática, demostrando una mejora significativa en la percepción general de la seguridad de la información. Las pruebas no paramétricas de Wilcoxon revelaron que la propuesta de concienciación, políticas y procedimientos, controles y norma de seguridad produjeron un efecto significativo. Estos datos confirman que la propuesta está sólidamente justificada para su implementación, asegurando que refleja de manera precisa las necesidades y percepciones reales de los trabajadores de la institución.

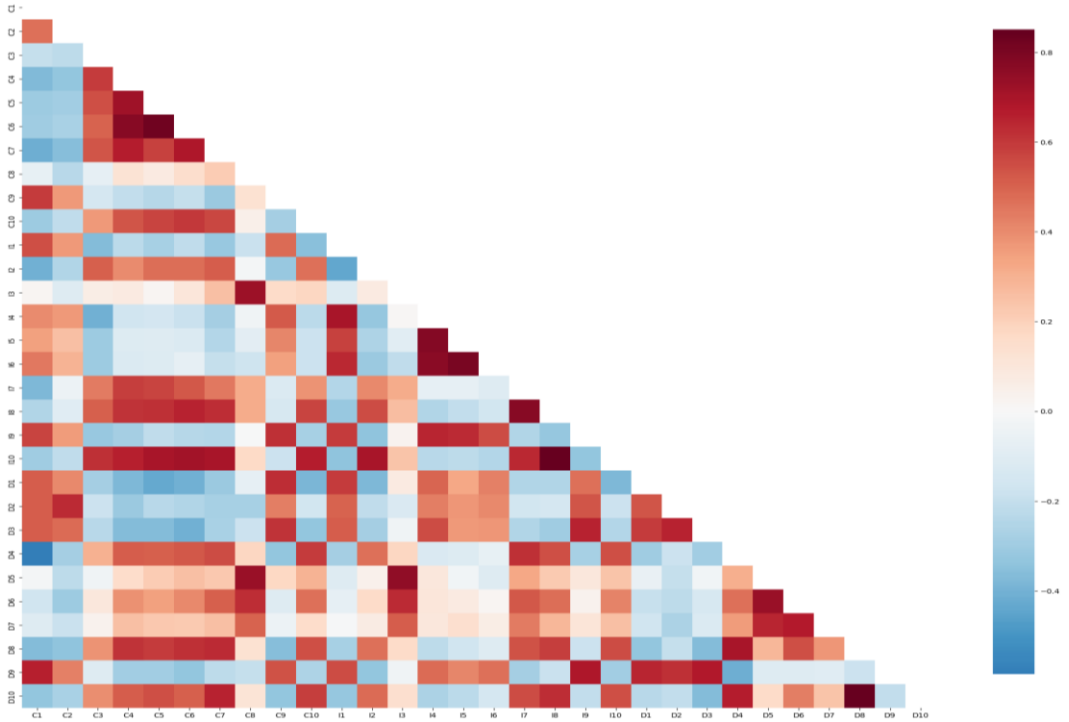
3.9. Aspectos éticos

IV. RESULTADOS Y DISCUSIÓN

4.1. Resultados

Figura 2

Matriz de correlación policórica (30 variables)



Fuente: *Elaboración propia*

La matriz de correlaciones policóricas de 30 variables confirma la idoneidad de los datos para un Análisis Factorial Exploratorio (AFE). Visualmente, se observa una estructura multidimensional bien definida, con bloques diagonales de color rojo intenso que evidencian correlaciones positivas fuertes y la posible presencia de al menos tres factores latentes, Aunque la correlación promedio es baja (r=0.128), el rango amplio de valores (mínimo -0.586, máximo 0.851) y el 12.4% de correlaciones superiores a 0.6 reflejan una dispersión adecuada y una estructura factorial potencialmente rica. En el AFE se aprovecharán las correlaciones más elevadas para identificar los núcleos de cohesión interna y definir con precisión la composición de cada constructo.

Análisis factorial exploratorio

Tabla 15

Cargas de los factores data postest

Factor	Rotación Varimax		Rotación oblimin	
	Ítems	Carga Fac.	Ítems	Carga Fac.
Factor 01	D4	0.655	D4	0.598
	I2	0.607	I2	0.628
	C3	0.628	C10	0.667
	C10	0.672	I7	0.669
	I7	0.682	C3	0.704
	D10	0.711	D10	0.705
	D8	0.736	D8	0.705
	C7	0.741	C7	0.735
	C4	0.764	C4	0.76
	C5	0.786	C5	0.794
	C6	0.796	C6	0.797
	I8	0.819	I8	0.86
	I10	0.863	I10	0.91
Factor 02	C2	0.572	I9	0.503
	I9	0.62	C2	0.574
	D1	0.669	D1	0.631
	C1	0.686	C1	0.658
	C9	0.718	C9	0.707
	D2	0.722	D3	0.72
	D3	0.744	D2	0.724
	D9	0.774	D9	0.756
Factor 03	D7	0.654	D7	0.624
	D6	0.753	D6	0.702
	C8	0.835	C8	0.859
	I3	0.844	I3	0.871
	D5	0.886	D5	0.89
Factor 04	I5	0.779	I1	0.529
	I6	0.807	I4	0.726
	I4	0.732	I5	0.792
	I1	0.557	I6	0.824

Fuente: *Elaboración propia*

El análisis factorial confirmatorio permitió identificar cuatro factores principales (1, 2, 3 y 4), los cuales se vinculan de manera coherente con las propuestas teóricas de la

investigación.

Concienciación en seguridad referido al primer factor (F1) agrupa ítems relacionados con la formación, sensibilización y compromiso del personal respecto a la seguridad de la información. Incluye preguntas sobre la necesidad de capacitaciones (C3, C4), la importancia de conocer y difundir las políticas institucionales (C5, C6), y aspectos prácticos vinculados al uso seguro de los sistemas, como la actualización de antivirus (C7) o el cambio regular de contraseñas (C10). Asimismo, considera la implementación de auditorías (I2), la firma digital (I7, I8) y mecanismos de alerta o revisión constante (D8, D10). Este conjunto de ítems refleja un enfoque orientado al desarrollo de una cultura organizacional en seguridad, donde la concienciación y la formación del personal son pilares fundamentales. Por ello, el AFE (Análisis Factorial Exploratorio) identificó este grupo como representativo a la concienciación en seguridad, en tanto busca fortalecer los conocimientos, actitudes y comportamientos del personal frente a los riesgos informáticos.

Controles de seguridad se refiere al segundo factor (F2) está conformado por ítems que aluden al establecimiento y efectividad de medidas técnicas y operativas destinadas a proteger la información institucional. En este grupo se encuentran preguntas como la eficacia de las medidas para evitar accesos no autorizados (C1, C2), la gestión segura de contraseñas (C9), la prevención de modificaciones indebidas de los datos (I9), así como la disponibilidad, restauración y monitoreo de los sistemas críticos (D1, D2, D3, D9). Estos ítems están directamente vinculados con la implementación de controles de seguridad que aseguren la integridad, disponibilidad y confidencialidad de la información. En consecuencia, el AFE determinó que este factor representa a los controles de seguridad, ya que agrupa elementos que buscan mantener la protección efectiva de los activos informáticos mediante la vigilancia, la revisión constante y la respuesta técnica ante posibles vulnerabilidades.

Las políticas y procedimientos de seguridad que corresponde al tercer factor (F3) agrupa ítems asociados a las acciones normadas y sistemáticas que la organización debe aplicar para garantizar la continuidad operativa y la seguridad de la información. Incluye ítems como la adecuación del software antivirus (C8), la realización periódica de copias de seguridad (I3), la existencia de sistemas de respaldo o redundancia (D6), la instalación de UPS (D5) y el mantenimiento regular de los equipos (D7). Estos elementos conforman un conjunto de políticas y procedimientos técnicos que permiten prevenir interrupciones, pérdidas de datos o fallas en los sistemas. El AFE agrupó

estos ítems bajo una misma dimensión debido a su coherencia interna, evidenciando que el factor representa a las políticas y procedimientos de seguridad, orientada a establecer lineamientos formales para la gestión y operatividad segura de los recursos tecnológicos.

Norma de seguridad que finalmente es el cuarto factor (F4) integra ítems que reflejan la necesidad de establecer una norma formal de seguridad dentro de la institución. Comprende aspectos como el control de acceso a la información (I1), la recuperación de datos ante pérdidas o daños (I4), la detección rápida de cambios no autorizados (I5) y la respuesta oportuna ante incidentes (I6). Estos ítems aluden a una estructura normativa que regula y estandariza los procesos de seguridad de la información en toda la organización. Por ello, el AFE identificó este conjunto como norma de seguridad, ya que representa el marco institucional que permite coordinar, supervisar y evaluar la implementación de todas las medidas y controles en materia de seguridad informática.

En conjunto, la correspondencia entre los factores empíricamente identificados y las propuestas teóricas reafirma la pertinencia del modelo planteado, evidenciando que los ítems seleccionados no solo se agrupan de manera consistente, sino que también reflejan dimensiones esenciales para la implementación de una gestión integral de la seguridad de la información en la organización.

Tabla 16

Prueba de χ² para el ajuste exacto del modelo de análisis factorial confirmatorio

Ajuste del Modelo		
Prueba Para un Ajuste Exacto		
χ²	**gl**	**p**
802	399	<.001

Fuente: *Elaboración propia*

La prueba de Chi-cuadrado ($\boldsymbol{x^2 = 802,\ gl = 399,\ p < .0001}$) resulta estadísticamente significativa, lo cual indica que el modelo teórico presenta diferencias respecto a la matriz de covarianzas observada en los datos. Sin embargo, es importante destacar que este estadístico es altamente sensible al tamaño de la muestra, por lo que en muestras medianas o grandes tiende a rechazar el ajuste incluso cuando el modelo es razonablemente adecuado.

Por esta razón, la significancia del $\boldsymbol{x^2}$ no debe interpretarse de manera aislada; se

complementa con otros índices de ajuste (CFI, TLI, RMSEA, SRMR) que permiten evaluar de manera más robusta la calidad del modelo propuesto.

Tabla 17

Medidas de ajuste del modelo de análisis factorial confirmatorio

Medidas de Ajuste							
				IC 90% del RMSEA			
CFI	**TLI**	**SRMR**	**RMSEA**	**Inferior**	**Superior**	**AIC**	**BIC**
0.739	0.715	0.0949	0.13	0.117	0.143	4056	4257

Fuente: *Elaboración propia*

Los índices de ajuste muestran que el modelo no alcanza niveles satisfactorios. En primer lugar, el CFI = 0.739 y el TLI = 0.715 se encuentran por debajo del umbral mínimo de 0.90 recomendado para un ajuste aceptable, lo que indica un bajo grado de mejora respecto al modelo nulo. En cuanto a las medidas de error, el RMSEA = 0.13 (IC 90% [0.117, 0.143]) se sitúa muy por encima del valor de 0.08 sugerido como aceptable, evidenciando un mal ajuste global. Asimismo, el SRMR = 0.0949 sobrepasa ligeramente el punto de corte de 0.08, confirmando que las discrepancias entre las covarianzas observadas y las estimadas son elevadas.

Finalmente, los criterios de parsimonia (AIC = 4056 y BIC = 4257) permiten comparar este modelo con alternativas más parsimoniosas, siendo preferibles aquellos con valores menores. En conjunto, estos resultados sugieren que el modelo propuesto no representa adecuadamente los datos, lo que justifica la consideración de ajustes o reespecificaciones teóricas y empíricas.

Si bien el análisis factorial confirmatorio (AFC) evidenció un ajuste limitado del modelo de cuatro factores identificado previamente en el análisis factorial exploratorio (AFE), ello no invalida la aplicación del diseño pre - experimental planteado. El AFE permitió identificar dimensiones teóricas relevantes que orientan la interpretación de los resultados, aunque el AFC mostró que el ajuste global del modelo requiere mejoras y que, por lo tanto, las conclusiones deben interpretarse con cautela. Sin embargo, en el marco del diseño pre - experimental, el objetivo central no es confirmar la estructura factorial del instrumento, sino evaluar el efecto de la intervención mediante la comparación de los puntajes obtenidos en el pretest y el postest. En este sentido, se procedió a la aplicación de pruebas paramétricas como la t de Student para muestras relacionadas o no paramétricas en caso de incumplimiento de supuestos, con el fin de establecer si existieron diferencias estadísticamente significativas tras la intervención.

4.1.1. Análisis descriptivo

Concienciación en seguridad

Tabla 18

Percepción de concienciación en seguridad antes y después del plan propuesto.

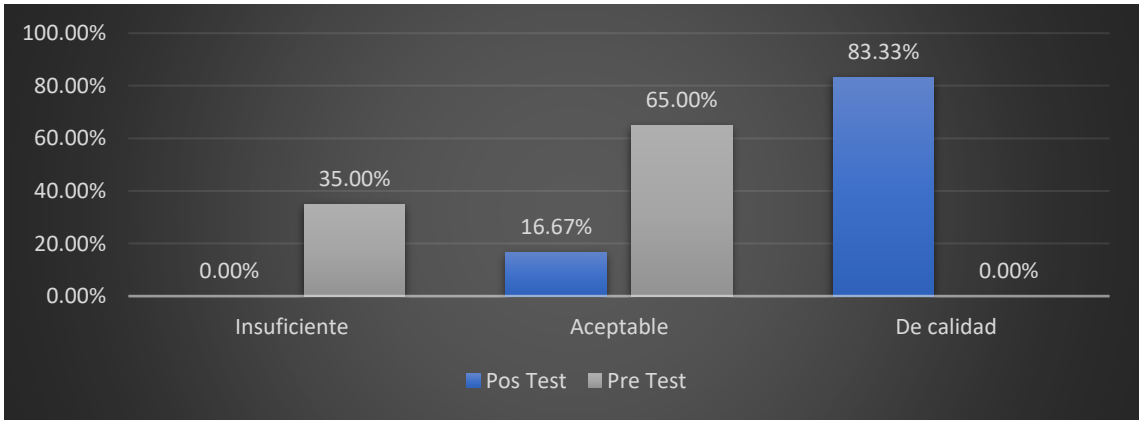
Concienciación en seguridad					
		Pos Test		Pre Test	
Categorías		f	%	f	%
	Insuficiente	0	0.00	21	35.00
	Aceptable	10	16.67	39	65.00
	De calidad	50	83.33	0	0.00
	Total	60	100.00	60	100.00

Fuente: *Elaboración propia*

Los resultados reflejan una percepción positiva del personal sobre la mejora esperada con la implementación del plan. Antes de su aplicación, el 35% consideró insuficiente el nivel de concienciación y el 65% lo calificó como aceptable, sin evidencias de un nivel de calidad. Tras la propuesta, el 83.33% de los encuestados percibe que el plan permitirá alcanzar un nivel de calidad, mientras que el 16.67% lo considera aceptable, sin registros en la categoría insuficiente. En conjunto, estos resultados muestran que la mayoría del personal confía en que el plan propuesto fortalecerá significativamente la cultura de seguridad de la información dentro de la institución.

Figura 3

Percepción de concienciación en seguridad antes y después del plan propuesto



Fuente: *Elaboración propia*

Controles de seguridad

Tabla 19

Percepción de los controles seguridad antes y después del plan propuesto.

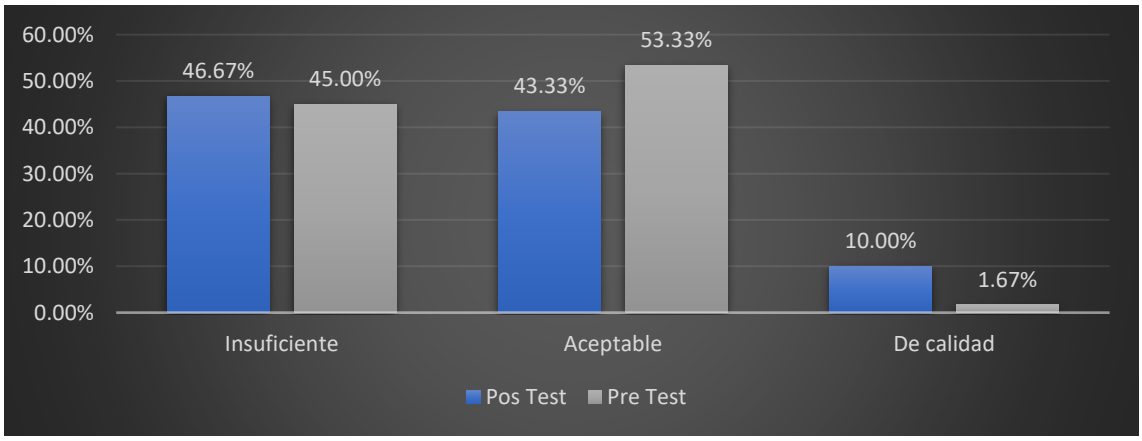
Controles de seguridad				
	Pos Test		Pre Test	
	f	%	f	%
Insuficiente	28	46.67	27	45.00
Aceptable	26	43.33	32	53.33
De calidad	6	10.00	1	1.67
Total	60	100.00	60	100.00

Fuente: *Elaboración propia*

Los resultados evidencian que las percepciones del personal sobre los controles de seguridad muestran una mejora moderada con la implementación del plan. En el pretest, el 45% consideró que los controles eran insuficientes, el 53.33% los calificó como aceptables y solo el 1.67% los percibió de calidad. Tras la aplicación del plan, el 46.67% mantuvo la percepción de insuficiencia, mientras que el 43.33% los consideró aceptables y el 10% observó un avance hacia la calidad. En conjunto, los encuestados perciben que el plan propuesto podría contribuir a fortalecer los mecanismos de protección, aunque reconocen que aún existen áreas críticas que requieren un control más efectivo y sostenido en la gestión de la seguridad informática.

Figura 4

Percepción de los controles de seguridad antes y después del plan propuesto.



Fuente: *Elaboración propia*

Políticas y procedimientos de seguridad

Tabla 20

Percepción de las políticas y procedimientos de seguridad antes y después del plan propuesto.

Políticas y procedimientos de seguridad				
	Pos Test		Pre Test	
	f	%	f	%
Insuficiente	3	5.00	19	31.67

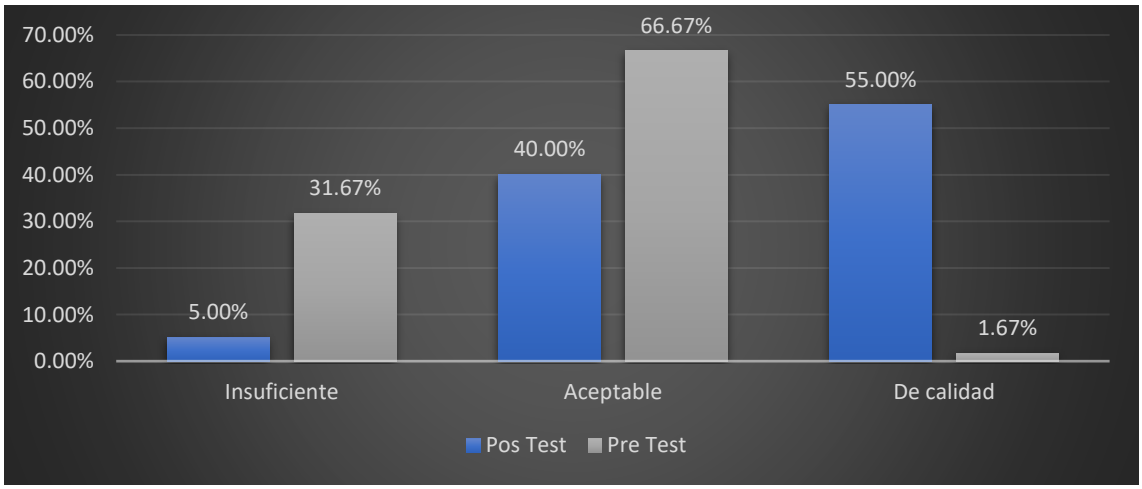
Aceptable	24	40.00	40	66.67
De calidad	33	55.00	1	1.67
Total	60	100.00	60	100.00

Fuente: *Elaboración propia*

Los resultados reflejan una clara percepción de mejora en las políticas y procedimientos de seguridad tras la implementación del plan. En el pretest, el 31.67% de los encuestados consideró que las políticas eran insuficientes, el 66.67% las calificó como aceptables y solo el 1.67% las percibió de calidad. Luego de la aplicación del plan, las percepciones cambiaron significativamente: el 55% de los participantes considera ahora que son de calidad, el 40% las percibe aceptables y apenas el 5% las califica como insuficientes. En general, los encuestados reconocen que el plan propuesto fortalecería considerablemente la estructura normativa y los procedimientos, promoviendo una gestión más organizada y efectiva de la seguridad informática institucional.

Figura 5

Percepción de las políticas y procedimientos de seguridad antes y después del plan propuesto.



Fuente: *Elaboración propia*

Norma de seguridad

Tabla 21

Percepción de la norma de seguridad antes y después del plan propuesto.

Norma de seguridad				
	Pos Test		**Pre Test**	
	f	%	f	%
Insuficiente	27	45.00	7	11.67

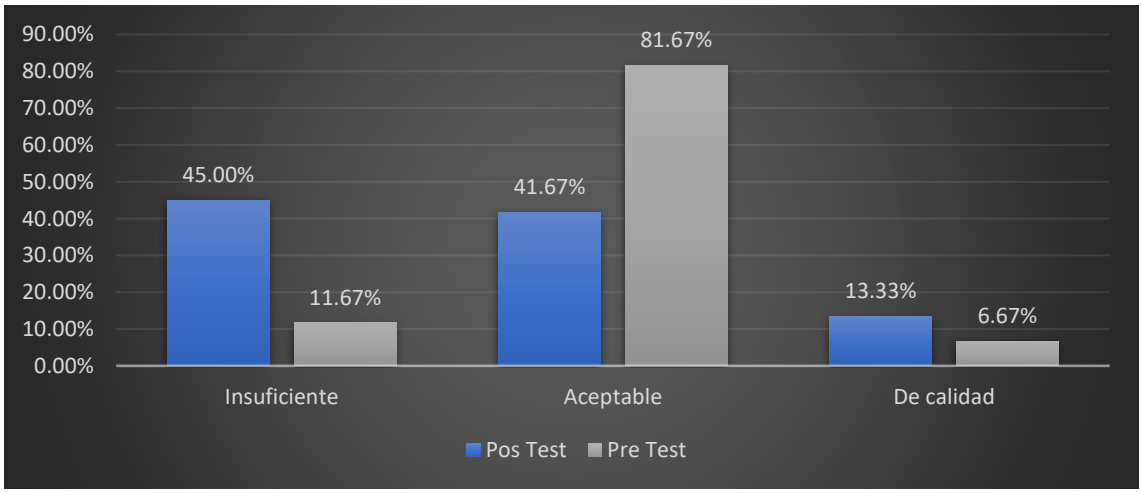
Aceptable	25	41.67	49	81.67
De calidad	8	13.33	4	6.67
Total	60	100.00	60	100.00

Fuente: *Elaboración propia*

Los resultados muestran percepciones mixtas respecto a la eficacia del plan en relación con la norma de seguridad. En el pretest, la mayoría (81.67%) consideró la norma como aceptable, mientras que el 11.67% la percibió insuficiente y solo el 6.67% la calificó de calidad. Tras la implementación del plan, se observa un cambio moderado: el 45% de los encuestados considera la norma insuficiente, el 41.67% la califica aceptable y el 13.33% la percibe de calidad. Estos resultados sugieren que, aunque algunos participantes reconocen una leve mejora, una parte importante aún duda de la efectividad del plan propuesto, considerando que la norma de seguridad necesita fortalecerse y aplicarse de manera más uniforme para generar resultados sostenibles.

Figura 6

Percepción de la norma de seguridad antes y después del plan propuesto.



Fuente: *Elaboración propia*

Seguridad Informática

Tabla 22

Percepción sobre la seguridad informática antes y después del plan propuesto.

Seguridad informática (independiente)				
	Pos Test		Pre Test	
	f	%	f	%
Insuficiente	0	0.00	35	58.33
Aceptable	41	68.33	25	41.67
De calidad	19	31.67	0	0.00

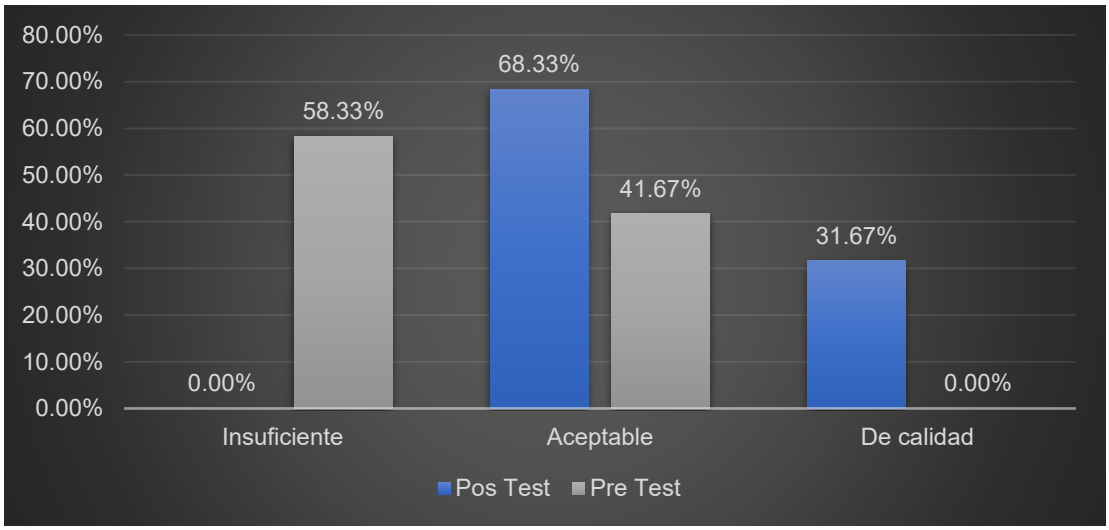
Total	60	100.00	60	100.00

Fuente: *Elaboración propia*

Los resultados evidencian una percepción altamente favorable hacia la implementación del plan propuesto de seguridad informática. Antes de su aplicación, el 58.33% de los encuestados consideraba el plan insuficiente, mientras que el 41.67% lo calificaba como aceptable y ninguno lo percibía de calidad. Después de la propuesta, se observa un cambio notable: el 68.33% lo considera aceptable, el 31.67% lo califica de calidad y no se registran opiniones de insuficiencia. Estos resultados reflejan que la mayoría de los participantes percibe que el plan propuesto fortalecería significativamente la gestión de la seguridad informática, aumentando la confianza en su capacidad para prevenir incidentes, garantizar la protección de la información y consolidar una cultura institucional más segura y responsable.

Figura 7

Percepción sobre la seguridad informática antes y después del plan propuesto.



Fuente: *Elaboración propia*

4.1.2. Análisis inferencial

Tabla 23

Prueba de normalidad.

Pruebas de normalidad			
	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Concienciación en seguridad _POS	0.222	60	0.000
Controles de seguridad _POS	0.118	60	0.036
Políticas y procedimientos de seguridad _POS	0.165	60	0.000
Norma de seguridad _POS	0.140	60	0.005
Seguridad informática (independiente)_POS	0.072	60	,200*

Concienciación en seguridad _PRE	0.112	60	0.060
Controles de seguridad _PRE	0.102	60	0.195
Políticas y procedimientos de seguridad _PRE	0.114	60	0.050
Norma de seguridad _PRE	0.150	60	0.002
Seguridad informática (independiente)_PRE	0.098	60	,200*

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Los resultados del test de Kolmogorov-Smirnov con corrección de Lilliefors evidencian que, en el postest, la mayoría de las dimensiones (concienciación, controles, políticas y norma de seguridad) presentan una distribución no normal ($p < 0.05$), mientras que solo la propuesta de plan de seguridad informática mantiene una distribución normal ($p = 0.200$). En el pretest, las propuestas de controles y plan de seguridad informática muestran normalidad ($p > 0.05$), en tanto que las demás evidencian desviaciones significativas. En general, los datos no siguen una distribución normal, por lo que se recomienda utilizar pruebas estadísticas no paramétricas para el análisis comparativo.

Hipótesis general

H0: La propuesta de plan de seguridad informática no mejora el nivel de seguridad de la información en la Dirección de Salud Virgen de Cocharcas en la provincia de Chincheros, 2024.

H1: La propuesta de plan de seguridad informática mejora el nivel de seguridad de la información en la Dirección de Salud Virgen de Cocharcas en la provincia de Chincheros, 2024

Tabla 24

Comparación pretest y postest sobre la percepción del plan de seguridad informática en la Dirección de Salud Virgen de Cocharcas.

Prueba de muestras emparejadas

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior	Superior			
La propuesta de plan de seguridad informática (independiente)_POS - La propuesta de plan de seguridad informática (independiente)_PRE	26.950	13.505	1.7435	23.46	30.439	15.4659		0.000

Tabla 25

Tamaños de efecto de muestras emparejadas.

		Standardizera	Estimación de puntos	Intervalo de confianza al 95%	
				Inferior	Superior
La propuesta de plan de seguridad informática (independiente)_POS - La propuesta de plan de seguridad informática (independiente)_PRE	d de Cohen	13.50508	1.996	1.553	2.432
	corrección de Hedges	13.59169	1.983	1.543	2.416

a. El denominador utilizado en la estimación de tamaños del efecto.
La d de Cohen utiliza la desviación estándar de muestra de la diferencia de medias.
La corrección de Hedges utiliza la desviación estándar de muestra de la diferencia de medias, más un factor de corrección.

La tabla 24, muestra los resultados de la prueba t para muestras emparejadas evidencian una mejora significativa en la percepción de la seguridad de la información tras la implementación del nuevo plan de seguridad informática en la Dirección de Salud Virgen de Cocharcas. La diferencia de medias entre el pos test y el pre test fue de 26.95 puntos, con una t = 15.46, gl = 59 y p = 0.000, lo que confirma un cambio altamente significativo. De la tabla 25, el tamaño del efecto calculado mediante la d de Cohen (1.996) y la corrección de Hedges (1.983) indica un efecto grande, demostrando que la propuesta tuvo un impacto considerable. Estos resultados muestran que los encuestados perciben una clara mejora en los niveles de seguridad de la información con el nuevo plan. Por lo tanto, se confirma la hipótesis de que la propuesta mejora significativamente la seguridad informática institucional.

Hipótesis especifica 01

H0: La propuesta de una norma de seguridad no mejora el nivel de seguridad de la información.

H1: La propuesta de una norma de seguridad mejora el nivel de seguridad de la información.

Tabla 26

Rangos de la prueba de Wilcoxon para la variable "Propuesta de una norma de seguridad" (pre y post test).

Rangos				
		N	Rango promedio	Suma de rangos
La propuesta de una norma de seguridad _PRE - La propuesta de una norma de seguridad _POS	Rangos negativos	18[a]	29.03	522.50
	Rangos positivos	39[b]	28.99	1130.50
	Empates	3[c]		

	Total	60

a. La propuesta de una norma de seguridad _PRE < La propuesta de una norma de seguridad _POS
b. La propuesta de una norma de seguridad _PRE > La propuesta de una norma de seguridad _POS
c. La propuesta de una norma de seguridad _PRE = La propuesta de una norma de seguridad _POS

Tabla 27

Estadísticos de prueba de Wilcoxon para la variable "Propuesta de una norma de seguridad" (pre y post test)

Estadísticos de prueba[a]	
	La propuesta de una norma de seguridad _PRE - La propuesta de una norma de seguridad _POS
Z	-2,422[b]
Sig. asin. (bilateral)	0.015
r	-0.3127

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos negativos.

Los resultados de la prueba de rangos con signo de Wilcoxon muestran una diferencia significativa entre los resultados del pretest y el postest respecto a la variable "Propuesta de una norma de seguridad". Se observa que 39 participantes presentaron rangos positivos (mejoría en su percepción), frente a 18 rangos negativos (disminución) y 3 empates, lo que indica una tendencia general hacia la mejora. El valor obtenido de Z = -2.422 con una significación bilateral de p = 0.015 confirma que los cambios son estadísticamente significativos. Además, el tamaño del efecto r = -0.3127 sugiere un impacto moderado. En conjunto, los encuestados perciben que la implementación del nuevo plan con una norma de seguridad mejora el nivel de protección de la información. Por tanto, se acepta la hipótesis alterna, confirmando que la propuesta incrementa la seguridad informacional en la institución.

Hipótesis específica 02

H0: La propuesta de controles de seguridad no mejora el nivel de seguridad de la información.

H1: La propuesta de controles de seguridad mejora el nivel de seguridad de la información.

Tabla 28

Rangos de la prueba de Wilcoxon para la variable propuesta de controles de seguridad (pre y post test).

Rangos

		N	Rango promedio	Suma de rangos
La propuesta de controles de seguridad _PRE - La propuesta de controles de seguridad _POS	Rangos negativos	37[a]	32.27	1194.00
	Rangos positivos	18[b]	19.22	346.00
	Empates	5[c]		
	Total	60		

a. La propuesta de controles de seguridad _PRE < La propuesta de controles de seguridad _POS
b. La propuesta de controles de seguridad _PRE > La propuesta de controles de seguridad _POS
c. La propuesta de controles de seguridad _PRE = La propuesta de controles de seguridad _POS

Tabla 29

Estadísticos de prueba de Wilcoxon para la variable propuesta de controles de seguridad (pre y post test).

Estadísticos de prueba[a]	
	La propuesta de controles de seguridad _PRE - La propuesta de controles de seguridad _POS
Z	-3,559[b]
Sig. asin. (bilateral)	0.000
r	-0.4595

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

La tabla 28 muestra los resultados de la prueba de rangos con signo de Wilcoxon evidencian una diferencia significativa entre las mediciones del pretest y el postest en la variable “Propuesta de controles de seguridad”. Se observa que 37 participantes presentaron rangos negativos (mejor valoración en el postest), mientras que 18 mostraron rangos positivos y 5 mantuvieron el mismo nivel, lo que indica una percepción general de mejora tras la implementación del nuevo plan. La tabla 29, muestra el estadístico obtenido que fue Z = -3.559 con un valor de p = 0.000, lo que demuestra una diferencia altamente significativa. El tamaño del efecto r = -0.4595 señala un impacto moderado a grande, reforzando la eficacia de la propuesta. En síntesis, los encuestados consideran que el nuevo plan fortalece los mecanismos de control y protección de la información en la institución. Por lo tanto, se acepta la hipótesis alterna, confirmando que la propuesta mejora el nivel de seguridad de la información.

Hipótesis específica 03

H0: La propuesta de políticas y procedimientos de seguridad no mejora el nivel de seguridad de la información.

H1: La propuesta de políticas y procedimientos de seguridad mejora el nivel de seguridad de la información.

Tabla 30

Rangos de la prueba de Wilcoxon para la variable propuesta de políticas y procedimientos de seguridad (pre y post test).

Rangos				
		N	Rango promedio	Suma de rangos
La propuesta de políticas y procedimientos de seguridad _PRE - La propuesta de políticas y procedimientos de seguridad _POS	Rangos negativos	52[a]	31.79	1653.00
	Rangos positivos	6[b]	9.67	58.00
	Empates	2[c]		
	Total	60		

a. La propuesta de políticas y procedimientos de seguridad _PRE < La propuesta de políticas y procedimientos de seguridad _POS
b. La propuesta de políticas y procedimientos de seguridad _PRE > La propuesta de políticas y procedimientos de seguridad _POS
c. La propuesta de políticas y procedimientos de seguridad _PRE = La propuesta de políticas y procedimientos de seguridad _POS

Tabla 31

Estadísticos de prueba de Wilcoxon para la variable propuesta de controles de políticas y procedimientos (pre y post test).

Estadísticos de prueba[a]	
	La propuesta de políticas y procedimientos de seguridad _PRE - La propuesta de políticas y procedimientos de seguridad _POS
Z	-6,179[b]
Sig. asin. (bilateral)	0.000
r	-0.7977

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Los resultados de la prueba de rangos con signo de Wilcoxon muestran una diferencia altamente significativa entre el pretest y el postest en la variable “Propuesta de políticas y procedimientos de seguridad”. Se observa que 52 participantes presentaron rangos negativos (mejor percepción en el postest), frente a 6 rangos positivos y 2 empates, lo que evidencia una amplia percepción de mejora tras la aplicación del nuevo plan. El valor obtenido de Z = -6.179 y una significación p = 0.000 confirman que la diferencia es estadísticamente significativa. Asimismo, el tamaño del efecto r = -0.7977 indica un impacto grande, demostrando la efectividad del plan en fortalecer la gestión de políticas y procedimientos de seguridad. En general, los encuestados perciben que la nueva propuesta mejora de forma notable la organización, claridad y cumplimiento de las normas internas. Por lo tanto, se acepta la hipótesis H1, confirmando su eficacia.

Hipótesis específica 04

H0: La propuesta de concienciación en seguridad no mejora el nivel de seguridad de la información.

H1: La propuesta de concienciación en seguridad mejora el nivel de seguridad de la información.

Tabla 32

Rangos de la prueba de Wilcoxon para la variable propuesta de concienciación en seguridad (pre y post test).

Rangos				
		N	Rango promedio	Suma de rangos
La propuesta de concienciación en seguridad _PRE - La propuesta de concienciación en seguridad _POS	Rangos negativos	58[a]	31.38	1820.00
	Rangos positivos	2[b]	5.00	10.00
	Empates	0[c]		
	Total	60		

a. La propuesta de concienciación en seguridad _PRE < La propuesta de concienciación en seguridad _POS
b. La propuesta de concienciación en seguridad _PRE > La propuesta de concienciación en seguridad _POS
c. La propuesta de concienciación en seguridad _PRE = La propuesta de concienciación en seguridad _POS

Tabla 33

Estadísticos de prueba de Wilcoxon para la variable propuesta de concienciación en seguridad (pre y post test)

Estadísticos de prueba[a]	
	La propuesta de concienciación en seguridad _PRE - La propuesta de concienciación en seguridad _POS
Z	-6,665[b]
Sig. asin. (bilateral)	0.000
r	-0.8604478

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Los resultados de la prueba de rangos con signo de Wilcoxon revelan una diferencia altamente significativa entre los resultados del pretest y el postest en la variable “Propuesta de concienciación en seguridad”. De los 60 participantes, 58 mostraron rangos negativos, es decir, una mejor percepción tras la implementación del nuevo plan, mientras que solo 2 presentaron rangos positivos y no hubo empates. El valor obtenido de Z = -6.665 y una significación p = 0.000 confirman que el cambio es estadísticamente muy significativo. Asimismo, el tamaño del efecto r = -0.860 indica un

impacto muy grande, evidenciando que los encuestados perciben una notoria mejora en la cultura de seguridad y en la conciencia del personal sobre la protección de la información. En consecuencia, se acepta la hipótesis H1, confirmando que la propuesta de concienciación fortalece significativamente el nivel de seguridad de la información en la institución.

4.2. Discusión

Los resultados de la presente investigación evidencian que la propuesta de plan de seguridad informática basada en la norma ISO/IEC 27002:2022 produce una mejora significativa en el nivel de seguridad de la información en la Dirección de Salud “Virgen de Cocharcas”. La prueba t de Student para muestras emparejadas arrojó una diferencia de medias de 26.95 puntos ($t = 15.46$, $gl = 59$, $p = 0.000$), con un tamaño de efecto grande según la d de Cohen (1.996), lo que confirma la hipótesis general.

En relación con la dimensión de concienciación en seguridad, los resultados muestran el mayor impacto de la intervención, con un efecto muy grande ($r = –0.860$, $p = 0.000$). En el pretest, el 35% del personal calificó la concienciación como insuficiente; en el postest, el 83.33% la percibió de calidad. Estos hallazgos son consistentes con lo reportado por Huallpa (2020), quien documentó una mejora sustancial en el nivel de capacitación del personal tras la implementación de un SGSI basado en ISO/IEC 27001:2013 en la UNAMBA, y con Moya (2023), quien concluyó que el fomento de una cultura de seguridad es determinante para la eficacia de los controles implementados. La diferencia favorable observada en la presente investigación puede atribuirse al programa integral de formación —presencial y virtual— diseñado específicamente para las características del personal de la DISA.

Respecto a la dimensión de políticas y procedimientos de seguridad, la prueba de Wilcoxon reveló un efecto grande ($r = –0.798$, $p = 0.000$), con 52 de 60 participantes mostrando mejoras en su percepción. El porcentaje de trabajadores que calificó esta dimensión como “de calidad” pasó del 1.67% al 55.00%. Estos resultados coinciden con los hallazgos de Vílchez (2023), quien determinó que la implementación de un plan basado en ISO/IEC 27002:2013 contribuye significativamente al fortalecimiento de la seguridad informática en instituciones públicas, y con Delgado Ojeda (2024), quien evidenció que la ISO/IEC 27002:2022, con sus cuatro dominios reorganizados, resulta más práctica y eficaz para la implementación de controles. La mejora observada puede explicarse por la elaboración de documentos normativos claros y su difusión sistemática al personal.

En cuanto a la dimensión de controles de seguridad, si bien la prueba de Wilcoxon confirmó una diferencia significativa (Z = –3.559, p = 0.000, r = –0.460), los resultados descriptivos muestran una mejora moderada: el 46.67% del personal aún percibió los controles como insuficientes en el postest. Este hallazgo es coherente con lo reportado por Abad y Cruz (2022), quienes documentaron mejoras significativas pero diferenciadas entre las dimensiones de confidencialidad, integridad y disponibilidad tras la aplicación de la ISO/IEC 27002:2013 en la UGEL Utcubamba. La percepción moderada en esta dimensión puede explicarse porque los controles técnicos requieren tiempo para su plena implementación y el personal necesita experimentar sus beneficios operativos para modificar su percepción.

Respecto a la dimensión de norma de seguridad, la prueba de Wilcoxon mostró un efecto moderado (r = –0.313, p = 0.015), siendo la dimensión con menor magnitud de cambio. El 45% del personal calificó la norma como insuficiente en el postest, frente al 11.67% del pretest. Estos resultados mixtos coinciden con lo señalado por Rumiche (2021), quien identificó que el desconocimiento de estándares de seguridad por parte del personal constituye una barrera persistente, y con Carrillo García (2023), quien evidenció que la adopción de marcos normativos requiere un proceso gradual de socialización y apropiación institucional. La paradoja del incremento en la categoría “insuficiente” en el postest puede interpretarse como un efecto de sensibilización: al conocer la norma ISO/IEC 27002:2022, el personal adquiere mayor conciencia de las brechas existentes y evalúa con mayor rigor el estado actual de la seguridad.

Los hallazgos de la presente investigación aportan evidencia empírica sobre la viabilidad de implementar planes de seguridad informática basados en estándares internacionales en instituciones de salud de entornos rurales con recursos limitados, un área poco documentada en la literatura científica peruana. A diferencia de estudios previos que utilizaron la versión 2013 de la norma (Vílchez, 2023; Abad y Cruz, 2022; Huallpa, 2020), esta investigación emplea la versión actualizada ISO/IEC 27002:2022, que reorganiza los controles en cuatro dominios —organización, personas, objetos físicos y tecnología—, lo que facilita una implementación más sistemática y adaptada al contexto institucional, como también lo demostró Delgado Ojeda (2024) en el sector tecnológico ecuatoriano.

No obstante, es necesario señalar limitaciones del estudio: el diseño preexperimental sin grupo de control limita la validez interna de las inferencias causales, y los índices

de ajuste del análisis factorial confirmatorio (CFI = 0.739, RMSEA = 0.13) no alcanzaron valores óptimos, lo que sugiere que la estructura factorial del instrumento requiere refinamiento en futuras investigaciones. Asimismo, el tamaño reducido de la muestra (N = 60) y la naturaleza censal del estudio limitan la generalización de los resultados a otras instituciones de salud.

V. CONCLUSIONES

Primera. La propuesta de plan de seguridad informática basada en la norma ISO/IEC 27002:2022 mejora significativamente el nivel de seguridad de la información en la Dirección de Salud “Virgen de Cocharcas” de la provincia de Chincheros, 2024, evidenciado por una diferencia de medias de 26.95 puntos entre el postest y el pretest ($t = 15.46$, $gl = 59$, $p = 0.000$), con un tamaño de efecto grande (d de Cohen = 1.996). La percepción del nivel de seguridad pasó de 58.33% insuficiente a 68.33% aceptable y 31.67% de calidad tras la propuesta.

Segunda. La propuesta de una norma de seguridad basada en la ISO/IEC 27002:2022 mejora el nivel de seguridad de la información, con una diferencia estadísticamente significativa según la prueba de Wilcoxon ($Z = –2.422$, $p = 0.015$) y un tamaño de efecto moderado ($r = –0.313$). Se identificó que 39 de 60 participantes presentaron mejora en su percepción, aunque la dimensión requiere mayor fortalecimiento dado que el 45% aún la percibió como insuficiente en el postest, lo que refleja un proceso de sensibilización crítica del personal.

Tercera. La propuesta de controles de seguridad mejora significativamente el nivel de seguridad de la información, demostrado por la prueba de Wilcoxon ($Z = –3.559$, $p = 0.000$) con un tamaño de efecto moderado a grande ($r = –0.460$). De los 60 participantes, 37 mostraron mejora en su percepción. Se implementaron 12 controles distribuidos en los cuatro dominios de la norma ISO/IEC 27002:2022: organización (3 controles), personas (3 controles), objetos físicos (3 controles) y tecnología (3 controles), seleccionados según las necesidades críticas de la DISA.

Cuarta. La propuesta de políticas y procedimientos de seguridad mejora significativamente el nivel de seguridad de la información, con la prueba de Wilcoxon mostrando la segunda mayor magnitud de efecto ($Z = –6.179$, $p = 0.000$, $r = –0.798$). El porcentaje de trabajadores que calificó esta dimensión como “de calidad” pasó del 1.67% en el pretest al 55.00% en el postest, evidenciando que la elaboración de documentos normativos claros y su difusión sistemática al personal produce un impacto favorable en la percepción de la seguridad institucional.

Quinta. La propuesta de concienciación en seguridad produce la mayor mejora en el nivel de seguridad de la información, con un efecto muy grande según la prueba de Wilcoxon ($Z = –6.665$, $p = 0.000$, $r = –0.860$). De los 60 participantes, 58 mostraron mejora en su percepción, pasándose de 35% insuficiente y 65% aceptable en el

pretest a 83.33% de calidad en el postest, lo que confirma que la capacitación y sensibilización del personal constituyen el pilar más efectivo del plan de seguridad informática propuesto.

RECOMENDACIONES

Primera. A la Dirección de la DISA “Virgen de Cocharcas”, se recomienda institucionalizar el plan de seguridad informática propuesto mediante una resolución directoral que establezca su carácter obligatorio, asigne presupuesto específico para su sostenimiento y designe formalmente al responsable de la Unidad de Estadística e Informática como oficial de seguridad de la información.

Segunda. A la Unidad de Estadística e Informática de la DISA, se recomienda ampliar progresivamente la cobertura de controles ISO/IEC 27002:2022 implementados, pasando de los 12 controles actuales a un mínimo de 25 controles en un horizonte de dos años, priorizando los dominios de tecnología y organización que presentaron menor percepción de mejora.

Tercera. A la Dirección de la DISA, se recomienda implementar un programa permanente de capacitación y sensibilización en seguridad de la información, con frecuencia trimestral como mínimo, dado que la dimensión de concienciación mostró el mayor impacto en la mejora del nivel de seguridad ($r = –0.860$).

Cuarta. A la Unidad de Estadística e Informática, se recomienda implementar herramientas SIEM de código abierto (Wazuh, OSSEC o Graylog) para el monitoreo continuo de eventos de seguridad, así como fortalecer la infraestructura tecnológica con la adquisición de UPS para todos los equipos críticos y la implementación de VPN con autenticación de dos factores para el trabajo remoto.

Quinta. A los investigadores en seguridad informática y sistemas de información en salud, se recomienda realizar estudios con diseños cuasiexperimentales o experimentales que incluyan grupo de control, y con muestras de mayor tamaño, para fortalecer la validez interna y la generalización de los hallazgos. Asimismo, se recomienda refinar el instrumento de medición para mejorar los índices de ajuste del modelo factorial.

Sexta. A la Escuela Profesional de Ingeniería de Sistemas de la UNSCH, se recomienda incorporar la seguridad de la información en instituciones de salud como línea de investigación, promoviendo la formación de competencias en análisis de riesgos, implementación de controles ISO 27002 y auditoría de sistemas de información sanitaria.

Referencias bibliográficas

Abad, J. y Cruz, L. (2022). Mejora de la seguridad informática mediante la aplicación de la norma ISO/IEC 27002:2013 en la UGEL Utcubamba [Tesis de pregrado, Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas]. Repositorio Institucional UNTRM.

Aguilar Villanueva, L. (2015). Gobernanza y gestión pública. Fondo de Cultura Económica.

ALTAOS. (2017). ISO 27002.

Arias, F. G. (2012). El proyecto de investigación: Introducción a la metodología científica (6.ª ed.). Editorial Episteme.

Bhaskar, R., & Kapoor, B. (2013). Manual de seguridad informática y de la información (segunda edición). Aravaca, Madrid: McGraw-Hill Interamericana de España, S.L.

Carrillo García, A. (2023). Análisis de seguridad de la información aplicando la norma ISO/IEC 27001 en una empresa de transacciones interbancarias [Tesis de maestría, Universidad Técnica de Ambato]. Repositorio Institucional UTA.

Cochran, W. G. (1977). Sampling techniques (3rd ed.). John Wiley & Sons.

Congreso de la República. (2011). Ley N.° 29733 – Ley de Protección de Datos Personales. Diario Oficial El Peruano.

Congreso de la República del Perú. (2013). Normas Legales del Congreso de la República del Perú.

Constantinescu, R. (2006). Planificación de la seguridad en los sistemas de TI. Academia de Estudios Económicos - Bucarest, Rumania, 81–85.

De La Torre Yamberla, J. (2024). Plan de SGSI aplicando el estándar ISO/IEC 27001 para fortalecer la disponibilidad de los servicios en la Cooperativa de Ahorro y Crédito Imbacoop Ltda. [Tesis de pregrado, Universidad Técnica del Norte]. Repositorio Institucional UTN.

Delgado Ojeda, D. (2024). Diseño de un SGSI basado en las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 para Airmaxtelecom Soluciones Tecnológicas S.A. [Tesis de maestría, Pontificia Universidad Católica del Ecuador]. Repositorio Institucional PUCE.

Direccion de Salud Virgen de Cocharcas - Chincheros. (2022). Portal de Transparencia.

Fitzgerald, M. (2007). Administración de la seguridad de la información. México D.F., México: McGraw-Hill Interamericana.

Fuel Rodríguez, M. (2024). Implementación de un sistema de protección de datos personales integrando ISO/IEC 27001:2022, ISO/IEC 27002:2022 e ISO/IEC 27701:2019 en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega [Tesis de

maestría, Universidad Técnica del Norte]. Repositorio Institucional UTN.

Gobierno del Perú. (2018). Decreto Supremo N° 003-2018-PCM/SGP.

Hernández-Sampieri, R., Fernández-Collado, C. y Baptista-Lucio, M. P. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill.

Huallpa, E. (2020). Mejora de la seguridad de la información mediante la implementación de un SGSI basado en la norma ISO/IEC 27001:2013 en la DTI de la Universidad Nacional Micaela Bastidas de Apurímac [Tesis de pregrado, UNAMBA]. Repositorio Institucional UNAMBA.

INDECOPI. (2014). Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.

International Organization for Standardization. (2022a). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.

International Organization for Standardization. (2022b). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. ISO.

ISO Tools. (2020). Evaluación de Riesgos de Seguridad de la Información según la ISO 27001.

ISO/IEC. (2018). Organización Internacional de Normalización.

Jaime Miranda, M. (2015). Métodos de investigación en ciencias de la salud: Diseños de estudio. Ediciones de la U.

Joyanes Aguilar, L. (2010). Ciberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia, (149), 11–68.

Khan, M. (2024). Concientización sobre la ciberseguridad. Revista científica india de investigación en ingeniería y gestión, 1-14.

Mauwa, E. (01 de 01 de 2007). Concienciación sobre seguridad de la información: contenidos genéricos, herramientas y técnicas.

McCumber, R. (2002). Construyendo una Red Segura. Upper Saddle River, New Jersey: Pearson Education.

Méndez, A. (2024). El análisis factorial: una introducción conceptual para la enseñanza y aprendizaje. Revista del Consejo Nacional para la Enseñanza e Investigación en Psicología, 2-10.

Merino, J. (2021). Plan de seguridad informática basado en la norma ISO/IEC 27001 en RANSA Comercial S.A. – Piura [Tesis de pregrado, Universidad César Vallejo]. Repositorio Institucional UCV.

Ministerio de Salud. (2019). Resolución Ministerial N° 005-2019/MINSA - Aprueba la Directiva para la Gestión de la Seguridad de la Información en el Sector Salud.

Diario Oficial El Peruano.

MINSA. (2018). Resolución Ministerial N.° 214-2018/MINSA – Norma técnica de salud para la gestión de la historia clínica. Diario Oficial El Peruano.

MINSA. (2020). Directiva Administrativa N.° 294-MINSA/2020/OGTI – Tratamiento de datos personales relacionados con la salud. Diario Oficial El Peruano.

Moya, A. (2023). Plan de seguridad informática basado en ISO/IEC 27001:2013 y metodología MAGERIT para la EP-EMAPA de Ambato [Tesis de maestría, Universidad Técnica de Ambato]. Repositorio Institucional UTA.

Murray, W., Ulmer, W., & Ranade, D. (2007). Gestión de la seguridad de la información: un enfoque de gestión de riesgos. Nueva York: Wiley & Sons, Inc.

Roa Buendía, J. F. (2013). Seguridad informática. España: ISBN edición.

Rumiche Huamani, E. (2021). Plan de seguridad informática para la Corte Superior de Justicia de Lima [Tesis de pregrado, Universidad Nacional Federico Villarreal]. Repositorio Institucional UNFV.

Ruiz Olabuenága, J. I. (2012). Metodología de la investigación cualitativa (5.ª ed.). Universidad de Deusto.

Scolnik, H. D. (2016). Qué es la seguridad informática. Ciudad Autónoma de Buenos Aires, Argentina: Paidós.

Steinberg, J. (2022). Ciberseguridad para Dummies. Nueva Jersey: John Wiley & Sons, Inc.

Taylor, A., Alexander, D., Finch, A., & Sutton, D. (2020). Information Security Management Principles. BCS, The Chartered Institute for IT1.

Triola, M. F. (2013). Estadística (11.ª ed.). Pearson Educación.

Vílchez Guevara, J. (2023). Plan de seguridad informática conforme a la norma ISO/IEC 27002:2013 para la Municipalidad Distrital de San Juan Bautista [Tesis de pregrado, Universidad Nacional de San Cristóbal de Huamanga]. Repositorio Institucional UNSCH.

Vega Briceño, E. (2021). SEGURIDAD DE LA INFORMACIÓN. Alicante, Valencia: Área de Innovación y Desarrollo,S.L.

Velásquez Henao, J. M. (2016). Gestión de la Seguridad de la Información. Bogota , Colombia: ECOE Ediciones.

Viteri Peñafiel, C. P. (2022). Linkedin.

Whitman, M. E., & Mattord, H. J. (2009). Principios de seguridad de la información. Boston, Massachusetts. : Cengage Learning.

Lista de abreviaturas

AFC	:	Análisis Factorial Confirmatorio
AFE	:	Análisis Factorial Exploratorio
AIC	:	Criterio de Información de Akaike
BIC	:	Criterio de Información Bayesiano
CAP	:	Cuadro de Asignación de Personal
CCTV	:	Circuito Cerrado de Televisión
CFI	:	Comparative Fit Index (Índice de Ajuste Comparativo)
DISA	:	Dirección de Salud
HTTPS	:	Hypertext Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)
ISO	:	International Organization for Standardization (Organización Internacional de Normalización)
ISO/IEC 27001	:	Norma internacional para sistemas de gestión de seguridad de la información
ISO/IEC 27002	:	Norma internacional de controles de seguridad de la información
MAGERIT	:	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MINSA	:	Ministerio de Salud del Perú
OSSEC	:	Open Source Security (Sistema de detección de intrusiones de código abierto)
PDCA	:	Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar)
RMSEA	:	Root Mean Square Error of Approximation (Error Cuadrático Medio de Aproximación)
SFTP	:	Secure File Transfer Protocol (Protocolo Seguro de Transferencia de Archivos)
SGSI	:	Sistema de Gestión de Seguridad de la Información
SIEM	:	Security Information and Event Management (Gestión de Eventos e Información de Seguridad)
SIGA	:	Sistema Integrado de Gestión Administrativa
SIAF	:	Sistema Integrado de Administración Financiera
SRMR	:	Standardized Root Mean Square Residual
TLI	:	Tucker-Lewis Index (Índice de Tucker-Lewis)
UGEL	:	Unidad de Gestión Educativa Local
UPS	:	Uninterruptible Power Supply (Sistema de Alimentación

		Ininterrumpida)
VPN	:	Virtual Private Network (Red Privada Virtual)
2FA	:	Two-Factor Authentication (Autenticación de Dos Factores)

Glosario

Análisis factorial confirmatorio (AFC). Técnica estadística multivariante que evalúa si un modelo teórico de factores latentes se ajusta adecuadamente a los datos empíricos observados, mediante índices de bondad de ajuste (Hernández-Sampieri et al., 2014).

Análisis factorial exploratorio (AFE). Técnica estadística que identifica la estructura subyacente de un conjunto de variables observadas, agrupando ítems correlacionados en factores latentes sin una estructura previa definida.

Concienciación en seguridad. Grado de conocimiento y sensibilización del personal respecto a los riesgos de seguridad y las prácticas necesarias para proteger la información institucional (ISO/IEC 27002:2022).

Confidencialidad. Propiedad de la información que garantiza que esta sea accesible únicamente por personas o sistemas autorizados, evitando su divulgación no autorizada (ISO/IEC 27002:2022).

Controles de seguridad. Medidas técnicas, administrativas y físicas implementadas para prevenir, detectar y responder a incidentes de seguridad que puedan comprometer la información o los sistemas informáticos.

d de Cohen. Medida estandarizada del tamaño del efecto que indica la magnitud de la diferencia entre dos medias en unidades de desviación estándar; valores de 0.2, 0.5 y 0.8 se interpretan como efecto pequeño, mediano y grande, respectivamente.

Diseño preexperimental. Diseño de investigación que evalúa el efecto de una intervención mediante mediciones antes y después del tratamiento, sin incluir grupo de control (Hernández-Sampieri et al., 2014).

Disponibilidad. Propiedad de la información que asegura que los datos y sistemas estén accesibles y operativos cuando los usuarios autorizados los requieran, sin interrupciones no planificadas (ISO/IEC 27002:2022).

Integridad. Propiedad de la información que garantiza que los datos se mantengan exactos, completos y sin alteraciones no autorizadas durante su almacenamiento, procesamiento y transmisión (ISO/IEC 27002:2022).

ISO/IEC 27002:2022. Norma internacional que proporciona un catálogo de controles de seguridad de la información organizados en cuatro dominios: organización, personas, objetos físicos y tecnología, con 93 controles en total.

Norma de seguridad. Marco institucional que regula y estandariza los procesos de seguridad de la información, estableciendo requisitos mínimos para la gestión de riesgos y la protección de activos informáticos.

Plan de seguridad informática. Conjunto estructurado de normas, controles, políticas, procedimientos y estrategias de concienciación orientados a proteger la

confidencialidad, integridad y disponibilidad de la información institucional.

Políticas de seguridad. Lineamientos formales y documentados que establecen las directrices, responsabilidades y procedimientos que debe seguir el personal para garantizar la protección de la información.

Prueba de Wilcoxon. Prueba estadística no paramétrica para muestras relacionadas que compara las medianas de dos mediciones realizadas al mismo grupo, utilizada cuando los datos no cumplen el supuesto de normalidad.

Prueba t de Student. Prueba estadística paramétrica que compara las medias de dos mediciones realizadas al mismo grupo (muestras emparejadas), utilizada cuando los datos cumplen el supuesto de normalidad.

Seguridad de la información. Disciplina que abarca el conjunto de medidas preventivas, detectivas y correctivas orientadas a proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas de una organización.

SIEM. Sistema de gestión de eventos e información de seguridad que centraliza la recolección, correlación y análisis de registros de múltiples fuentes para detectar amenazas y eventos anómalos en tiempo real.

V de Aiken. Coeficiente estadístico que cuantifica la validez de contenido de un instrumento a partir de las valoraciones de jueces expertos, con valores entre 0 y 1 (Aiken, 1985).

Anexos

Anexo 1. Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	MÉTODO DE INVESTIGACIÓN
PROBLEMA GENERAL ¿Cómo es el plan de seguridad informática que mejora el nivel de la seguridad de la información en la Dirección de Salud Virgen de Cocharcas en la provincia de Chincheros, 2024? PROBLEMAS ESPECÍFICOS a. ¿Cómo es la norma de seguridad que mejora el nivel de seguridad de la información? b. ¿Cómo son los controles de seguridad que mejora el nivel de seguridad de la información? c. ¿Cómo son las políticas y procedimientos de seguridad que mejora el nivel de seguridad de la información? d. ¿Cómo es la concienciación en seguridad que mejora el nivel de seguridad de la información?	OBJETIVO GENERAL Desarrollar una propuesta de plan de seguridad informática que mejora el nivel de seguridad de la información en la Dirección de Salud Virgen de Cocharcas en la provincia de Chincheros, 2024 OBJETIVOS ESPECÍFICOS a. Identificar la norma de seguridad que mejora el nivel de seguridad de la información. b. Identificar los controles de seguridad que mejora el nivel de seguridad de la información. c. Diseñar las políticas y procedimientos de seguridad que mejora el nivel de seguridad de la información. d. Diseñar la concienciación en seguridad que mejora el nivel de seguridad de la información.	HIPÓTESIS GENERAL La propuesta de plan de seguridad informática mejora el nivel de seguridad de la información en la Dirección de Salud Virgen de Cocharcas en la provincia de Chincheros, 2024 HIPÓTESIS ESPECÍFICAS a. La propuesta de una norma de seguridad mejora el nivel de seguridad de la información. b. La propuesta de controles de seguridad mejora el nivel de seguridad de la información. c. La propuesta de políticas y procedimientos de seguridad mejora el nivel de seguridad de la información. d. La propuesta de concienciación en seguridad mejora el nivel de seguridad de la información.	VARIABLE INDEPENDIENTE X: Plan de seguridad informática DIMENSIONES X1: Norma de seguridad X2: Controles de seguridad X3: Políticas y procedimientos de seguridad. X4: Concienciación en seguridad. VARIABLE DEPENDIENTE Y: Nivel de seguridad de la información. DIMENSIONES Y1: Confidencialidad de la información. Y2: Integridad de la información. Y3: Disponibilidad de la información.	TIPO DE INVESTIGACIÓN Experimental, prospectivo, longitudinal, analítico. NIVEL DE INVESTIGACIÓN Aplicativo. DISEÑO Pre experimental. POBLACIÓN La población comprende un total de 60 trabajadores, los cuales son específicamente 38 trabajadores del área administrativa y 22 trabajadores de las coordinaciones de salud, que laboran en la Dirección de Salud Virgen de Cocharcas – Chincheros, 2024. MUESTRA No existe muestra, será un censo, porque se estudia al personal administrativo y de coordinación de salud compuesto por 38 y 22 personas respectivamente en la Dirección de Salud Virgen de Cocharcas de la provincia de Chincheros, 2024 TÉCNICA Encuesta INSTRUMENTO Cuestionario

Anexo 2. Instrumento de recolección de datos

CUESTIONARIO SOBRE NIVEL DE SEGURIDAD DE LA INFORMACIÓN

Dirección de Salud "Virgen de Cocharcas" – Provincia de Chincheros

Estimado(a) trabajador(a): El presente cuestionario tiene como objetivo evaluar su percepción sobre el nivel de seguridad de la información en la DISA "Virgen de Cocharcas". Sus respuestas serán tratadas de manera confidencial y anónima, y se utilizarán exclusivamente con fines académicos.

Instrucciones: Marque con una "X" la opción que mejor refleje su opinión para cada enunciado, utilizando la siguiente escala: 1 = Totalmente en desacuerdo, 2 = En desacuerdo, 3 = Ni de acuerdo ni en desacuerdo, 4 = De acuerdo, 5 = Totalmente de acuerdo.

Área: _____ **Fecha:** _____

N.°	Enunciado	1	2	3	4	5
Dimensión Y1: Confidencialidad de la Información						
1	¿Cree que la DISA toma medidas efectivas para evitar accesos no autorizados a la información?					
2	¿Considera que se llevan a cabo revisiones suficientes para detectar accesos no autorizados a la información en la DISA?					
3	¿Está de acuerdo en que las capacitaciones sobre protección de la información son necesarias para el personal de la DISA?					
4	¿Cree que sería útil que la DISA implemente un programa de capacitación regular sobre seguridad de la información?					
5	¿Está de acuerdo en que es importante que el personal de la DISA reciba y lea las políticas de seguridad de la información?					
6	¿Cree que la DISA debería implementar políticas claras sobre la seguridad de la información y					

	asegurar su difusión al personal?					
7	¿Considera que es esencial que todos los equipos de la DISA tengan software antivirus actualizado?					
8	¿Cree que el software antivirus instalado en los equipos de la DISA es adecuado para protegerlos contra amenazas de seguridad?					
9	¿Cree que la gestión y protección de las contraseñas en la DISA es adecuada y segura?					
10	¿Está de acuerdo en que es importante implementar procedimientos claros para el cambio regular de contraseñas en la DISA?					
Dimensión Y2: Integridad de la Información						
11	¿Está de acuerdo en que el control de acceso a la información en la DISA es efectivo para prevenir accesos no autorizados?					
12	¿Cree que la DISA debería implementar auditorías periódicas para detectar accesos no autorizados?					
13	¿Está de acuerdo en que la DISA realiza copias de seguridad de la información de manera regular y segura?					
14	¿Cree que la DISA está preparada para recuperar la información de manera efectiva en caso de pérdida o daño de los datos?					
15	¿Cree que la DISA detecta rápidamente los cambios no autorizados en la información?					
16	¿Está de acuerdo en que la DISA responde de manera oportuna cuando se identifican problemas o alteraciones en la información?					
17	¿Está de acuerdo en que la firma digital es una herramienta importante para garantizar la autenticidad de los documentos en la DISA?					
18	¿Considera necesario implementar el uso de firmas					

	digitales en los procesos clave de la DISA?					
19	¿Cree que la DISA toma las medidas necesarias para evitar modificaciones no autorizadas en los datos?					
20	¿Está de acuerdo en que se deberían implementar mejores medidas para detectar cambios no autorizados en los datos de la DISA?					
Dimensión Y3: Disponibilidad de la Información						
21	¿Está de acuerdo en que la DISA restaura rápidamente los servicios tras una interrupción?					
22	¿Cree que la comunicación sobre interrupciones del servicio en la DISA es oportuna y clara para el personal?					
23	¿Está de acuerdo en que los sistemas críticos de la DISA están disponibles la mayor parte del tiempo y funcionan sin problemas?					
24	¿Cree que la DISA debería implementar medidas adicionales para garantizar la operación continua de los sistemas críticos?					
25	¿Está de acuerdo en que los UPS instalados en la DISA son efectivos para prevenir interrupciones durante cortes de energía?					
26	¿Considera necesario implementar sistemas redundantes para asegurar el funcionamiento continuo en caso de fallas del servidor principal de la DISA?					
27	¿Está de acuerdo en que el mantenimiento regular de los equipos de la DISA es efectivo para prevenir fallas?					
28	¿Cree que se deberían realizar revisiones más frecuentes para evitar problemas en los equipos de la DISA?					

29	¿Está de acuerdo en que la DISA monitorea adecuadamente el estado de los equipos para prevenir fallos?					
30	¿Cree que sería útil recibir alertas automáticas cuando hay problemas con los equipos de la DISA?					

Anexo 3. Formato de validez de contenido del instrumento por Juicio de expertos

Instrumento: Cuestionario sobre nivel de seguridad de la información

Variable: Y – Nivel de seguridad de la información

Datos del experto evaluador

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

Especialidad del validador: ……

Instrucciones: Estimado(a) experto(a), sírvase evaluar cada ítem del instrumento según los tres criterios indicados. Asigne una valoración de 1 a 4 donde:

1 = No cumple el criterio 2 = Bajo nivel 3 = Moderado nivel 4 = Alto nivel

P = Pertinencia: *El ítem corresponde al concepto teórico formulado.*

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

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

N.°	Nivel de seguridad de la Información	P	R	C	Sugerencias
Dimensión Y1: Confidencialidad de la Información					
1	¿Cree que la DISA toma medidas efectivas para evitar accesos no autorizados a la información?				
2	¿Considera que se llevan a cabo revisiones suficientes para detectar accesos no autorizados a la información en la DISA?				
3	¿Está de acuerdo en que las capacitaciones sobre protección de la información son necesarias para el personal de la DISA?				
4	¿Cree que sería útil que la DISA implemente un programa de capacitación regular sobre seguridad de la información?				
5	¿Está de acuerdo en que es importante que el personal de la DISA reciba y lea las políticas de seguridad de la información?				
6	¿Cree que la DISA debería implementar políticas claras sobre la seguridad de la información y asegurar su difusión al personal?				
7	¿Considera que es esencial que todos los equipos de				

	la DISA tengan software antivirus actualizado?				
8	¿Cree que el software antivirus instalado en los equipos de la DISA es adecuado para protegerlos contra amenazas de seguridad?				
9	¿Cree que la gestión y protección de las contraseñas en la DISA es adecuada y segura?				
10	¿Está de acuerdo en que es importante implementar procedimientos claros para el cambio regular de contraseñas en la DISA?				
Dimensión Y2: Integridad de la Información					
11	¿Está de acuerdo en que el control de acceso a la información en la DISA es efectivo para prevenir accesos no autorizados?				
12	¿Cree que la DISA debería implementar auditorías periódicas para detectar accesos no autorizados?				
13	¿Está de acuerdo en que la DISA realiza copias de seguridad de la información de manera regular y segura?				
14	¿Cree que la DISA está preparada para recuperar la información de manera efectiva en caso de pérdida o daño de los datos?				
15	¿Cree que la DISA detecta rápidamente los cambios no autorizados en la información?				
16	¿Está de acuerdo en que la DISA responde de manera oportuna cuando se identifican problemas o alteraciones en la información?				
17	¿Está de acuerdo en que la firma digital es una herramienta importante para garantizar la autenticidad de los documentos en la DISA?				
18	¿Considera necesario implementar el uso de firmas digitales en los procesos clave de la DISA?				
19	¿Cree que la DISA toma las medidas necesarias para evitar modificaciones no autorizadas en los datos?				
20	¿Está de acuerdo en que se deberían implementar mejores medidas para detectar cambios no autorizados en los datos de la DISA?				
Dimensión Y3: Disponibilidad de la Información					

21	¿Está de acuerdo en que la DISA restaura rápidamente los servicios tras una interrupción?				
22	¿Cree que la comunicación sobre interrupciones del servicio en la DISA es oportuna y clara para el personal?				
23	¿Está de acuerdo en que los sistemas críticos de la DISA están disponibles la mayor parte del tiempo y funcionan sin problemas?				
24	¿Cree que la DISA debería implementar medidas adicionales para garantizar la operación continua de los sistemas críticos?				
25	¿Está de acuerdo en que los UPS instalados en la DISA son efectivos para prevenir interrupciones durante cortes de energía?				
26	¿Considera necesario implementar sistemas redundantes para asegurar el funcionamiento continuo en caso de fallas del servidor principal de la DISA?				
27	¿Está de acuerdo en que el mantenimiento regular de los equipos de la DISA es efectivo para prevenir fallas?				
28	¿Cree que se deberían realizar revisiones más frecuentes para evitar problemas en los equipos de la DISA?				
29	¿Está de acuerdo en que la DISA monitorea adecuadamente el estado de los equipos para prevenir fallos?				
30	¿Cree que sería útil recibir alertas automáticas cuando hay problemas con los equipos de la DISA?				

Opinión de aplicabilidad:

( ) Aplicable ( ) Aplicable después de corregir ( ) No aplicable

Ayacucho…… de …… del 2025

……

Firma del Experto

Anexo 4. Validez de contenido del instrumento por Juicio de expertos

COEFICIENTE V DE AIKEN POR ÍTEM, CRITERIO Y EXPERTO

n = 5 Jueces

k = 1 (escala dicotómica: 0 = No, 1 = Sí)

V = S / [n(k)]

Dimensión	V Aiken Relevancia	V Aiken Representatividad	V Aiken Claridad	V Aiken Global
Y1: Confidencialidad	0.98	0.96	0.96	**0.97**
Y2: Integridad	0.98	0.98	0.96	**0.97**
Y3: Disponibilidad	0.96	1.00	1.00	**0.99**
Promedio global	**0.97**	**0.98**	**0.97**	**0.97**

Nota. *Valores calculados a partir de las valoraciones de 5 jueces expertos con escala dicotómica (0 = No, 1 = Sí). Todos los coeficientes superan el valor crítico de 0.80, confirmando la validez de contenido del instrumento.*

Interpretación. El coeficiente V de Aiken global del instrumento es 0.97, con valores por criterio de: Relevancia = 0.97, Representatividad = 0.98, Claridad = 0.97. Todos los coeficientes superan el valor crítico de 0.80 para n = 5 jueces (Aiken, 1985), lo que confirma la alta validez de contenido del instrumento. Los valores individuales por ítem oscilaron entre 0.80 y 1.00, evidenciando un alto grado de acuerdo entre los jueces evaluadores. Los ítems con V = 0.80 (4 de 90 evaluaciones) corresponden a casos donde un juez emitió valoración negativa, sin comprometer la validez global del instrumento.

Anexo 5 Confiabilidad del instrumento de recolección de datos

Resumen de procesamiento de casos

		N	%
Casos	Válido	60	100,0
	Excluido[a]	0	,0
	Total	60	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,906	30

Anexo 6 Plan de mantenimiento preventivo y correctivo

GOBIERNO REGIONAL APURÍMAC

DIRECCIÓN DE SALUD VIRGEN DE COCHARCAS-CHINCHEROS

DIRECCION DE SALUD VIRGEN DE COCHARCAS CHINCHEROS

PLAN DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIPOS INFORMATICOS DE LA DIRECCION DE SALUD "VIRGEN DE COCHARCAS" - CHINCHEROS

UNIDAD DE ESTADISTICA E INFORMATICA

Dirección: Espaldas de la Municipalidad –Chincheros Ex Jardín de Niños/Teléf. 983686892

http://www.risvirgendecocharcas.gob.pe/ gmail-disachincheros035@gmail.com

Contenido

INTRODUCCION

El presente documento constituye un plan de trabajo, que propone la elaboración y ejecución de un Plan de Mantenimiento para los Equipos Informáticos de la Dirección de Salud Virgen de Cocharcas.

La Unidad de Estadística e Informática se ve en la tarea de establecer planes de mantenimiento para evitar la falla de los equipos, encontrar y corregir algunas dificultades antes de que estos provoquen daños mayores. Su finalidad es mantener los equipos en estado óptimo y operativo.

La Unidad responsable de este documento es la Unidad de estadística e informática por lo tanto cualquier duda sobre el documento podrán hacerla saber a dicha Unidad.

1. **OBJETIVO GENERAL**

   Mantener en óptimas condiciones los equipos informáticos y de telecomunicaciones, mediante la implementación del mantenimiento preventivo de hardware y software, a fin de mantener la continuidad de las operaciones de los usuarios en sus labores cotidianas.

2. **OBJETIVOS ESPECIFICOS**

   a) Establecer una programación para la ejecución de los mantenimientos preventivos
   b) Realizar el mantenimiento de los equipos informáticos
   c) Disminuir los costos por fallas de los equipos informáticos
   d) Mejorar la eficiencia y eficacia en el soporte tecnológico de los equipos
   e) Establecer los mecanismos para evaluar condiciones generales de los equipos informáticos

3. **AMBITO DE APLICACIÓN**

   El mantenimiento preventivo se realizará a todos los equipos informáticos pertenecientes a la Dirección de Salud Virgen de Cocharcas.

4. **ETAPAS DEL PLAN**

   a) Adquisición de insumos para mantenimientos: En este punto se llevará a cabo un inventario de los insumos de mantenimiento de equipo informático y se determinará la cantidad correspondiente para los mantenimientos del año.
   b) Elaboración de la programación para la ejecución de los mantenimientos preventivos y correctivos.
   c) Ejecución del mantenimiento: en este se desarrolla de forma estructurada en base al equipo informático.
   d) Evaluación del plan: Este plan se evaluará una vez en el año, en el mes de febrero.

      La evaluación se realizará con base a los datos recolectados en el cuadro "Registro de mantenimientos" **(ver Anexo 1)**.

5. **DEFINICION**

   Mantenimiento preventivo es la actividad que garantiza la existencia de un servicio dentro de una calidad esperada. Para ello se elaboró un plan de trabajo con respecto al mantenimiento de los equipos informáticos. Así mismo, minimiza la tasa de fallas y eleva la productividad de los equipos.

6. DIAGNOSTICO SITUACIONAL

Actualmente la Dirección de Salud Virgen de Cocharcas cuenta con 63 equipos informáticos (PC, Laptop) distribuidas en las diferentes oficinas tal como se muestran a continuación:

OFICINAS	CANTIDAD DE EQUIPOS
DIRECCION	01
IMAGEN INSTITUCIONAL	01
ASESORIA LEGAL	02
PLANIFICACION	02
TESORERIA	02
ALMACEN	02
LOGISTICA	05
CONTABILIDAD	02
PATRIMONIO	01
ADMINISTRACION	02
ESTADISTICA	03
DEMID	06
ALMACEN ESPECIALIZADO	03
UNIDAD DE SEGUROS	04
REMUNERACIONES	02
ASISTENCIA	01
ESCALAFON	02
PAD	01
RECURSOS HUMANOS	02
SERVICIOS GENERALES	01
SALUD INDIVIDUAL	10
SALUD COLECTIVA	09
TOTAL	**64**

Además, la Dirección de Salud "Virgen de Cocharcas" cuenta con equipos informáticos como son: Ups, impresora, proyector, switch, router wifi, etc., donde en su mayoría nunca se ha realizado mantenimientos correctivos, por lo que están expuestos a futuras fallas o descomposiciones en su totalidad.

7. JUSTIFICACION

Es importante brindar el mantenimiento preventivo a los equipos informáticos para su óptimo funcionamiento, el desarrollar este tipo de actividad permite reducir el riesgo de falla de los equipos, los cuales pueden ser el resultado de daños a largo plazo, requiriendo de un mantenimiento correctivo y afectando de forma directa la vida útil de los mismos.

Realizar mantenimiento en los equipos informáticos de forma regular ayuda a extender la vida del equipo y permite su funcionamiento óptimo por periodos de tiempo más largos, evitando la inoperatividad y costos más altos para su reparación.

8. LOGROS QUE SE ESPERAR ALCANZAR

Desarrollar los mantenimientos preventivos en los tiempos programados ofrece un óptimo funcionamiento de los equipos informáticos, así como proteger toda la información procesada y almacenada de cada equipo de cómputo, de igual forma que los usuarios queden satisfechos con el trabajo realizado y garantizar el cumplimiento de este documento.

Con base a lo anterior se espera lograr las siguientes metas:

I. Lograr que se lleven dos veces al año el mantenimiento preventivo - correctivo
II. Realizar el 100% de los mantenimientos a cada equipo informático

9. ACTIVIDADES A REALIZAR

a) Revisión de inventario

Para realizar el plan de mantenimiento, es necesario contar con un inventario actualizado de los equipos informáticos, por lo cual, el Área de Control Patrimonial deberá trabajar conjuntamente con la Unidad de Estadística e informática con la finalidad de consolidar la información.

b) Mantenimiento preventivo de equipo informático

La Unidad de estadística e informática segmentara el mantenimiento de los equipos de la siguiente forma:

- **Equipos fuera de garantía**, el mantenimiento deberá ser realizado dos veces al año.
- **Para los equipos que se encuentren en garantía,** la Unidad de estadística e informática hará el seguimiento de acuerdo al tiempo y puntos que cubre la garantía y evaluara la ejecución de mantenimiento de software y hardware.
- Registro del manteamiento realizado por equipo, **(ver anexo 1)**

c) Mantenimiento correctivo de equipo informático

Este tipo de mantenimiento se desarrollará para que la vida útil del equipo se extienda, se ofrece una solución inmediata a cualquier dificultad no prevista con el equipo, por medio de tareas de limpieza, reparación y/o cambios de piezas.

En los casos que no se brinde una solución inmediata porque no existan piezas de reemplazo, se asignara un equipo en calidad de préstamo con características similares, de acuerdo a la disponibilidad de equipo

informático, esto con la finalidad de permitir la continuidad de las labores de los usuarios.

10. PERIODO DE EJECUCION

Se ha elaborado una programación para el desarrollo de dos mantenimientos preventivos al año, junio y diciembre dos veces por semana, de acuerdo al siguiente cuadro

MES	Semana 1	Semana 2	Semana 3	Semana 4
JUNIO				
DICIEMBRE				

Observación: Las fechas serán programadas una vez se tenga el visto bueno de Dirección, las fechas podrán ser modificables de acuerdo a necesidad institucional o inconvenientes anticipadas.

11. COSTOS DEL MANTENIMIENTO PREVENTIVO - CORRECTIVO

En la actualidad la Unidad de estadística e informática, optimiza el capital humano para el desarrollo de cada una de sus actividades, por lo anterior se realizará la programación del mantenimiento en base a la cantidad de personal que se cuenta (2 personas actualmente) además de la participación del Área de control patrimonial haciendo un mínimo de 3 personas.

Contar con los insumos o materiales es necesarios para el mantenimiento preventivo, es importante para el desarrollo de forma eficiente y eficaz, los materiales necesarios son: aspiradora, brochas, pasta térmica, kit de desarmadores, repuestos, etc.

Los repuestos que se utilizarán serán de acuerdo a la necesidad de los equipos informáticos, esos repuestos son: Memoria RAM, Fuente de poder, disco sólido, procesador, tarjeta de video, placas, fusor de impresora, unidad de imagen, etc. Todo ello se detalla a continuación en ítems de costo aproximados, cantidad aproximada, etc. Anual.

Gasto Institucional por día los días donde se realice mantenimiento

Tipo de recurso	Cantidad
Humano	03

Gasto total de insumos para los mantenimientos

Tipo de recurso	Cantidad	Tipo de gasto	Costo x UND	total
BIEN	02	Disco externo 1tb	s/250.00	S/500.00
BIEN	02	LOWER SOPLETE	S/200.00	S/400.00
BIEN	02	LUBRICANTE 3EN1	S/3.00	S/6.00
BIEN	10	MEMORIA RAM	S/150.00	S/1,500.00
BIEN	05	FUENTE DE PODER	S/50.00	S/250.00
BIEN	10	DISCO SOLIDO M2 Y SATA	S/150.00	S/1,500.00
BIEN	03	TARJETA DE VIDEO	S/250.00	S/750.00
BIEN	05	PLACAS	S/350.00	S/1,750.00
BIEN	01	CABLE ETHERNET	S/350.00	S/350.00
BIEN	01	FRANELA 1 METRO	S/10.00	S/10.00
BIEN	01	JUEGO DESARMADORES	S/80.00	S/80.00
BIEN	01	IMPROVISTOS	S/350.00	S/350.00
TOTAL, APROXIMADO				**S/7,446.00**

Gasto total de insumos para los mantenimientos

TOTAL, GASTO GENERAL

Tipo de recurso	total
TOTAL, APROXIMADO	**S/7,446.00**

Total, gasto aproximado para mantenimiento preventivo y correctivo.

12. SEGUIMIENTO Y MONITOREO

El seguimiento se efectuará por medio de la programación de mantenimientos **(ver anexo 2)** establecido en el que se detalla establecimiento y fecha donde se realizará el mantenimiento. Este documento servirá de guía para el control y el estado de los mantenimientos realizados, en ejecución y pendientes.

13. RIESGOS PARA EL DESARROLLO DEL MANTENIMIENTO

- Falta de presupuesto para la ejecución del plan de mantenimiento, adquisición de materiales de mantenimiento, repuestos para los equipos informáticos al momento de iniciar con el plan.
- Al finalizar el mantenimiento pueden presentarse dificultades en los equipos.

ANEXOS

Anexo 1: Registro de mantenimiento

DIRECCION DE SALUD VIRGEN DE COCHARCAS
UNIDAD DE ESTADISTICA E INFORMATICA
REGISTRO DE MANTENIMIENTO PREVENTIVO

N°	Oficina	Nombre de responsable	Codigo de inventario	Fecha	Firma	Comentario
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Dirección: Espaldas de la Municipalidad –Chincheros Ex Jardín de Niños/Teléf. 983686892
http://www.risvirgendecocharcas.gob.pe/ gmail-disachincheros035@gmail.com

Anexo 2: Calendario de mantenimiento preventivo

DIRECCION DE SALUD VIRGEN DE COCHARCAS
UNIDAD DE ESTADISTICA E INFORMATICA
CALENDARIO DE MANTENIMIENTO PREVENTIVO

N°	Oficina	Responsable	Fechas
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Dirección: Espaldas de la Municipalidad –Chincheros Ex Jardín de Niños/Teléf. 983686892
http://www.risvirgendecocharcas.gob.pe/ gmail-disachincheros035@gmail.com

UNSCH FACULTAD DE INGENIERÍA DE MINAS, GEOLOGIA Y CIVIL

ACTA DE SUSTENTACIÓN DE TESIS Nº 54-2026-FIMGC

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

En la Universidad Nacional de San Cristóbal de Huamanga, en la ciudad de Ayacucho, en cumplimiento a la **Resolución Decanal No 235-2026-FIMGC-D**, a los **veintitres días del mes de julio de 2026**, siendo las **10:24 a.m.**, reunidos en el **Auditorio de la Escuela Profesional de Ingeniería Minas**, bajo la presidencia del **MSc. José Ernesto ESTRADA CARDENAS**, y los miembros: **Dr. Efraín Elías PORRAS FLORES**, y **Mg. Karel PERALTA SOTOMAYOR**, actuando como secretario docente el **Ing. Saul Walter RETAMOZO FERNANDEZ**, para proceder a la sustentación de tesis para optar el **Título Profesional de Ingeniero de Sistemas**, del Bachiller en Ingeniería de Sistemas:

MARCO ANTONIO HUARACA HUARHUACHI

Quien presentó la tesis denominada:

Propuesta de plan de seguridad informática para mejorar el nivel de seguridad de la información, dirección de salud "Virgen de Cocharcas", provincia de Chincheros, 2024

Los señores miembros del jurado luego de expuesta la tesis y absueltas las preguntas, deliberaron y declararon:

Aprobado con 16 (dieciséis)

Siendo las **11:21 a.m.** del día **23 de julio del 2026**, culmina el acto de sustentación de tesis, y en conformidad de lo actuado los miembros del jurado firmamos al pie del presente.

MSc. José Ernesto ESTRADA CARDENAS
Presidente

Mg. Karel PERALTA SOTOMAYOR
Miembro

Dr. Efraín Elías PORRAS FLORES
Miembro - Asesor

Ing. Saul Walter RETAMOZO FERNANDEZ
Secretario docente de la FIMGC

FACULTAD DE INGENIERÍA
DE MINAS Y CIVIL
Av. Independencia S/N
Ciudad Universitaria
Central Tel. 066 312510
Anexo 151

UNSCH FACULTAD DE INGENIERÍA DE MINAS, GEOLOGIA Y CIVIL

turnitin

CONSTANCIA DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

CONSTANCIA Nº 041-2026-KPS-FIMGC/UNSCH

El que suscribe; responsable verificador de originalidad de trabajos de tesis de pregrado con el software Turnitin, en segunda instancia para las **Escuelas Profesionales** de la **Facultad de Ingeniería de Minas, Geología y Civil**; en cumplimiento a la **Resolución de Consejo Universitario Nº 039-2021-UNSCH-CU**, Reglamento de Originalidad de Trabajos de Investigación de la Universidad Nacional San Cristóbal de Huamanga y **Resolución Decanal Nº 697-2024-FIMGC-D**, deja constancia de originalidad de trabajo de investigación, que el/la Sr./Srta.

Nombres y Apellidos	:	Marco Antonio Huaraca Huarhuachi
Escuela Profesional	:	INGENIERÍA DE SISTEMAS
Título de la Tesis	:	Propuesta de plan de seguridad informática para mejorar el nivel de seguridad de la información, dirección de salud "Virgen de Cocharcas", provincia de Chincheros, 2024
Evaluación de la Originalidad	:	**6%** Índice de Similitud
Identificador de la entrega	:	3008232038

Por tanto, según los Artículos 12, 13 y 17 del Reglamento de Originalidad de Trabajos de Investigación, es **PROCEDENTE** otorgar la **Constancia de Originalidad** para los fines que crea conveniente.

En señal de conformidad y verificación se firma la presente constancia

Ayacucho, 05 de agosto de 2026

FIRMA DIGITAL

Firmado digitalmente por: PERALTA SOTOMAYOR Karel FAU 20143660754 soft
Motivo: Soy el autor del documento
Fecha: 05/08/2026 13:03:00-0500

Con depósito para Sustentación y Tramites
C.c. Archivo

FACULTAD DE INGENIERIA DE MINAS, GEOLOGIA Y CIVIL
Av. Independencia S/N Ciudad Universitaria
Central Tel. 066 312510
Anexo 151

Propuesta de plan de seguridad informática para mejorar el nivel de seguridad de la información, dirección de salud “Virgen de Cocharcas”, provincia de Chincheros, 2024

por Marco Antonio Huaraca Huarhuachi

Fecha de entrega: 04-ago-2026 06:58p. m. (UTC-0500)
Identificador de la entrega: 3008232038
Nombre del archivo: CERTIFICADO_DE_ORIGINALIDAD-_MARCO_ANTONIO_HUARACA.pdf (3.62M)
Total de palabras: 26314
Total de caracteres: 158895

Propuesta de plan de seguridad informática para mejorar el nivel de seguridad de la información, dirección de salud “Virgen de Cocharcas”, provincia de Chincheros, 2024

INFORME DE ORIGINALIDAD

6%	8%	6%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	1%
2	repositorio.udh.edu.pe Fuente de Internet	1%
3	repositorio.ucv.edu.pe Fuente de Internet	1%
4	repositorio.unamba.edu.pe Fuente de Internet	1%
5	repositorio.upn.edu.pe Fuente de Internet	<1%
6	www.perplexity.ai Fuente de Internet	<1%
7	Submitted to Universidad Nacional San Antonio Abad del Cusco Trabajo del estudiante	<1%
8	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1%
9	repositorio.unitec.edu Fuente de Internet	<1%
10	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	<1%
11	Submitted to Universidad Politécnica Estatal de Carchi Trabajo del estudiante	<1%
12	Submitted to Universitat Oberta de Catalunya Trabajo del estudiante	<1%
13	documentop.com Fuente de Internet	<1%
14	Submitted to Universidad Mariano Gálvez de Guatemala Trabajo del estudiante	<1%
	www.pcm.gob.pe	

15	Fuente de Internet	<1 %
16	Submitted to USIL-D.A. FAC. EDUCACION(C.VALDERRAMA) Trabajo del estudiante	<1 %
17	pdfcoffee.com Fuente de Internet	<1 %
18	capitalis-it.com Fuente de Internet	<1 %
19	repository.unipiloto.edu.co:8080 Fuente de Internet	<1 %
20	www.dian.gov.co Fuente de Internet	<1 %
21	dspace-uh-tmp.igniteonline.la Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		