UNIVERSIDAD DE HUANUCO

FACULTAD DE INGENIERIA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

“Diseño e implementación de un modelo de gestión en seguridad digital para el Grupo Cediamedical basándose en ISO/IEC 27001, ISO/IEC 27002”

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR: Mariano Beraun, Hugo Romario

ASESOR: Huapaya Condori, Freddy Ronald

HUÁNUCO – PERÚ

2025

TIPO DEL TRABAJO DE INVESTIGACIÓN:

- Tesis (X)
- Trabajo de Suficiencia Profesional( )
- Trabajo de Investigación ( )
- Trabajo Académico ( )

LÍNEAS DE INVESTIGACIÓN: Gestión y Desarrollo de Sistemas de Información

AÑO DE LA LÍNEA DE INVESTIGACIÓN (2020)

CAMPO DE CONOCIMIENTO OCDE:

Área: Ingeniería, Tecnología

Sub área: Ingeniería eléctrica, Ingeniería electrónica

Disciplina: Ingeniería de sistemas y comunicaciones

DATOS DEL PROGRAMA:

Nombre del Grado/Título a recibir: Título Profesional de Ingeniero de sistemas e informática

Código del Programa: P06

Tipo de Financiamiento:

- Propio (X)
- UDH ( )
- Fondos Concursables ( )

DATOS DEL AUTOR:

Documento Nacional de Identidad (DNI): 76366503

DATOS DEL ASESOR:

Documento Nacional de Identidad (DNI): 22506586

Grado/Título: Doctor en ingeniería informática y de automatización

Código ORCID: 0000-0003-4783-3803

DATOS DE LOS JURADOS:

N°	APELLIDOS Y NOMBRES	GRADO	DNI	Código ORCID
1	Jacha Rojas, Johnny Prudencio	Doctor en medio ambiente y desarrollo sostenible	40895876	0000-0001-7920-1304
2	Jara Trujillo, Alberto Carlos	Maestro en ingeniería, con mención en gestión ambiental y desarrollo sostenible	41891649	0000-0001-8392-1769
3	Reynoso Palpa, Jenny Rocio	Magíster en administración estratégica de empresas	43227744	0009-0000-5195-1904

UNIVERSIDAD DE HUANUCO

Facultad de Ingeniería

P. A. DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO(A) DE SISTEMAS E INFORMÁTICA

En la ciudad de Huánuco, siendo las 16:00 horas del dia lunes 01 del mes de diciembre de año 2025, se lleva a cabo la sustentación presencial en cumplimiento de lo señalado en el Reglamento de Grados y Títulos de la Universidad de Huánuco, quienes se reunieron los **Jurados Calificadores** integrado por los Docentes:

- Dr. Johnny Prudencio Jacha Rojas — PRESIDENTE.
- Mg. Alberto Carlos Jara Trujillo — SECRETARIO.
- Mg. Jenny Rocio Reynoso Palpa — VOCAL.

Nombrados mediante la RESOLUCIÓN N° 2643-2025-D-FI-UDH para evaluar la Tesis intitulada: **"DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN EN SEGURIDAD DIGITAL PARA EL GRUPO CEDIAMEDICAL BASÁNDOSE EN ISO/IEC 27001, ISO/IEC 27002"** Presentado por el (la) **Bach: Hugo Romario MARIANO BERAUN** para optar el Título Profesional de Ingeniero(a) de Sistemas e Informática.

Dicho acto de sustentación se desarrolló en dos etapas: exposición y absolución de preguntas: procediéndose luego a la evaluación por parte de los miembros del Jurado.

Habiendo absuelto las objeciones que le fueron formuladas por los miembros del Jurado y de conformidad con las respectivas disposiciones reglamentarias, procedieron a deliberar y calificar, declarándolo(a) Aprobado por unanimidad con el calificativo cuantitativo de ...13... y cualitativo de Suficiente según el (Art. 47).

Siendo las 17:28 horas del día 01 del mes de diciembre del año 2025, los miembros del Jurado Calificador firman la presente Acta en señal de conformidad.

Dr. Johnny Prudencio Jacha Rojas
ORCID: 0000-0001-7920-1304
DNI: 40895876
Presidente

Mg. Alberto Carlos Jara Trujillo
ORCID: 0000-0001-8392-1769
DNI: 41891649
Secretario

Mg. Jenny Rocio Reynoso Palpa
ORCID: 0009-0000-5195-1904
DNI: 43227744
Vocal

VICERRECTORADO DE INVESTIGACIÓN

UNIVERSIDAD DE HUÁNUCO

CONSTANCIA DE ORIGINALIDAD

El comité de integridad científica, realizó la revisión del trabajo de investigación del estudiante: HUGO ROMARIO MARIANO BERAUN, de la investigación titulada "DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN EN SEGURIDAD DIGITAL PARA EL GRUPO CEDIAMEDICAL BASÁNDOSE EN ISO/IEC 27001, ISO/IEC 27002", con asesor(a) FREDDY RONALD HUAPAYA CONDORI, designado(a) mediante documento: RESOLUCIÓN N° 0233-2025-D-FI-UDH del P. A. de INGENIERÍA DE SISTEMAS E INFORMÁTICA.

Puede constar que la misma tiene un índice de similitud del 11 % verificable en el reporte final del análisis de originalidad mediante el Software Turnitin.

Por lo que concluyo que cada una de las coincidencias detectadas no constituyen plagio y cumple con todas las normas de la Universidad de Huánuco.

Se expide la presente, a solicitud del interesado para los fines que estime conveniente.

Huánuco, 23 de octubre de 2025

UNIVERSIDAD DE HUÁNUCO
RESPONSABLE DE INTEGRIDAD CIENTÍFICA
HUÁNUCO - PERÚ

RICHARD J. SOLIS TOLEDO
D.N.I.: 47074047
cod. ORCID: 0000-0002-7629-6421

UNIVERSIDAD DE HUÁNUCO
RESPONSABLE DE TURNITIN
HUÁNUCO - PERÚ

MANUEL E. ALIAGA VIDURIZAGA
D.N.I.: 71345687
cod. ORCID: 0009-0004-1375-5004

162. HUGO ROMARIO MARIANO BERAUN.docx

INFORME DE ORIGINALIDAD

11%	11%	9%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	2%
2	repositorio.udh.edu.pe Fuente de Internet	1%
3	www.coursehero.com Fuente de Internet	1%
4	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
5	repositorio.ucv.edu.pe Fuente de Internet	1%

UNIVERSIDAD DE HUÁNUCO
RESPONSABLE DE INTEGRIDAD CIENTÍFICA
HUÁNUCO - PERÚ

RICHARD J. SOLIS TOLEDO
D.N.I.: 47074047
cod. ORCID: 0000-0002-7629-6421

UNIVERSIDAD DE HUÁNUCO
RESPONSABLE DE TURNITIN
HUÁNUCO - PERÚ

MANUEL E. ALIAGA VIDURIZAGA
D.N.I.: 71345687
cod. ORCID: 0009-0004-1375-5004

DEDICATORIA

A la persona que siempre aposto por mí y ahora no puede estar presente por fuerza mayor, mi padre que en paz descanse Hugo Mariano, la persona que me sigue dando motivo para luchar y seguir adelante.

Por el todo mi esfuerzo y dedicación.

AGRADECIMIENTO

Gracias infinitas a mis padres, por su amor incondicional y su apoyo moral, su fe en mí, incluso en los momentos más difíciles, ha sido el pilar de este logro. También expreso mi gratitud mis abuelos quienes supieron estar cuando más los necesitaba. Su amor y sacrificio han sido la luz que guio mi camino a través de este viaje académico.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tuvo como objetivo: determinar la mejora en la confiabilidad y seguridad de la información en el Grupo Cediamedical a partir del diseño e implementación de un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002. Tuvo un enfoque cuantitativo. El diseño adoptado fue pre-experimental con medición pretest y postest en un solo grupo; el instrumento utilizado fue un cuestionario estructurado tipo Likert (1–5) elaborado con base en el Anexo A de ISO/IEC 27001 y las buenas prácticas de ISO/IEC 27002. La población estuvo constituida por colaboradores que gestionan información crítica en Cediamedical; la muestra fue de 18 participantes. Como técnica se empleó la encuesta y, como instrumentos complementarios, reuniones de trabajo y revisión documental para verificar controles y generar evidencias (política de seguridad, SoA, plan de tratamiento de riesgos, actas de capacitación y registros de incidentes). Los principales resultados muestran incrementos estadísticamente y prácticamente relevantes en indicadores de cumplimiento alto (A menudo + Siempre) entre el pretest y el postest. Por ejemplo, en políticas documentadas el cumplimiento alto pasó de 16,7% a 77,8% (Tabla 1); en controles de acceso pasó de 16,7% a 77,8% (Tabla 7); y en capacitaciones periódicas se incrementó de 22,2% a 72,2% (Tabla 10). Estos cambios se corresponden con los desplazamientos observados en las distribuciones pre/post y con los incrementos de medias descritos en las Figuras respectivas, se llegó a las siguientes conclusiones: al inicio no existían políticas formalizadas ni manual de respuesta a incidentes, se observó bajo cierre de sesiones y gestión deficiente de contraseñas; tras la intervención, el SGSI formalizó procesos, mejoró prácticas del personal y redujo la exposición al riesgo. Se recomienda mantener el ciclo PDCA, realizar auditorías internas semestrales y capacitaciones periódicas para sostener las mejoras.

Palabras clave: seguridad de la información, SGSI, ISO/IEC 27001, ISO/IEC 27002, evaluación pretest–postest, sector salud

ABSTRACT

The present research aimed to determine the improvement in information reliability and security at the Cediamedical Group through the design and implementation of a digital security management model based on ISO/IEC 27001 and ISO/IEC 27002 standards. Its approach was quantitative. The design adopted was pre-experimental with pre-test and post-test measurements in a single group; the instrument used was a structured Likert-type questionnaire (1–5) developed based on Annex A of ISO/IEC 27001 and the good practices of ISO/IEC 27002. The population consisted of collaborators who manage critical information at Cediamedical; the sample was 18 participants. The technique used was a survey, and as complementary instruments, work meetings and document review to verify controls and generate evidence (security policy, SoA, risk treatment plan, training minutes, and incident logs). The main results show statistically and practically relevant increases in high compliance indicators (Often + Always) between the pre-test and post-test. For example, in documented policies, high compliance increased from 16.7% to 77.8% (Table 1); in access controls, it increased from 16.7% to 77.8% (Table 7); and in periodic training, it increased from 22.2% to 72.2% (Table 10). These changes correspond to the shifts observed in the pre/post distributions and with the increases in means described in the respective Figures. The following conclusions were reached: at the beginning, there were no formalized policies or incident response manual, which would be controlled by session logouts and poor password management; after the intervention, the ISMS formalized processes, improved staff practices, and reduced risk exposure. It is recommended to maintain the PDCA cycle, conduct semi-annual internal audits, and conduct periodic training to sustain improvements.

Keywords: information security, ISMS, ISO/IEC 27001, ISO/IEC 27002, pretest–posttest, healthcare sector.

INTRODUCCIÓN

La seguridad de la información es un requisito transversal para cualquier organización, y adquiere una relevancia crítica en el sector salud por el carácter sensible de los datos clínicos y administrativos. En ausencia de prácticas y controles adecuados, las instituciones están expuestas a incidentes que pueden comprometer la confidencialidad, integridad y disponibilidad de sus activos de información, con impactos operativos, legales y reputacionales. Si bien no existe la seguridad perfecta, es posible reducir el riesgo a niveles aceptables mediante políticas, procedimientos y controles técnicos coherentes con estándares reconocidos.

Con ese propósito, este proyecto se apoya en la ISO/IEC 27001 y la ISO/IEC 27002, marcos que orientan la gestión de riesgos y la implantación de controles para proteger la información, sin importar el tamaño o naturaleza de la organización. En el Grupo Cediamedical, la adopción de estas normas se tradujo en la formulación de políticas, la definición del alcance de un SGSI, la selección de controles (SoA), la capacitación del personal y la operación de procesos de respaldo y respuesta a incidentes; todo ello orientado a elevar la confiabilidad y seguridad de la información.

La investigación tuvo como objetivo general: diseñar e implementar un modelo de gestión en seguridad digital, basado en ISO/IEC 27001 e ISO/IEC 27002, para mejorar la seguridad de la información en el Grupo Cediamedical. El estudio adoptó un enfoque cuantitativo y un diseño pre-experimental de pretest–postest con un solo grupo. El instrumento principal fue un cuestionario estructurado tipo Likert (1–5) elaborado a partir del Anexo A de ISO/IEC 27001 y de las buenas prácticas de ISO/IEC 27002, aplicado a 18 colaboradores que gestionan información crítica. La medición inicial permitió establecer la línea base y priorizar brechas; la medición final evidenció la mejora tras la intervención.

Los resultados más representativos muestran incrementos en: conocimiento de políticas de seguridad (28% -> 94%), uso de contraseñas robustas (38% -> 94%) y conocimiento/aplicación del protocolo de incidentes

(22% -> 88%). Estos avances se sustentan con documentación formal (política de seguridad, alcance del SGSI, SoA, plan de implementación, actas de capacitación, registro de incidentes) y con evidencia operativa generada durante la ejecución.

En coherencia con este enfoque, el documento se organiza como sigue:

- Capítulo I. Planteamiento del problema. Describe la problemática, objetivos (general y específicos), justificación y alcances de la investigación.
- Capítulo II. Marco teórico y conceptual. Presenta antecedentes internacionales, nacionales y locales; fundamentos teóricos; definiciones; hipótesis y variables.
- Capítulo III. Metodología. Detalla el enfoque, nivel y diseño del estudio; población y muestra; técnicas e instrumentos de recolección; y procedimientos de análisis.
- Capítulo IV. Implementación y resultados. Expone, de forma narrativa y técnica, el diagnóstico inicial, el diseño del SGSI, la ejecución de controles, la capacitación, la verificación de resultados y las actividades de mejora continua, con sus medios de verificación y porcentajes de mejora.
- Capítulo V. Discusión, conclusiones y recomendaciones. Contrasta los hallazgos con la literatura y las normas; presenta las conclusiones alineadas a los objetivos; y formula recomendaciones para la sostenibilidad del SGSI.

Finalmente, se incluyen las referencias bibliográficas y los anexos, donde se ubican el instrumento de medición, las plantillas y los documentos que certifican el cumplimiento de los objetivos. Esta estructura busca que el lector—técnico o no—comprenda con claridad qué se hizo, cómo se hizo y qué evidencias demuestran la mejora de la seguridad de la información en el Grupo Cediamedical.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN DEL PROBLEMA

En el entorno actual, la International Organization for Standardization (2013) sostiene que las organizaciones que gestionan información sensible, especialmente en sectores críticos como el de la salud, enfrentan crecientes amenazas cibernéticas debido a la falta de implementación de normas de seguridad adecuadas. La acelerada transformación digital, impulsada por la adopción de tecnologías emergentes como la computación en la nube, el Internet de las Cosas (IoT) y el trabajo remoto, ha incrementado la exposición de datos a ataques informáticos, comprometiendo su confidencialidad, integridad y disponibilidad. La ausencia de medidas de seguridad no solo convierte a estas entidades en objetivos vulnerables, sino que también puede derivar en la pérdida de datos críticos, afectando su operatividad y reputación institucional.

A nivel mundial, los ciberataques se han posicionado entre los principales riesgos para la estabilidad de organizaciones públicas y privadas. Prey Project (2023) informa que en 2021 los ciberataques fueron clasificados como el quinto riesgo más alto a nivel global y se proyecta que los ataques dirigidos al IoT se dupliquen para 2025. En el sector salud, Check Point Software Technologies (2023) reporta que, durante el primer trimestre del año, el sector experimentó un promedio de 1,684 ataques semanales, lo que representa un incremento del 22% con respecto al año anterior. Este panorama evidencia la vulnerabilidad de las instituciones sanitarias ante la creciente sofisticación de los ataques informáticos.

A nivel internacional, el impacto de los ciberataques se ha manifestado con mayor intensidad en América Latina. De acuerdo con el Foro Económico Mundial (2023), durante la pandemia, los ataques dirigidos al sector salud en la región se incrementaron considerablemente, generando interrupciones en cirugías, desabastecimiento de medicamentos y filtraciones de historiales

clínicos. De manera similar, Americasistemas (2023) indica que el sector financiero y sanitario han sido los más afectados, con un crecimiento sostenido en la cantidad de incidentes de seguridad reportados. Estos datos demuestran que, a pesar de los avances en normativas y estrategias nacionales de ciberseguridad, la región sigue siendo altamente vulnerable.

En el caso de Perú, la tendencia no es diferente. ICEX (2023) informa que, en 2022, el país experimentó más de 15,000 millones de intentos de ciberataques, lo que representó un aumento del 35% en comparación con el año anterior. Dentro de estos ataques, los métodos más empleados fueron el phishing y el ransomware. Asimismo, Infobae (2024) advierte que, en lo que va del año, se han detectado más de un millón de casos de phishing, lo que representa la cifra más alta registrada en los últimos años. Particularmente en el sector salud, Stakeholders (2023) señala que ciberdelincuentes pueden acceder a datos críticos de instituciones médicas en un tiempo estimado de 14 horas, comprometiendo la integridad de la información y exponiendo a las organizaciones a ataques de ransomware.

En un nivel local, el grupo Cediamedical, dedicado a la gestión de información crítica como historiales clínicos, registros de atención médica y datos financieros, enfrenta graves riesgos de ciberseguridad debido a la falta de políticas y controles adecuados. La ausencia de medidas de protección pone en peligro la integridad, disponibilidad y confidencialidad de los datos, lo que podría derivar en pérdidas económicas, daños reputacionales e incluso implicaciones legales. Se ha identificado que el personal de Cediamedical carece de procedimientos claros para el manejo seguro de la información y la administración de accesos a los sistemas, lo que incrementa la exposición a ciberataques. Prácticas inseguras como el uso de contraseñas débiles y la falta de capacitación en ciberseguridad agravan aún más la vulnerabilidad de la organización ante amenazas externas. En 2024, Cediamedical enfrentó cinco incidentes de ciberseguridad, incluyendo accesos no autorizados a sistemas internos y fallas en la protección de credenciales. Uno de estos eventos generó una interrupción operativa prolongada, afectando servicios administrativos y la gestión de citas

médicas. Estos incidentes tuvieron repercusiones económicas significativas, derivadas de costos asociados a la mitigación, tiempo de inactividad y recuperación de sistemas. Si bien los montos exactos no pueden divulgarse por confidencialidad, la magnitud de las pérdidas refuerza la necesidad de implementar estrategias robustas de seguridad digital. Este caso destaca la importancia de políticas proactivas para reducir vulnerabilidades y asegurar la continuidad del negocio, un área crítica para investigaciones en gestión de riesgos tecnológicos.

Para abordar esta problemática, la presente investigación propone el diseño de un modelo de gestión en seguridad digital basado en los estándares ISO/IEC 27001 e ISO/IEC 27002. Es importante resaltar que estos estándares no solo se aplican en el diseño de software, sino que también proporcionan directrices para mejorar la seguridad en los sistemas ya implementados dentro de la organización. A través de la adopción de estas normativas, se busca identificar vulnerabilidades en los procesos actuales y establecer mecanismos de control que permitan mitigar riesgos sin necesidad de desarrollar nuevas plataformas tecnológicas.

La presente investigación tiene como objetivo optimizar la gestión de seguridad digital en Cediamedical, asegurando que los procesos administrativos y tecnológicos cumplan con los más altos estándares internacionales de protección de la información. La aplicación de las normas ISO/IEC 27001 e ISO/IEC 27002 permitirá fortalecer los procedimientos de seguridad existentes, estableciendo lineamientos para la correcta administración de accesos, la protección de credenciales y la mitigación de amenazas cibernéticas. Con ello, Cediamedical no solo protegerá su información sensible, sino que también fortalecerá la confianza de sus pacientes y cumplirá con las regulaciones en materia de protección de datos. Sin un sistema robusto de gestión de seguridad de la información, las organizaciones que manejan datos sensibles quedan expuestas a amenazas digitales, lo que resalta la urgencia de aplicar estándares internacionales para reducir riesgos operativos y fortalecer su resiliencia digital.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. PROBLEMA GENERAL

¿De qué manera el diseño e implementación de un modelo de gestión en seguridad digital, basado en las normas ISO/IEC 27001 e ISO/IEC 27002, fortalecerá la protección de la información en el grupo Cediamedical, garantizando su integridad, disponibilidad y confidencialidad, y reduciendo los riesgos asociados a amenazas cibernéticas?

1.2.2. PROBLEMAS ESPECÍFICOS

- ¿De qué manera el diagnóstico del estado actual de la seguridad digital en el grupo Cediamedical permitirá identificar vulnerabilidades, amenazas y brechas en la gestión de la información, facilitando la formulación de estrategias de mitigación?
- ¿De qué manera el diseño de un modelo de gestión en seguridad digital, basado en las normas ISO/IEC 27001 e ISO/IEC 27002, contribuirá a establecer políticas, controles y procedimientos efectivos para la protección de la información crítica de la empresa?
- ¿De qué manera la implementación del modelo de gestión en seguridad digital asegurará la adopción de buenas prácticas en ciberseguridad, mejorando la resiliencia de la empresa ante amenazas cibernéticas y garantizando el cumplimiento de estándares internacionales?

1.3. OBJETIVO GENERAL

Diseñar e implementar un modelo de gestión en seguridad digital para el grupo Cediamedical basado en las normas ISO/IEC 27001 e ISO/IEC 27002, con el propósito de fortalecer la protección de la información, garantizar su integridad, disponibilidad y confidencialidad, y reducir los riesgos asociados a posibles amenazas cibernéticas.

1.4. OBJETIVOS ESPECÍFICOS

- Diagnosticar el estado actual de la seguridad digital en el grupo Cediamedical, identificando vulnerabilidades, amenazas y brechas en la gestión de la información.
- Diseñar un modelo de gestión en seguridad digital, estableciendo políticas, controles y procedimientos que permitan mitigar riesgos y proteger la información crítica de la empresa.
- Implementar el modelo de gestión en seguridad digital en el grupo Cediamedical, asegurando la adopción de buenas prácticas en ciberseguridad y el cumplimiento de estándares internacionales.

1.5. JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.5.1. JUSTIFICACIÓN TEÓRICA

El presente trabajo de investigación se desarrolló con la intención de aportar al conocimiento sobre la gestión de la seguridad digital en organizaciones del sector salud, tomando como base las normas internacionales ISO/IEC 27001 e ISO/IEC 27002. En este sentido, la aplicación de dichos estándares permitió construir un marco teórico firme para orientar mejores estrategias de protección de la información. Al mismo tiempo, los resultados obtenidos sirvieron como base para futuras propuestas académicas y profesionales, resaltando la importancia de contar con modelos de gestión que aseguren la confidencialidad, integridad y disponibilidad de los datos.

1.5.2. JUSTIFICACIÓN PRÁCTICA

Este estudio tuvo una gran relevancia práctica porque ayudó a mejorar la seguridad de la información en el grupo Cediamedical, reduciendo riesgos ligados a ciberataques y accesos indebidos. Al mismo tiempo, la aplicación del modelo de gestión en seguridad digital brindó herramientas y lineamientos que fortalecieron la protección de datos sensibles y fomentaron un entorno más confiable para toda la organización. De esta forma, los resultados obtenidos también pudieron

repetirse en otras empresas del sector salud que enfrentaban problemas parecidos al manejar su información, logrando mejoras reales.

1.5.3. JUSTIFICACIÓN METODOLÓGICA

Desde un enfoque metodológico, esta investigación propuso un modelo claro para mejorar la seguridad de la información, tomando como base las normas ISO/IEC 27001 e ISO/IEC 27002. Lo más valioso del planteamiento fue su aplicación directa al sector salud de la región, donde todavía era raro encontrar instituciones que trabajaran con sistemas formales de seguridad digital basados en estándares internacionales. Al mismo tiempo, la propuesta se convirtió en una herramienta práctica, adaptable y fácil de repetir, que podía servir a otras organizaciones médicas interesadas en fortalecer su ciberseguridad sin empezar de cero. De esta forma, el estudio no solo buscó dar respuesta a un problema concreto del entorno local, sino que también dejó un precedente técnico y académico que podría motivar futuras mejoras en realidades sanitarias parecidas, incluso a corto plazo.

1.6. LIMITACIONES DE LA INVESTIGACIÓN

La principal limitación de este estudio es el tamaño muestral reducido (n = 18), determinado por el carácter censal de la población objetivo (todos los colaboradores de Cediamedical involucrados en la gestión y seguridad de la información). Si bien el censo permite evaluar con precisión el efecto de la intervención en este grupo específico, restringe la validez externa y, por tanto, la generalización de los resultados a otras organizaciones o contextos con distinta estructura, cultura de seguridad o madurez tecnológica.

1.7. VIABILIDAD DE LA INVESTIGACIÓN

1.7.1. VIABILIDAD TÉCNICA

El estudio fue viable debido a la disponibilidad de información actualizada sobre la seguridad digital y la existencia de recursos que permitieron aplicar las normas ISO/IEC 27001 e ISO/IEC 27002 de manera efectiva. Para ello, se contó con herramientas tecnológicas especializadas como RiskLens, utilizada para el análisis cuantitativo de riesgos, y Open-AudIT, que permitió realizar el inventario y monitoreo de activos tecnológicos. Asimismo, se empleó Microsoft Excel para la elaboración de matrices de riesgos y SPSS para el análisis estadístico de los resultados obtenidos en las fases de pretest y postest. La documentación del proceso fue respaldada mediante Microsoft Word.

1.7.2. VIABILIDAD SOCIOECONÓMICA

El estudio fue viable desde el punto de vista económico, ya que se contó con los recursos financieros necesarios para la ejecución del proyecto. Se gestionaron los costos asociados a la implementación del modelo de gestión sin que ello representara un obstáculo para la investigación.

1.7.3. VIABILIDAD INSTITUCIONAL

El estudio fue viable institucionalmente, ya que se contó con el respaldo del grupo Cediamedical, incluyendo la colaboración del personal y directivos. Su disposición para participar en el proceso de recopilación de datos y evaluación permitió el desarrollo exitoso de la investigación.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. ANTECEDENTES A NIVEL INTERNACIONAL

Gómez (2021), en la tesis titulada Implementación de un Sistema de Gestión de Seguridad de la Información en una entidad financiera según la norma ISO/IEC 27001:2013, Universidad de Buenos Aires, Argentina, desarrolló una investigación sobre la implementación de un Sistema de Gestión de Seguridad de la Información (MGSI) en el sector financiero, con base en la norma ISO/IEC 27001:2013. Para la realización del estudio se empleó una metodología cualitativa basada en estudios de caso, reuniendo información de diferentes áreas de la entidad financiera analizada. En este sentido, la investigación permitió identificar los riesgos más notorios en seguridad y reconocer, al mismo tiempo, las estrategias de mitigación que funcionaban mejor dentro del marco normativo. Como resultado se optimizó el manejo de la seguridad de la información, fortaleciendo la protección de los datos más críticos e impulsando la confidencialidad, la integridad y la disponibilidad, lo que finalmente aseguró un control más confiable.

La investigación mostró que era posible aplicar un MGSI basado en ISO 27001 dentro del sector financiero, con mejoras visibles en la protección de datos sensibles y en el control de los riesgos. No obstante, el estudio se enfocó en grandes empresas con recursos amplios y dejó sin revisar su uso en entidades medianas del sector salud, donde los presupuestos son limitados y requieren adaptaciones.

Smith (2020), en su artículo titulado Evaluación de riesgos en seguridad de la información en hospitales utilizando ISO/IEC 27001, publicado en el Journal of Information Security, presentó una evaluación de riesgos en el sector salud aplicando la norma ISO/IEC 27001 y mostró, a partir de un enfoque cuantitativo con encuestas y

análisis de información en hospitales públicos y privados, que muchas instituciones no contaban con un MGSI adecuado, lo que las dejaba más expuestas a ciberataques y filtraciones. De esta forma, los resultados evidenciaron una realidad frecuente en la región: la falta de controles sólidos y personal capacitado. Finalmente, se concluyó que la adopción de la norma ISO/IEC 27001 podría elevar de manera notable la seguridad de los datos médicos, reduciendo incidentes y evitando la fuga de información sensible, tan común actualmente.

La investigación mostró serias fallas en hospitales sin un MGSI, evidenciando el alto riesgo que enfrentan estas instituciones. Sin embargo, no profundizó en soluciones para centros de mediana escala ni en programas constantes de capacitación, de modo que esta tesis busca cubrir esas carencias con un enfoque más integral y ajustado a la realidad local.

Chen (2020), en el artículo Adopción de la norma ISO/IEC 27001 en pequeñas y medianas empresas: Un estudio de caso en China, publicado en el International Journal of Information Management, analizó cómo se aplicaba la norma ISO/IEC 27001 en pequeñas y medianas empresas tecnológicas en China y, mediante entrevistas y revisión de documentos, detectó que muchas no tenían controles claros de seguridad, lo que generaba riesgos operativos y las dejaba expuestas a ataques cibernéticos. Al mismo tiempo, la adopción de un MGSI basado en ISO/IEC 27001 ayudó a ordenar los procesos, mejorar la protección de la información y disminuir los gastos provocados por incidentes de seguridad.

La investigación confirmó que las PYMEs tecnológicas fortalecen su seguridad con ISO 27001, aunque dejó de lado al sector salud. Por ello, surge la necesidad de estudiar cómo ajustar estos estándares a instituciones médicas pequeñas, donde el dinero escasea pero los riesgos continúan siendo igual de serios.

2.1.2. ANTECEDENTES A NIVEL NACIONAL

Rojas (2022), en la tesis titulada Diseño de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001 para una universidad pública en Lima, Universidad Nacional Mayor de San Marcos, Perú, llevó a cabo un estudio sobre la puesta en marcha de un MGSI dentro del entorno universitario y, a través de entrevistas y revisión de documentos, pudo reconocer los principales riesgos que afectaban la información en la institución. En este sentido, el análisis mostró fallas que abrían la puerta a pérdidas de datos y accesos indebidos. De esta forma, el estudio sostuvo que aplicar un MGSI alineado con ISO/IEC 27001 ayudaría a reducir esos riesgos y, al mismo tiempo, fortalecer la confidencialidad y la disponibilidad de la información institucional.

La investigación confirmó que ISO 27001 era útil en el entorno universitario peruano, aunque su propuesta no tomó en cuenta las particularidades del manejo de datos médicos ni las limitaciones económicas comunes en regiones, punto que este trabajo busca cubrir y desarrollar.

Fernández (2021), en su investigación titulada Implementación de controles de seguridad de la información según ISO/IEC 27002 en una entidad gubernamental peruana, publicada en la Revista Peruana de Informática y Sistemas, analizó cómo se aplicaban los controles de seguridad dentro de una institución pública en Perú y, usando una metodología de auditoría, se identificaron varias brechas que afectaban la protección de los sistemas. En este sentido, el estudio planteó acciones correctivas basadas en la norma ISO/IEC 27002 y los resultados mostraron mejoras claras, ya que la implementación de dichos controles fortaleció la seguridad, reduciendo la exposición frente a amenazas y distintos ataques informáticos que afectaban a la entidad.

La investigación logró aplicar controles de ISO 27002 en entidades del Estado y mostró buenos resultados, aunque su mirada centrada en organizaciones grandes no consideró la realidad de clínicas medianas, de modo que aún se requiere un modelo accesible para el sector salud local.

García (2020), en la tesis Evaluación de la madurez en seguridad de la información en empresas del sector financiero peruano aplicando ISO/IEC 27001, Pontificia Universidad Católica del Perú, realizó un estudio para conocer el nivel de madurez en seguridad de la información dentro de empresas del sector financiero en Perú. Con un modelo de evaluación basado en ISO/IEC 27001 se revisaron varios aspectos, entre ellos la gobernanza de la seguridad, el cumplimiento de las normas y la manera en que se manejaban los riesgos. En este sentido, aunque muchas compañías tenían medidas básicas, se repitió la idea de que un MGSI ayudaría a resistir ciberataques y a proteger mejor los activos de información.

La investigación analizó el sector financiero peruano y confirmó que, aunque existían medidas básicas, todavía se necesitaban MGSI más sólidos. Sin embargo, al no incluir instituciones médicas, donde los datos son más delicados y los recursos escasos, dejó sin atender una área clave que esta tesis retoma y desarrolla.

2.1.3. ANTECEDENTES A NIVEL LOCAL

Martínez (2023), en la tesis titulada Propuesta de un Sistema de Gestión de Seguridad de la Información para una clínica privada en Huánuco basado en ISO/IEC 27001, Universidad de Huánuco, desarrolló un estudio que resaltó la urgencia de aplicar un MGSI en instituciones de salud de la región y, mediante un análisis de riesgos, se detectaron vulnerabilidades serias en la protección de datos clínicos. Al mismo tiempo, la investigación mostró que adoptar un MGSI basado en ISO/IEC 27001 mejoraría la confidencialidad, la disponibilidad y la

integridad de la información médica, fortaleciendo la seguridad digital dentro de la clínica.

La investigación encontró vulnerabilidades serias en clínicas de Huánuco, aunque no desarrolló un plan claro de capacitación para el personal, un aspecto clave según los propios hallazgos para asegurar la continuidad y sostenibilidad del MGSI en el tiempo.

López (2022), en su artículo Análisis de riesgos de seguridad de la información en una institución educativa de Huánuco según la norma ISO/IEC 27005, publicado en la Revista Científica de la Universidad Nacional Hermilio Valdizán, evaluó los riesgos más comunes que afectan la seguridad de la información en varias instituciones educativas de la región y, al mismo tiempo, mediante un enfoque centrado en la evaluación de riesgos, se detectaron fallas en el acceso a los sistemas, en el manejo de credenciales y en la poca cultura de seguridad digital. El estudio señaló que aplicar controles basados en ISO/IEC 27005 ayudaría a disminuir estas amenazas y reforzar la protección de los datos académicos y administrativos.

La investigación encontró problemas en el manejo de credenciales dentro de instituciones educativas locales y, al mismo tiempo, mostró que esta situación también ocurre en el sector salud. Aunque resaltó la necesidad de aplicar controles estrictos de acceso, no ofreció herramientas concretas para el personal médico, punto clave en esta investigación.

Vargas (2021), en la tesis titulada Implementación de políticas de seguridad de la información en una empresa de telecomunicaciones en Huánuco siguiendo las directrices de ISO/IEC 27002, Universidad Nacional Hermilio Valdizán, realizó una investigación donde se analizó la necesidad de reforzar la seguridad de la información en empresas tecnológicas de Huánuco. A través de un análisis de brechas se detectaron fallas en el control de accesos, el cuidado de los datos y la atención frente a incidentes. En este sentido, la puesta en marcha de

políticas alineadas con ISO IEC 27002 permitió mejorar la protección de los sistemas, fortaleciendo la seguridad y reduciendo el impacto de amenazas digitales cada vez más frecuentes.

La investigación demostró que políticas basadas en ISO 27002 mejoran la seguridad en empresas tecnológicas locales. Sin embargo, al no abordar el sector salud - donde la protección de datos es más crítica - dejó sin resolver un vacío importante que esta tesis pretende cubrir con un modelo adaptado a instituciones médicas.

2.2. MARCO TEÓRICO

2.2.1. NORMAS ISO/IEC 27001 E ISO/IEC 27002

Las normas ISOIEC 27001 e ISOIEC 27002 son estándares internacionales creados para ayudar a que las organizaciones protejan mejor su información, y al mismo tiempo reduzcan riesgos que suelen afectar a cualquier institución. En este sentido, estas normas ofrecen una guía útil para ordenar la seguridad y garantizar la confidencialidad, integridad y disponibilidad de los datos, de forma que las entidades puedan cuidar su información crítica y reaccionar ante incidentes que pongan en peligro sus actividades (ISO/IEC, 2022).

En un contexto donde las amenazas cibernéticas crecen y aparecen con más frecuencia, la adopción de estándares internacionales de seguridad se vuelve una necesidad real. Según el informe de IBM Security 2022, el 83% de las organizaciones pasó por más de una brecha en los últimos años, lo que demuestra la importancia de contar con sistemas sólidos basados en normativas reconocidas globalmente.

2.2.1.1. ISO/IEC 27001: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (MGSI)

La ISOIEC 27001 es la norma internacional más usada para aplicar un Sistema de Gestión de Seguridad de la Información, y su finalidad es orientar a las organizaciones para establecer,

mantener y mejorar este sistema de forma constante, de manera que puedan manejar sus riesgos de seguridad con un método ordenado, práctico y realmente eficaz en el tiempo (ISO/IEC, 2022).

Esta norma se basa en un enfoque centrado en los riesgos, por lo que las organizaciones deben reconocer y revisar sus propios problemas de seguridad de la información para luego aplicar controles que realmente reduzcan el impacto, incluso en situaciones cotidianas que suelen pasarse por alto. Según Peltier (2016), la ISOIEC 27001 ayuda a construir un marco claro para manejar la seguridad, alineando los procesos con metas estratégicas y respetando regulaciones internacionales vigentes.

- **Principales Beneficios de Implementar la ISO/IEC 27001**

La aplicación de esta norma ofrece beneficios importantes para cualquier organización y, de todas maneras, se vuelve clave para reforzar la seguridad y la confianza en el manejo de los datos. Por otra parte, entre los aspectos más valorados se encuentran los siguientes:

1. Protección de la Información Sensible: La norma plantea medidas claras para proteger datos financieros e información de clientes, cuidando registros confidenciales frente a accesos indebidos y riesgos digitales actuales (ISO/IEC, 2022).

2. Cumplimiento Normativo: Facilita el respeto de disposiciones reconocidas a nivel internacional, como el Reglamento General de Protección de Datos GDPR y la Ley de Portabilidad y Responsabilidad del Seguro de Salud HIPAA (European Commission, 2021).

3. Reducción de Riesgos y Costos: Un MGSI bien aplicado disminuye las vulnerabilidades y evita gastos derivados de incidentes de seguridad (Peltier, 2016).

4. Mayor Confianza y Reputación: as entidades certificadas bajo ISOIEC 27001 generan credibilidad ante clientes, socios y demás interesados al evidenciar un compromiso real con la seguridad (Whitman & Mattord, 2019).

- **Estructura de la Norma ISO/IEC 27001**

a norma ISO/IEC 27001 se organiza en cláusulas y anexos que marcan la base para gestionar la seguridad de la información dentro de una institución, y de esta forma se entiende mejor su aplicación en la práctica:

- Cláusulas 4-10: Explican el marco del MGSI y abarcan el contexto, el liderazgo, la planificación, el soporte, la operación, la evaluación y la mejora continua (ISO/IEC, 2022).
- Anexo A: resenta 114 controles agrupados en 14 dominios, donde se incluye la gestión de riesgos, el control de accesos, la seguridad de operaciones y la protección de datos en la nube (ISO/IEC, 2022).

2.2.1.2. ISO/IEC 27002: CONTROLES Y MEJORES PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN

La norma ISO/IEC 27002 complementa la ISO/IEC 27001 al ofrecer controles más detallados y buenas prácticas que ayudan a reforzar la seguridad dentro de una organización, y de esta forma se vuelve más clara su aplicación. Por otra parte, mientras la ISO/IEC 27001 señala lo que se debe hacer, la ISO/IEC 27002 explica cómo aplicar esos controles de manera efectiva (ISO/IEC, 2022).

- **Principales Directrices de la ISO/IEC 27002**

Los controles definidos en la ISOIEC 27002 abarcan varios aspectos importantes de la seguridad de la información:

1. Gestión de Riesgos de Seguridad: Aplicación de procesos para reconocer, evaluar y reducir riesgos de seguridad dentro de la organización (ISO/IEC, 2022).

2. Control de Accesos y Protección de Datos: Uso de métodos de autenticación, control de permisos de usuarios y protección mediante cifrado de datos importantes (Peltier, 2016).

3. Monitorización y Auditorías de Seguridad: Supervisión constante de los sistemas de información mediante herramientas para analizar el tráfico, detectar intrusos y realizar diversas pruebas especializadas (Whitman & Mattord, 2019).

4. Capacitación del Personal en Buenas Prácticas de Seguridad: Desarrollo de programas de capacitación en ciberseguridad para los trabajadores, asegurando que comprendan las amenazas y aprendan a prevenir distintos incidentes (Peltier, 2016).

- **Comparación entre ISO/IEC 27001 e ISO/IEC 27002**

Tabla 1

Comparativa

Característica	**ISO/IEC 27001**	**ISO/IEC 27002**
Propósito	Definir requisitos para un MGSI	Proporcionar controles y mejores prácticas
Enfoque	Basado en la gestión de riesgos	Basado en la implementación de controles
Obligatoriedad	Norma certificable	No certificable, de apoyo a ISO/IEC 27001
Aplicación	Cualquier organización	Organizaciones que buscan mejorar la seguridad

- **Importancia de la Adopción de las Normas ISO/IEC 27001 e ISO/IEC 27002**

La implementación de estas normas es fundamental para cualquier organización que maneje información crítica, especialmente en sectores como el financiero, tecnológico y salud. Según el Informe de Seguridad Cibernética de Verizon (2022), el 82% de los incidentes de seguridad están relacionados con la falta de controles adecuados, lo que resalta la importancia de adoptar estándares robustos como ISO/IEC 27001 e ISO/IEC 27002 para reducir riesgos.

En el sector salud, donde proteger los registros médicos electrónicos es tan importante, estas normas sirven como guía clara para aplicar controles que cuiden la privacidad de los datos y, al mismo tiempo, permitan mantener la continuidad del servicio, incluso en situaciones inesperadas que puedan afectar la atención diaria (European Commission, 2021).

2.2.2. MODELOS DE GESTIÓN EN SEGURIDAD DIGITAL

La gestión de la seguridad digital es hoy una tarea clave en cualquier organización, porque busca definir acciones y cuidados para proteger la información y los activos que se usan a diario frente a distintas amenazas. Al mismo tiempo, los modelos de gestión permiten ordenar el trabajo, reconocer riesgos reales e implementar controles, revisando después si esas medidas funcionan o necesitan mejoras constantes (Calder & Watkins, 2019).

En un contexto donde los ataques informáticos crecen y se vuelven más elaborados, las organizaciones necesitan trabajar con modelos de seguridad que fortalezcan su respuesta frente a cualquier amenaza. Al mismo tiempo, el Informe de Ciberseguridad de Verizon (2022) indica que el 82% de las violaciones de datos se origina por errores humanos o por engaños que aprovechan vulnerabilidades, lo

que refleja la urgencia de contar con una gestión sólida y flexible que pueda adaptarse con rapidez.

- **Principios Fundamentales de un Modelo de Gestión en Seguridad Digital**

Un modelo de gestión en seguridad digital debe estar fundado en tres pilares fundamentales, según Calder y Watkins (2019):

1. Identificación de amenazas y vulnerabilidades: Consiste en realizar un análisis de riesgos para reconocer las posibles amenazas que pongan en peligro la seguridad de la información dentro de la organización y, al mismo tiempo, evaluar los activos digitales y los sistemas actuales, detectando fallas que podrían ser usadas por atacantes (Whitman & Mattord, 2019).

2. Implementación de controles y medidas de mitigación: Una vez identificadas las vulnerabilidades, es clave definir políticas de seguridad y controles que permitan reducir riesgos y, al mismo tiempo, ordenar el acceso a la información de forma más clara. Esto puede incluir el uso de normas como ISO/IEC 27001, la autenticación multifactor e incluso la asignación de permisos a roles específicos dentro de la organización (Calder & Watkins, 2019).

3. Monitoreo y auditoría constante: La seguridad digital no es un proceso fijo, sino uno que debe revisarse y mejorarse de forma constante; por eso, las organizaciones necesitan aplicar sistemas de detección y respuesta a incidentes, así como auditorías y pruebas especializadas, con el fin de asegurar la verdadera eficacia de las medidas adoptadas (Verizon, 2022).

- **Principales Modelos de Gestión en Seguridad Digital**

Con el paso del tiempo se han creado distintas metodologías para gestionar la seguridad digital en las organizaciones, y a continuación se muestran algunos de los modelos más usados hoy:

2.2.2.1. MODELO NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY)

El Marco de Ciberseguridad del NIST es considerado uno de los modelos más conocidos en todo el mundo para gestionar la seguridad digital y, al mismo tiempo, organizar la defensa frente a ataques. Este modelo fue creado por el National Institute of Standards and Technology NIST y ofrece un enfoque claro que ayuda a identificar, proteger, detectar, responder y recuperar los sistemas cuando ocurre un incidente, lo cual resulta clave para reducir daños, mantener la continuidad operativa y evitar mayores consecuencias (NIST, 2021).

- **Fases del Modelo NIST:**

- Identificar: Evaluar riesgos y activos críticos.
- Proteger: Implementar medidas de seguridad como cifrado y autenticación.
- Detectar: Monitorear redes y sistemas en busca de amenazas.
- Responder: Actuar ante incidentes mediante planes de contingencia.
- Recuperar: Restaurar sistemas y mejorar la estrategia de seguridad.

El modelo NIST es usado ampliamente por entidades públicas y también por empresas privadas, pues resulta flexible, práctico y sencillo de aplicar en distintos sectores (NIST, 2021).

2.2.2.2. MODELO DE SEGURIDAD BASADO EN RIESGOS (RISK-BASED SECURITY MODEL)

Este enfoque busca manejar el riesgo de manera activa, identificando y dando prioridad a las amenazas según el daño posible dentro de la organización (Whitman & Mattord, 2019).

- **Principios Claves del Modelo:**

1. Evaluación continua de riesgos: Identificación y clasificación de amenazas cibernéticas.
2. Priorización de activos críticos: Protección enfocada en los datos más sensibles.
3. Gestión adaptativa: Implementación de medidas de seguridad basadas en el nivel de riesgo detectado.

Las organizaciones que usan este modelo pueden organizar mejor sus recursos y enfocarse, en este sentido, en las zonas con mayor riesgo real (Calder & Watkins, 2019).

2.2.2.3. MODELO ZERO TRUST SECURITY (CERO CONFIANZA)

El enfoque Zero Trust es un modelo de seguridad que parte de la idea de que ningún usuario ni dispositivo es confiable por defecto, y por eso, en vez de permitir accesos solo por ubicación o credenciales, exige una verificación constante para asegurar la protección de los datos (Garrett, 2021).

- **Principios del Modelo Zero Trust:**

- Verificación continua: Evaluación en tiempo real de cada usuario y dispositivo.
- Acceso mínimo necesario: Los usuarios solo pueden acceder a la información estrictamente necesaria para su trabajo.

- Microsegmentación: Separación de redes para evitar movimientos laterales en caso de un ataque.

El modelo Zero Trust Security está siendo adoptado cada vez más por entidades públicas y grandes empresas, pues ayuda a disminuir el riesgo de accesos indebidos y ataques internos (Garrett, 2021).

- **Importancia de la Adaptabilidad en los Modelos de Gestión en Seguridad Digital**

No todas las organizaciones tienen las mismas necesidades de seguridad, por lo que los modelos de gestión deben ajustarse a distintos contextos. Según Calder y Watkins (2019), un modelo de seguridad realmente efectivo debe ser flexible y adaptable:

1. Ser escalable y ajustarse al crecimiento de la organización.
2. Cumplir con regulaciones internacionales, como ISO/IEC 27001, GDPR y HIPAA.
3. Fomentar una cultura de seguridad, capacitando a los empleados sobre buenas prácticas en ciberseguridad.

El Informe de Ciberseguridad de Microsoft (2022) señala que el 95% de los incidentes de seguridad se asocia a fallas humanas, lo que muestra la gran importancia de capacitar y concientizar en seguridad digital a todas las personas dentro de las organizaciones.

2.2.3. SEGURIDAD DE LA INFORMACIÓN

En la actualidad, la seguridad digital se ha vuelto un pilar esencial para cualquier organización, pues las amenazas siguen creciendo sin parar. Al mismo tiempo, la digitalización de procesos, el uso de equipos conectados y la migración a la nube ampliaron la superficie de ataque,

creando riesgos serios para la integridad y la disponibilidad de la información (Smith, 2021).

Según Tipton y Krause (2019), la seguridad digital consiste en aplicar técnicas y controles para proteger sistemas, redes y datos frente a accesos o daños malintencionados. Esta disciplina considera medidas como la autenticación multifactorial, el cifrado de información, el monitoreo constante de redes y la gestión oportuna de incidentes de seguridad dentro de la organización.

La importancia de la seguridad digital no solo está ligada al cuidado de los activos informáticos, sino también al cumplimiento de las normas vigentes. Al mismo tiempo, regulaciones como el Reglamento General de Protección de Datos GDPR en Europa y la Ley de Privacidad del Consumidor de California CCPA en Estados Unidos exigen que las organizaciones apliquen estrategias claras para proteger la información personal, de esta forma se garantiza su uso responsable y se evitan sanciones que pueden afectar seriamente a cualquier institución (Johnson & Lee, 2020).

Un informe de IBM Security (2022) muestra que el costo promedio de una brecha de seguridad en 2021 llegó a 4.24 millones de dólares, lo que evidencia la necesidad de aplicar medidas proactivas para reducir riesgos y evitar pérdidas económicas, además de proteger la reputación institucional.

2.2.4. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se basa en un conjunto de principios que ayudan a proteger los datos frente a accesos no autorizados, modificaciones indebidas e interrupciones que afecten su disponibilidad, y al mismo tiempo plantea acciones claras para evitar daños. Según Stallings y Brown (2018), la seguridad de la información se apoya en tres pilares esenciales, confidencialidad, integridad y disponibilidad, conocidos como la tríada CID Confidentiality, Integrity, Availability – CIA. Estos principios son aceptados de manera amplia

dentro de la gestión de la seguridad informática y sirven como punto de partida para cualquier modelo de protección, especialmente en sectores sensibles. En este sentido, el sector salud requiere un cuidado permanente porque la información de los pacientes es muy delicada; de esta forma, los controles y las buenas prácticas se vuelven necesarios para reducir riesgos y garantizar un manejo responsable (Whitman & Mattord, 2019).

- **Confidencialidad**

La confidencialidad trata de proteger la información y evitar que sea vista o difundida sin permiso, asegurando al mismo tiempo que solo las personas, entidades o sistemas con autorización puedan acceder a los datos sensibles, tal como lo indica Peltier, 2016. Para lograr este propósito se usan varias herramientas, entre ellas el cifrado de datos, la autenticación multifactor y listas de control de acceso, además de políticas internas que ayudan a ordenar la información y disminuir riesgos dentro de una organización, especialmente cuando se maneja contenido delicado.

En entornos donde se maneja información muy sensible, como en la salud o en el sector financiero, la confidencialidad es clave para evitar fugas de datos personales, historiales clínicos o información económica, tal como señala Andress (2019). Por otra parte, en hospitales y clínicas de Estados Unidos, la Ley de Portabilidad y Responsabilidad del Seguro Médico exige protocolos estrictos que protegen los datos de los pacientes y aseguran que solo el personal autorizado pueda revisar sus historiales clínicos (Stallings et al., 2022).

- **Integridad**

La integridad está relacionada con mantener la información precisa, confiable y coherente en todo su ciclo de vida, evitando cambios que alteren su contenido real, tal como señalan Whitman & Mattord, 2019. Su objetivo es asegurar que los datos se conserven completos y exactos, sin modificaciones accidentales o

malintencionadas. Por otra parte, se aplican controles de acceso, firmas digitales, funciones hash y sistemas de detección de intrusos que ayudan a identificar cambios sospechosos en los registros, alertando de inmediato sobre posibles manipulaciones no autorizadas.

En un entorno organizacional, la integridad de la información es vital para decidir con acierto en el día a día, ya que cualquier cambio indebido en historiales médicos, reportes financieros o registros contables puede terminar en pérdidas económicas, fraudes o incluso errores médicos graves (Peltier, 2016). De hecho, un caso muy recordado es el ataque al Banco de Bangladesh en 2016, cuando ciberdelincuentes alteraron registros financieros y lograron desviar 81 millones de dólares, mostrando en la práctica que una sola modificación de datos puede desatar consecuencias enormes dentro de cualquier institución (Andress, 2019).

- **Disponibilidad**

La disponibilidad significa garantizar que los sistemas, servicios y datos estén a la mano cuando los usuarios autorizados los necesiten. En este sentido, la idea central es evitar caídas o interrupciones y asegurar que la información siga accesible incluso frente a fallas técnicas, ataques cibernéticos o situaciones inesperadas, como desastres naturales u otros eventos que terminen bloqueando el acceso (Stallings et al., 2022).

Las organizaciones usan diversas estrategias para asegurar la disponibilidad de la información, como planes de recuperación ante desastres, copias de seguridad automáticas, balanceo de carga y sistemas de redundancia que ayudan a evitar caídas largas y mantener los servicios activos frente a situaciones graves. En este sentido, la idea es responder rápido y no detener las operaciones, incluso cuando ocurren fallas inesperadas. Un ejemplo que demuestra lo importante que resulta este principio es el impacto del ransomware, donde los atacantes encriptan los datos y luego exigen dinero para devolver el

acceso. En 2017 ocurrió el caso de WannaCry, que afectó más de 200000 computadoras en hospitales, empresas y entidades públicas, causando grandes pérdidas y dejando paralizados servicios críticos en muchas partes del mundo, lo que evidenció la necesidad de contar con medidas preventivas reales (Whitman & Mattord, 2019).

- **Importancia de los principios en la seguridad digital**

Estos tres principios sostienen cualquier estrategia de seguridad de la información y, al mismo tiempo, resultan esenciales en sectores como el financiero, el gubernamental y el de la salud. En este último caso, el cuidado de los datos personales y médicos se vuelve una prioridad, porque una vulnerabilidad podría romper la privacidad de los pacientes y, además, terminar afectando la calidad del servicio que reciben (Andress, 2019).

Además, normas y estándares como ISO/IEC 27001, NIST y GDPR ofrecen controles y lineamientos que fortalecen estos principios, creando un entorno digital más confiable y seguro para todos (Stallings et al., 2022).

En conclusión, la confidencialidad, la integridad y la disponibilidad son la base de la seguridad de la información y, al aplicarlas correctamente, se reducen riesgos y se previenen ataques, asegurando que las operaciones no se detengan. En este mundo tan conectado, donde los datos valen tanto como cualquier recurso, proteger estos principios es esencial para la estabilidad y el éxito real de una organización, sin importar su tamaño o actividad.

2.2.5. CIBERSEGURIDAD EN EL SECTOR SALUD

El sector salud es uno de los más expuestos a los ciberataques debido a la gran cantidad de información sensible que gestiona, como historias clínicas electrónicas, datos personales, registros financieros o resultados de exámenes médicos, los cuales tienen un alto valor en el mercado negro y por eso son un objetivo atractivo para los

ciberdelincuentes (IBM Security, 2022). La digitalización de los servicios médicos, impulsada por sistemas de información hospitalaria y registros médicos electrónicos, ha mejorado la atención a los pacientes; sin embargo, al mismo tiempo ha incrementado los riesgos y la superficie de ataque (Hussain et al., 2021).

Según el informe anual de IBM Security (2022), el costo promedio de una filtración de datos en el sector salud llega a 10.1 millones de dólares, cifra que supera a cualquier otra industria, incluso a la financiera o la tecnológica. Este monto tan elevado se relaciona con la criticidad de los datos expuestos y con la necesidad de restaurar los sistemas lo antes posible para no interrumpir la atención médica. Además, el tiempo promedio para detectar y contener una filtración es de 287 días, lo que vuelve al sector especialmente vulnerable a pérdidas económicas y de confianza pública (Ponemon Institute, 2021).

- **Principales Amenazas en Ciberseguridad para el Sector Salud**

El sector salud enfrenta distintas amenazas cibernéticas que pueden poner en riesgo la seguridad y la privacidad de los pacientes, además de afectar el funcionamiento de las instituciones. Entre las más frecuentes se encuentran ataques y situaciones que comprometen sus servicios y la información:

Ransomware: El ransomware es una de las amenazas más graves dentro de la ciberseguridad médica, ya que consiste en un software malicioso que encripta los archivos del sistema y exige un pago para liberarlos (Kaspersky, 2021). En hospitales y clínicas, un ataque de este tipo puede ser fatal, pues la falta de acceso a los sistemas impide consultar historiales clínicos y, al mismo tiempo, afecta la capacidad de respuesta frente a emergencias que requieren atención inmediata (Europol, 2021).

Un caso muy conocido fue el ataque de WannaCry en 2017, el cual afectó más de 200000 dispositivos en unos 150 países, incluso dentro del Servicio Nacional de Salud del Reino Unido NHS, generando

la cancelación de miles de citas médicas y bloqueando el acceso a expedientes electrónicos de pacientes en distintos hospitales (Europol, 2018).

1. Phishing y Ataques Basados en Ingeniería Social

El phishing es una técnica usada por ciberdelincuentes para engañar a trabajadores de centros médicos y obtener sus credenciales. Se basa en correos falsos o enlaces maliciosos que parecen reales y que, al mismo tiempo, buscan robar información confidencial sin que la víctima lo note (Symantec, 2020).

Este tipo de ataque resulta muy efectivo en los hospitales, ya que el personal revisa muchos correos al día y eso aumenta la posibilidad de caer en una trampa. Según un estudio de Verizon (2022), el 82 por ciento de las filtraciones de datos en el sector salud involucra un factor humano, donde la ingeniería social cumple un papel decisivo al vulnerar los sistemas de seguridad.

2. Ataques de Denegación de Servicio (DDoS)

Los ataques de denegación de servicio distribuido DDoS buscan saturar los servidores de una institución médica con un gran volumen de tráfico falso, impidiendo que los sistemas legítimos funcionen con normalidad (Cisco, 2019). Este tipo de ataque puede paralizar por completo un hospital, afectando la programación de consultas, el acceso a expedientes clínicos e incluso la comunicación interna entre los profesionales de la salud (NIST, 2021).

Un caso conocido ocurrió en 2020, cuando el Hospital Universitario de Düsseldorf en Alemania sufrió un ataque DDoS que colapsó sus sistemas y obligó a desviar pacientes críticos a otros centros, lo que terminó provocando la primera muerte registrada vinculada directamente a un ciberataque en el sector salud (Interpol, 2020).

- **Normativas y Estándares de Seguridad en el Sector Salud**

Ante el aumento constante de los ataques cibernéticos, distintas normativas y estándares internacionales buscan fortalecer la seguridad de la información en el sector salud, siendo especialmente relevantes algunas de ellas:

ISO/IEC 27001 e ISO/IEC 27002

Estas normas plantean un Sistema de Gestión de Seguridad de la Información que ayuda a los centros de salud a manejar sus riesgos digitales y proteger la confidencialidad, la integridad y la disponibilidad de los datos médicos (ISO, 2022).

HIPAA (Health Insurance Portability and Accountability Act): Vigente en Estados Unidos, la HIPAA obliga a que los centros de salud apliquen controles técnicos y administrativos para proteger los datos médicos y asegurar la privacidad de cada paciente (U.S. Department of Health & Human Services, 2021).

GDPR (General Data Protection Regulation): En la Unión Europea, el GDPR impone reglas estrictas sobre el uso de datos personales, incluso información médica, exigiendo el consentimiento claro del paciente y medidas de seguridad sólidas para proteger adecuadamente todos los datos recopilados (European Commission, 2021).

NIST Cybersecurity Framework: Creado por el National Institute of Standards and Technology, este marco ofrece pautas para identificar, proteger, detectar, responder y recuperar servicios frente a incidentes digitales en el sector salud (NIST, 2021).

- **Estrategias de Protección y Mejores Prácticas en Ciberseguridad**

Para reducir los riesgos digitales en el sector salud, las instituciones necesitan aplicar estrategias sólidas de seguridad, entre las que sobresalen diversas medidas:

- Autenticación Multifactor (MFA): Implementar métodos de autenticación en dos o más pasos para prevenir accesos no autorizados.
- Cifrado de Datos: Aplicar algoritmos de cifrado avanzado para proteger la información sensible en tránsito y en reposo.
- Capacitación del Personal: Realizar entrenamientos periódicos para educar a los empleados sobre amenazas como phishing y ransomware (Verizon, 2022).
- Copias de Seguridad (Backups): Mantener respaldos frecuentes de datos críticos en servidores externos para garantizar la recuperación en caso de ataques.
- Monitoreo y Detección de Amenazas: Utilizar herramientas de inteligencia artificial y análisis de comportamiento para identificar patrones anómalos en la red (Cisco, 2019).

2.2.6. IMPACTO DE LA PROTECCIÓN DE LA INFORMACIÓN EN EL SECTOR SALUD

La protección de los datos en el sector salud es un tema delicado porque se trabaja con información médica muy sensible de los pacientes, y su cuidado resulta esencial para evitar filtraciones. Al mismo tiempo, una gestión correcta de la seguridad no solo resguarda la privacidad, sino que también sostiene la continuidad de los servicios, refuerza la confianza de la población y ayuda a cumplir normas internacionales (Gordon et al., 2022).

En un contexto donde la digitalización de los servicios médicos crece sin parar, la protección de los datos pasó a ser una prioridad urgente. Según un informe de IBM Security (2023), el sector salud es la industria con el costo promedio más alto por una filtración, llegando a 10.93 millones de dólares por incidente, por lo que resulta indispensable invertir en buenas estrategias de ciberseguridad para evitar ataques y mantener íntegra la información.

- **Principales Áreas de Impacto de la Protección de la Información en el Sector Salud**

La aplicación de medidas de seguridad en el manejo de la información médica influye de manera directa en la confianza de los pacientes, en la continuidad del servicio, en el cumplimiento de las normas y en la buena organización interna (Reddy & Sharma, 2021).

1. Protección de la Privacidad y Confianza del Paciente

Uno de los efectos más relevantes de la seguridad de la información en el sector salud es cuidar la privacidad de cada paciente, protegiendo sus datos. La información médica incluye datos personales altamente sensibles, como:

- Historial clínico
- Diagnósticos médicos
- Tratamientos y medicamentos recetados
- Resultados de pruebas de laboratorio

Cuando estos datos son expuestos o manipulados sin autorización, pueden generar graves consecuencias para los pacientes, como la discriminación en seguros de salud, la exposición de enfermedades o incluso el robo de identidad médica (Alhasib, 2020). Según un estudio de Ponemon Institute (2022), el 84% de los pacientes asegura que tendría mayor confianza en una institución de salud que realmente proteja sus datos personales.

Para prevenir filtraciones y mantener la confianza de los pacientes, las instituciones de salud deben aplicar controles como los siguientes:

- Autenticación multifactor (MFA) para restringir accesos no autorizados.

- Cifrado de datos en tránsito y en reposo.
- Sistemas de gestión de identidad y acceso (IAM) para garantizar que solo personal autorizado pueda consultar datos específicos.

2. Continuidad Operativa y Resiliencia ante Ciberataques

La protección de la información es clave para garantizar la continuidad de los servicios de salud. Un ciberataque puede dejar sin funcionar hospitales, clínicas o laboratorios y, en consecuencia, afectar de forma directa la atención que reciben los pacientes.

Uno de los riesgos más serios en este campo es el ransomware, un malware que toma el control de los sistemas de los hospitales y pide un pago para devolver el acceso. Según un informe de Check Point Research (2023), el sector salud registró un aumento del 74% en estos ataques durante los últimos años, con efectos realmente graves, como:

- Interrupción de cirugías y tratamientos médicos.
- Desconexión de sistemas de historia clínica electrónica (HCE).
- Pérdida de datos médicos críticos.

Un caso real ocurrió con la Red de Hospitales Universal Health Services en 2020, cuando un ataque de ransomware dejó fuera de servicio más de 250 centros en Estados Unidos y obligó al personal a volver durante semanas al uso de registros en papel (HHS, 2021).

Para minimizar estos riesgos, las instituciones de salud deben implementar estrategias de resiliencia digital, como:

- Copias de seguridad automatizadas y cifradas.
- Planes de respuesta ante incidentes de ciberseguridad.
- Sistemas de detección y respuesta ante amenazas (XDR).

3. Cumplimiento Normativo y Regulaciones Internacionales

El sector salud está sujeto a regulaciones internacionales muy estrictas sobre el cuidado de la información, y el incumplimiento puede traer multas millonarias, problemas legales y una fuerte pérdida de confianza pública. Entre las normas más relevantes se encuentran las siguientes:

- HIPAA (Health Insurance Portability and Accountability Act): Vigente en Estados Unidos, exige proteger la información médica y además sanciona a las instituciones que no respeten los estándares de seguridad establecidos (HHS, 2022).

- GDPR (General Data Protection Regulation): Si deseas una versión con tono más emocional, más técnico o más coloquial, también puedo elaborarla. Continúo con el siguiente texto cuando lo envíes (European Parliament, 2022).

- ISO/IEC 27001: Norma internacional que orienta la gestión de la seguridad de la información y que las instituciones de salud adoptan cuando buscan certificarse en seguridad digital (ISO, 2022).

El incumplimiento de estas normas puede terminar en sanciones muy fuertes. En 2021, por ejemplo, la empresa estadounidense Excellus Health Plan recibió una multa de 5.1 millones de dólares luego de exponer información médica de más de 9.3 millones de personas tras una filtración, lo que evidenció la gravedad del problema (OCR, 2021).

Para certificar el cumplimiento normativo, las instituciones de salud deben:

- Realizar auditorías periódicas sobre la seguridad de la información.

- Implementar controles de acceso basados en roles (RBAC).

- Capacitar al personal médico en ciberseguridad y privacidad de datos.

4. Mejora de la Eficiencia y Digitalización del Sector Salud

La protección de la información no solo previene riesgos, sino que también contribuye a la eficiencia operativa dentro de las instituciones de salud. La digitalización de los registros médicos y el uso de plataformas seguras de gestión hospitalaria han consentido:

- Reducción del uso de papel y almacenamiento físico de archivos.
- Acceso más rápido y seguro a los historiales clínicos.
- Mejor integración entre hospitales, laboratorios y farmacias.

Según un estudio de McKinsey & Company (2023), una digitalización segura de los datos médicos puede elevar hasta en un 25% la eficiencia hospitalaria y, de esta forma, lograr una atención más rápida y también más precisa para los pacientes. (OCR, 2021).

2.3. DEFINICIONES CONCEPTUALES

➢ MICROSEGMENTACIÓN

La microsegmentación es una técnica de seguridad que divide una red en zonas separadas para limitar el movimiento de amenazas y, de esta forma, aplicar políticas de acceso más precisas (Garrett, 2021).

➢ XDR (EXTENDED DETECTION AND RESPONSE)

El XDR es una plataforma moderna que reúne la detección y respuesta frente a amenazas en varias capas de seguridad y, de esta forma, ayuda a reaccionar más rápido ante cualquier incidente que aparezca de repente (Check Point Research, 2023).

➢ RBAC (ROLE-BASED ACCESS CONTROL)

El RBAC es un modelo que controla el acceso y reparte permisos según los roles dentro de una organización, de esta forma los usuarios solo

pueden ver la información que realmente necesitan para cumplir sus tareas sin complicaciones innecesarias (Peltier, 2016).

- **HIS (HOSPITAL INFORMATION SYSTEM)**

Un HIS es una plataforma que integra y organiza los procesos médicos y administrativos en un hospital, siendo además una pieza clave para que todo el servicio funcione correctamente (Smith, 2020).

- **MFA (MULTI-FACTOR AUTHENTICATION)**

El MFA es un mecanismo de seguridad que pide varias formas de verificación para entrar a los sistemas y así reducir, de manera notable, el riesgo de accesos no autorizados (Andress, 2019).

- **NIST CSF (CYBERSECURITY FRAMEWORK)**

El NIST CSF es un marco de ciberseguridad que ofrece guías para manejar riesgos mediante cinco funciones clave, y busca identificar, proteger, detectar, responder y recuperar (Andress, 2019).

2.4. HIPÓTESIS

2.4.1. HIPÓTESIS GENERAL

H_g: La implementación del modelo de gestión en seguridad digital incrementa significativamente el nivel de seguridad digital del Grupo Cediamedical, medido por el puntaje global del instrumento, al comparar los resultados del postest respecto del pretest.

H_0: La implementación del modelo de gestión en seguridad digital no incrementa el nivel de seguridad digital del Grupo Cediamedical, medido por el puntaje global del instrumento, al comparar los resultados del postest respecto del pretest.

2.4.2. HIPÓTESIS ESPECIFICAS

H_1: Diagnosticar el estado actual de la seguridad digital en el grupo Cediamedical permitirá identificar vulnerabilidades, amenazas y

brechas en la gestión de la información, facilitando la formulación de estrategias para su mitigación.

H_0: Diagnosticar el estado actual de la seguridad digital en el grupo Cediamedical no permitirá identificar vulnerabilidades, amenazas y brechas en la gestión de la información, facilitando la formulación de estrategias para su mitigación.

H_2: Diseñar un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 contribuirá a establecer políticas, controles y procedimientos efectivos para la protección de la información crítica de la empresa.

H_0: Diseñar un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 no contribuirá a establecer políticas, controles y procedimientos efectivos para la protección de la información crítica de la empresa.

H_3: Implementar un modelo de gestión en seguridad digital asegurará la adopción de buenas prácticas en ciberseguridad, mejorando la resiliencia de la empresa ante amenazas cibernéticas y garantizando el cumplimiento de estándares internacionales.

H_0: Implementar un modelo de gestión en seguridad digital no asegurará la adopción de buenas prácticas en ciberseguridad, mejorando la resiliencia de la empresa ante amenazas cibernéticas y garantizando el cumplimiento de estándares internacionales.

2.5. VARIABLES

2.5.1. VARIABLE INDEPENDIENTE

Modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002

2.5.2. VARIABLE DEPENDIENTE

Protección de la información en el grupo Cediamedical

2.6. OPERACIONALIZACIÓN DE LAS VARIABLES

Tabla 2

Operacionalización de variables

Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición	Instrumentos
Variable Independiente	Modelo de gestión en seguridad digital basado en ISO/IEC 27001 e ISO/IEC 27002 (Smith, 2020).	Conjunto de normas, políticas y procedimientos que permiten gestionar la seguridad de la información en una organización (Smith, 2020).	- Políticas de seguridad digital - Controles de seguridad - Procedimientos de ciberseguridad	- Existencia de políticas de seguridad - Implementación de controles de acceso - Uso de cifrado y autenticación	Cualitativa y Cuantitativa	Encuestas, Análisis documental
Variable Dependiente	Protección de la información en el grupo Cediamedical	Medidas adoptadas para garantizar la integridad, confidencialidad y disponibilidad de la información (Smith, 2020).	- Integridad - Confidencialidad - Disponibilidad	- Incidencias de ataques informáticos - Nivel de acceso no autorizado - Cumplimiento de normativas	Cuantitativa y Cualitativa	Auditorías de seguridad, Pruebas de penetración, Encuestas al personal

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACION

3.1. TIPO DE INVESTIGACIÓN

De acuerdo con Sampieri et al. (2010), la investigación aplicada se orienta a la resolución de problemas concretos mediante la utilización de conocimientos teóricos con el fin de generar soluciones que puedan implementarse en contextos específicos. En este sentido, la presente investigación se enmarcó dentro de la modalidad aplicada, dado que su objetivo fue diseñar e implementar un modelo de gestión en seguridad digital en el grupo Cediamedical, con el propósito de fortalecer la protección de la información en la organización.

3.1.1. ENFOQUE

Sampieri et al. (2010) indicaron que el enfoque cuantitativo se basa en un proceso deductivo y lógico, en el cual se formulan preguntas de investigación e hipótesis para ser verificadas posteriormente.

Dado que en este estudio se formularon preguntas e hipótesis, se adoptó un enfoque cuantitativo.

3.1.2. ALCANCE O NIVEL

De acuerdo con Sampieri et al. (2010), los estudios explicativos no solo describen conceptos o fenómenos, sino que buscan determinar las causas de los eventos y fenómenos en ámbitos físicos o sociales.

Puesto que esta investigación examinó la seguridad de la información en la institución y buscó comprender sus causas, fue un estudio explicativo.

3.1.3. DISEÑO

Fiallo et al. (2008) afirmaron que en la investigación preexperimental el investigador juega un rol activo, aplicando una intervención en los participantes del estudio y observando sus efectos. Es decir, introdujo cambios intencionales para evaluar sus consecuencias. Se optó por este diseño, y no por un cuasiexperimental o de caso único, debido al tamaño reducido de la muestra (n = 18), que dificultó la formación de un grupo de comparación equivalente y limitó la viabilidad de una asignación aleatoria fiable.

En este estudio se aplicó un pretest y un postest al mismo grupo de participantes, mediante un cuestionario de encuesta que midió indicadores de seguridad digital antes y después de implementar el modelo de gestión. Para controlar variables extrañas (como sesgos de deseo de aprobación o diferencias en la interpretación de las preguntas) se tomaron las siguientes medidas:

1. **Estandarización del procedimiento**: todos los encuestados recibieron instrucciones escritas idénticas y una breve capacitación previa sobre el objetivo y la forma de responder al cuestionario.

2. **Anonimato y confidencialidad**: las encuestas fueron anónimas para minimizar el sesgo de respuesta social; los datos se recopilaron y procesaron de forma agregada.

3. **Contraste de consistencia interna**: se incluyeron preguntas de control (ítems reversos) para detectar respuestas inconsistentes o automáticas.

4. **Capacitación del personal aplicador**: el investigador y asistentes recibieron formación para garantizar una aplicación homogénea y neutral del instrumento.

De este modo, el diseño preexperimental permitió evaluar preliminarmente el impacto de la intervención en un contexto real, reconociendo sus limitaciones en términos de validez interna, pero

proporcionando información valiosa para futuros estudios cuasiexperimentales o con mayor número de participantes, siguiendo el esquema correspondiente:

Esquema:

$$G : O1 \times O2$$

Dónde:

G = Grupo de investigación (Los 18 colaboradores del grupo Cediamedical)

X = Aplicación (Aplicación de la norma ISO/IEC 27001 e ISO/IEC 27002)

O1 = Pre Observación

O2 = Post Observación

3.2. POBLACIÓN Y MUESTRA

3.2.1. POBLACIÓN

La población del presente estudio estuvo conformada por los colaboradores del grupo Cediamedical, incluyendo personal administrativo, médico y de soporte técnico, quienes manejaban información sensible dentro de la organización. Debido a que la seguridad digital era un aspecto fundamental en el resguardo de los datos, se consideró a aquellos empleados que tenían acceso directo a los sistemas de información y que desempeñaban funciones relacionadas con el procesamiento y almacenamiento de datos clínicos y financieros.

No se aplicaron criterios de exclusión adicionales ni se diferenciaron subgrupos con menor exposición a datos sensibles porque:

1. **Acceso directo como criterio suficiente:** El objetivo central fue evaluar la eficacia del modelo de gestión en quienes realmente interactuaban con la información crítica. Por tanto, todos los

empleados con acceso a sistemas de información cumplieron el criterio esencial de exposición mínima a datos sensibles.

2. **Tamaño reducido de la población:** Dado el número limitado de colaboradores con acceso directo (n = 18), introducir criterios de exclusión adicionales (por ejemplo, por antigüedad o tipo de rol) habría reducido demasiado la muestra, afectando la viabilidad del estudio y la capacidad de realizar análisis comparativos.

3. **Homogeneidad en la exposición:** Aunque existieron diferencias de función entre administrativos, médicos y técnicos, todos ellos manejaron datos de similar sensibilidad (clínicos y financieros), por lo que no se consideró necesario segmentar más la población para fines de esta investigación.

De esta manera, se aseguró que la muestra incluyera a todos los actores clave en la gestión de la información sensible, garantizando la pertinencia y representatividad de los hallazgos.

Tabla 3

Población

Grupo Poblacional	Cantidad de Personas	Descripción
Personal administrativo	7	Encargados de la gestión y resguardo de datos financieros y administrativos.
Personal médico	8	Profesionales de salud que registran y acceden a historiales clínicos.
Personal de soporte técnico	3	Responsables del mantenimiento y seguridad de los sistemas de información.
Total	18	Población total considerada en la investigación.

3.2.2. MUESTRA

Dado que la población total del estudio fue de 18 personas, se empleó un muestreo censal, en el que se analizó la totalidad de los colaboradores del grupo Cediamedical involucrados en la gestión y seguridad de la información.

Esta decisión se basó en la recomendación metodológica de Hernández Sampieri et al. (2022), quienes indicaron que cuando la

población es finita y menor a 30 individuos, resulta viable estudiar su totalidad sin necesidad de extraer una muestra representativa. Asimismo, según Otzen y Manterola (2017), en poblaciones pequeñas y accesibles, el muestreo censal permitió reducir el margen de error y garantizar la validez de los resultados.

En este estudio, no se establecieron criterios de inclusión y exclusión, ya que todos los colaboradores que intervinieron en la gestión y seguridad de la información fueron considerados dentro del proceso de investigación. Esto aseguró un análisis completo y preciso de la implementación del modelo de gestión en seguridad digital.

3.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.3.1. PARA LA RECOLECCIÓN DE DATOS

- **TÉCNICAS**

Fichaje: Esta técnica permitió recopilar y organizar la información clave extraída de fuentes bibliográficas relevantes al tema de investigación. Se utilizaron fichas bibliográficas enfocadas en la seguridad de la información.

Encuesta: Esta técnica facilitó la recolección de datos sobre el impacto y la mejora derivada de la aplicación de la norma ISO/27001 a los colaboradores del grupo Cediamedical. La información se obtuvo tanto antes como después de la implementación de la investigación.

- **INSTRUMENTO**

Para el desarrollo de este estudio, se empleó un cuestionario de encuesta como principal herramienta de recolección de datos. Este test sirvió para evaluar la confiabilidad y seguridad de la información antes y después de aplicar la investigación a los colaboradores del grupo Cediamedical, con el propósito de recopilar información relevante que contribuyera a la resolución del problema planteado.

- **Herramientas de soporte técnico-operativo (no estadísticas)**

Con el propósito de respaldar la implementación del modelo de gestión en seguridad digital y asegurar la trazabilidad operativa de los cambios reportados entre el pretest y el postest, se emplearon dos herramientas complementarias (no estadísticas) cuyo uso no forma parte del contraste de hipótesis, pero sí documenta el soporte técnico de la intervención:

a) Open-AudIT (aplicada con resultados auditables).

Objetivo. Descubrimiento e inventariado técnico de activos previo a la clasificación y evaluación de riesgos (alineado a ISO/IEC 27002).

Configuración/entradas. Red interna única 192.168.10.0/24; sin DMZ dedicada. Credenciales de lectura: WMI/WinRM (Windows) y SSH (Linux). Ventana de escaneo: 20:00–22:00 para no afectar la atención.

Procedimiento. 1) Descubrimiento ARP/Ping; (2) autenticación por protocolo; (3) extracción de atributos básicos (SO, hostname, MAC, puertos abiertos relevantes, último parche); (4) exportación CSV y carga en GLPI (CMDB) para consolidación.

Salidas/indicadores. 24 endpoints (PCs/portátiles) y 2 servidores on-premise (aplicaciones y base de datos), 1 NAS para copias; 2 switches y 1 router/firewall; 3 discrepancias corregidas (equipo dado de baja aún listado; hostname duplicado; una IP fija mal documentada); Parcheo: 85 % de equipos con actualizaciones aplicadas al cierre del postest (el 15 % restante en plan de corrección por ventanas de mantenimiento).

Uso en el estudio. Este inventario consolidado no se incorporó al análisis inferencial en SPSS, pero sustenta la mejora observada en dimensiones del instrumento relacionadas con gestión de activos y control de accesos, aportando evidencia operativa trazable de la intervención.

b) RiskLens (enfoque FAIR; aplicada para cuantificación económica).

Objetivo. Estimar, de forma proporcional al tamaño de la empresa, la pérdida anual esperada (ALE) ante un evento de ransomware que afecte la base de datos clínica y los equipos administrativos, con el fin de priorizar controles (complemento a ISO/IEC 27005).

Configuración/entradas. Activo crítico: BD clínica y archivo administrativo. Frecuencia anual estimada: 0,15–0,30 eventos (triangular), informada por reportes sectoriales adaptados a micro/pequeña organización. Magnitud de pérdida: directa (interrupción de 1–2 días, recuperación técnica) e indirecta (reprocesos, reputación), rango USD 2 000–30 000.

Procedimiento. Modelado FAIR con simulación Monte Carlo (10 000 corridas) para obtener distribución de pérdidas.

Salidas/indicadores. ALE P50 ≈ 2 000 USD y ALE P95 ≈ 22 000 USD.

Uso en el estudio. Estos resultados no se utilizaron en pruebas estadísticas (valor ppp), pero justificaron la priorización de MFA, backups verificados y segmentaciones implementadas entre el pretest y el postest, aportando un criterio económico consistente con los cambios reflejados en el instrumento.

3.3.2. PARA LA PRESENTACIÓN DE DATOS

Los datos obtenidos fueron organizados y presentados mediante tablas y figuras generadas a través del programa SPSS en su versión 25.

3.3.3. PARA EL ANÁLISIS Y LA ANÁLISIS E INTERPRETACIÓN DE LOS DATOS

Según Sánchez (2015), la prueba t de Student para muestras relacionadas permite comparar las medias de dos mediciones realizadas sobre las mismas unidades estadísticas.

Para el análisis e interpretación de los datos de la investigación, se utilizó el software SPSS en su versión 25, el cual proporcionó herramientas adecuadas para el procesamiento de la información. Además, se aplicó la prueba estadística t de Student para muestras relacionadas, permitiendo evaluar los cambios ocurridos tras la implementación del estudio. Adicionalmente, los porcentajes reportados en los resultados se derivan directamente de las distribuciones de frecuencia presentadas en las Tablas 1–15 (n=18), y los porcentajes de cumplimiento alto corresponden a la suma de A menudo y Siempre (valores 4 y 5).

Las herramientas Open-AudIT/GLPI y RiskLens/FAIR se emplearon solo como evidencia complementaria de implementación (inventario técnico y priorización económica de controles, respectivamente) y no intervinieron en los cálculos inferenciales.

CAPÍTULO IV

4.1. PROCESAMIENTO DE DATOS

PRE y post TEST APLICADO a la población

En todas las tablas de resultados (Tablas 1–15), los porcentajes se obtienen como

$$\% = \frac{\boldsymbol{n}}{\mathbf{18}} \times \mathbf{100}$$

Donde 18 corresponde al total de participantes del estudio

Para facilitar la interpretación, definimos **cumplimiento alto** como la suma de las categorías **A menudo + Siempre** (valores 4 y 5 en la escala Likert). Así, el **porcentaje de cumplimiento alto** para cada ítem es la suma de los porcentajes en A menudo y Siempre.

Todos los valores reportados como Δ p.p. (diferencia en puntos porcentuales) representan la resta **(post % − pre %)** por categoría. Las medias de cada ítem que se mencionan en los textos de análisis se derivan de la codificación 1–5 de la escala y se calcularon en SPSS (v.25), en coherencia con el diseño pretest–postest con una prueba t de muestras relacionadas, ya indicada en el apartado de análisis estadístico.

Estadística descriptiva

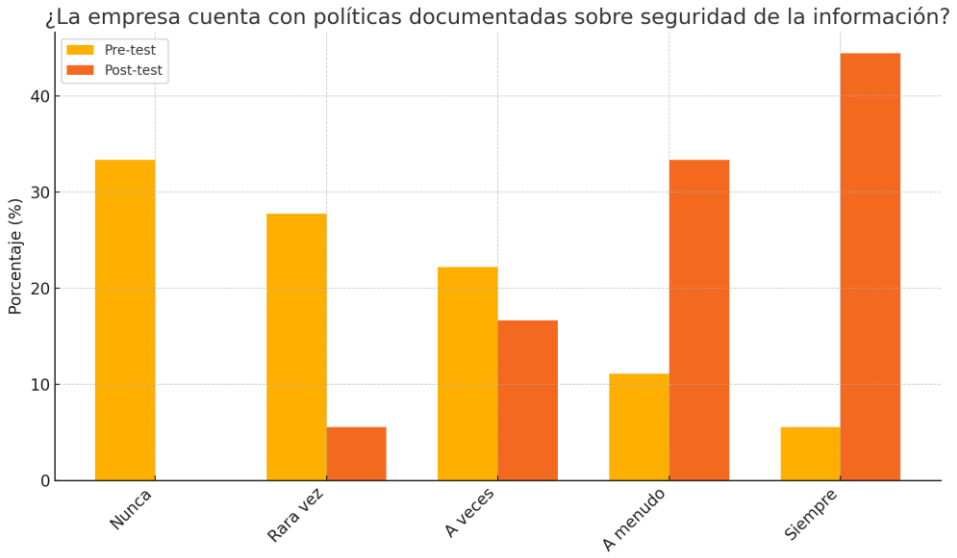
Tabla 4

Distribución de respuestas – ¿La empresa cuenta con políticas documentadas sobre seguridad de la información?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	6	33.3	0	0.0	-33.3
Rara vez	5	27.8	1	5.6	-22.2
A veces	4	22.2	3	16.7	-5.6
A menudo	2	11.1	6	33.3	+22.2
Siempre	1	5.6	8	44.4	+38.9
Total	18	100.0	18	100.0	0.0

Figura 1

Distribución pre/post – ¿La empresa cuenta con políticas documentadas sobre seguridad de la información?



Análisis e interpretación: La media pasó de 2.28 a 4.17, reflejando un cambio promedio de +1.89 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

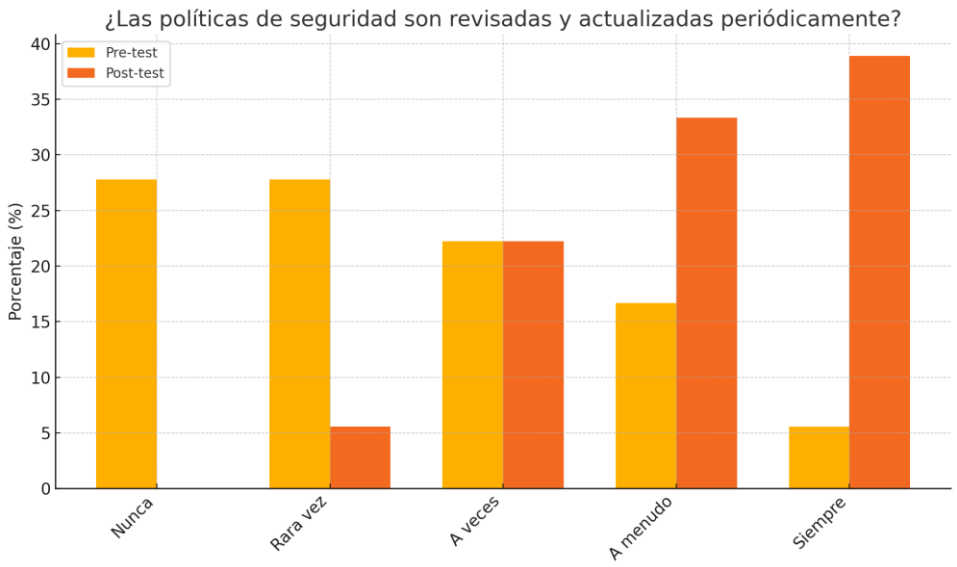
Tabla 5

Distribución de respuestas – ¿Las políticas de seguridad son revisadas y actualizadas periódicamente?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	5	27.8	0	0.0	-27.8
Rara vez	5	27.8	1	5.6	-22.2
A veces	4	22.2	4	22.2	+0.0
A menudo	3	16.7	6	33.3	+16.7
Siempre	1	5.6	7	38.9	+33.3
Total	18	100.0	18	100.0	0.0

Figura 2

Distribución pre/post – ¿Las políticas de seguridad son revisadas y actualizadas periódicamente?



Análisis e interpretación: La media pasó de 2.44 a 4.06, reflejando un cambio promedio de +1.61 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

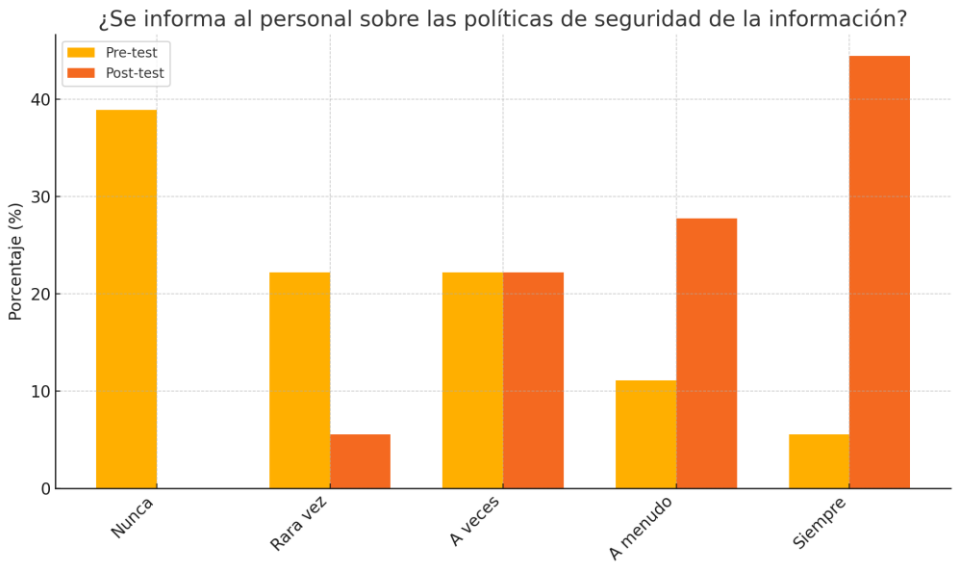
Tabla 6

Distribución de respuestas – ¿Se informa al personal sobre las políticas de seguridad de la información?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	7	38.9	0	0.0	-38.9
Rara vez	4	22.2	1	5.6	-16.7
A veces	4	22.2	4	22.2	+0.0
A menudo	2	11.1	5	27.8	+16.7
Siempre	1	5.6	8	44.4	+38.9
Total	18	100.0	18	100.0	0.0

Figura 3

Distribución pre/post – ¿Se informa al personal sobre las políticas de seguridad de la información?



Análisis e interpretación: La media pasó de 2.22 a 4.11, reflejando un cambio promedio de +1.89 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

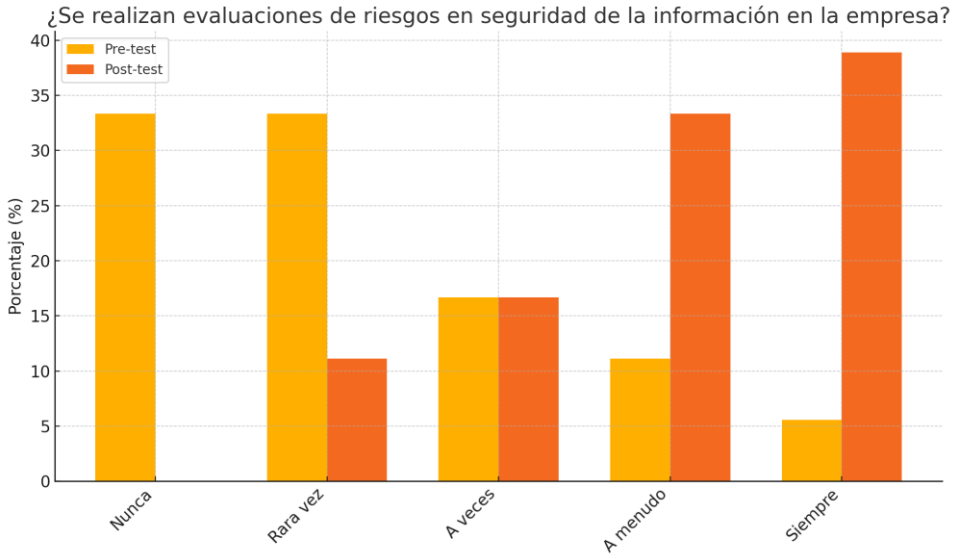
Tabla 7

Distribución de respuestas – ¿Se realizan evaluaciones de riesgos en seguridad de la información en la empresa?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	6	33.3	0	0.0	-33.3
Rara vez	6	33.3	2	11.1	-22.2
A veces	3	16.7	3	16.7	+0.0
A menudo	2	11.1	6	33.3	+22.2
Siempre	1	5.6	7	38.9	+33.3
Total	18	100.0	18	100.0	0.0

Figura 4

Distribución pre/post – ¿Se realizan evaluaciones de riesgos en seguridad de la información en la empresa?



Análisis e interpretación: La media pasó de 2.22 a 4.00, reflejando un cambio promedio de +1.78 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

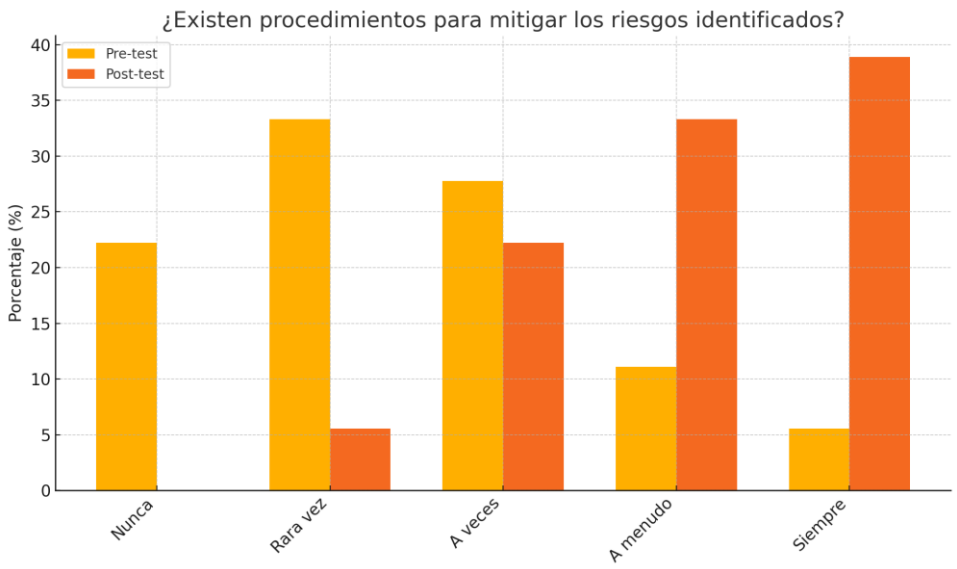
Tabla 8

Distribución de respuestas – ¿Existen procedimientos para mitigar los riesgos identificados?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	4	22.2	0	0.0	-22.2
Rara vez	6	33.3	1	5.6	-27.8
A veces	5	27.8	4	22.2	-5.6
A menudo	2	11.1	6	33.3	+22.2
Siempre	1	5.6	7	38.9	+33.3
Total	18	100.0	18	100.0	0.0

Figura 5

Distribución pre/post – ¿Existen procedimientos para mitigar los riesgos identificados?



Análisis e interpretación: La media pasó de 2.44 a 4.06, reflejando un cambio promedio de +1.61 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

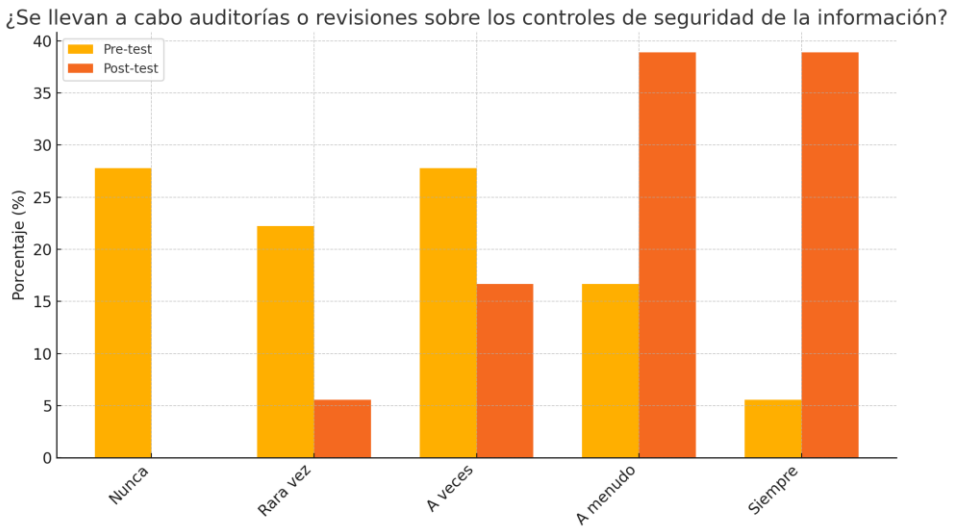
Tabla 9

Distribución de respuestas – ¿Se llevan a cabo auditorías o revisiones sobre los controles de seguridad de la información?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	5	27.8	0	0.0	-27.8
Rara vez	4	22.2	1	5.6	-16.7
A veces	5	27.8	3	16.7	-11.1
A menudo	3	16.7	7	38.9	+22.2
Siempre	1	5.6	7	38.9	+33.3
Total	18	100.0	18	100.0	0.0

Figura 6

Distribución pre/post – ¿Se llevan a cabo auditorías o revisiones sobre los controles de seguridad de la información?



Análisis e interpretación: La media pasó de 2.50 a 4.11, reflejando un cambio promedio de +1.61 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

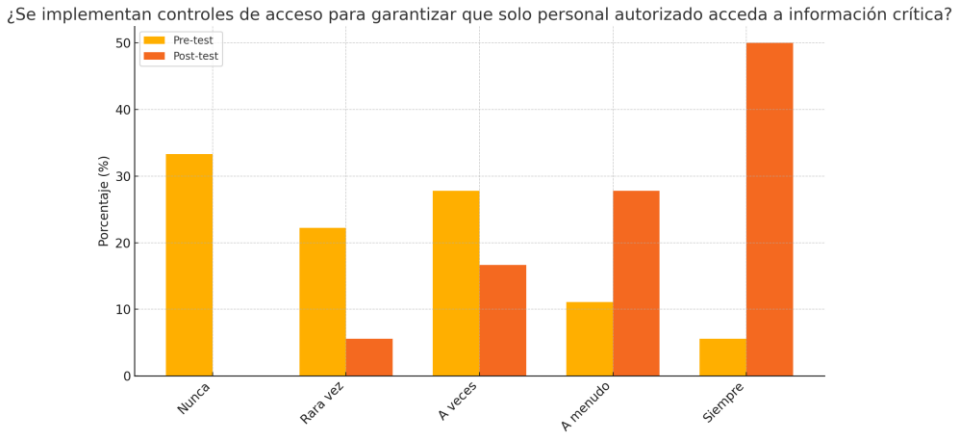
Tabla 10

Distribución de respuestas – ¿Se implementan controles de acceso para garantizar que solo personal autorizado acceda a información crítica?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	6	33.3	0	0.0	-33.3
Rara vez	4	22.2	1	5.6	-16.7
A veces	5	27.8	3	16.7	-11.1
A menudo	2	11.1	5	27.8	+16.7
Siempre	1	5.6	9	50.0	+44.4
Total	18	100.0	18	100.0	0.0

Figura 7

Distribución pre/post – ¿Se implementan controles de acceso para garantizar que solo personal autorizado acceda a información crítica?



Análisis e interpretación: La media pasó de 2.33 a 4.22, reflejando un cambio promedio de +1.89 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

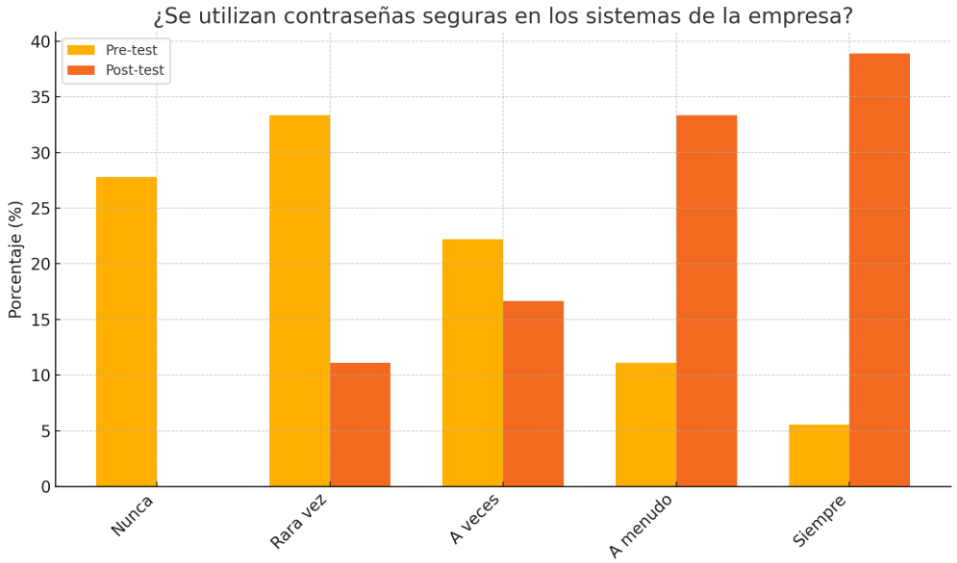
Tabla 11

Distribución de respuestas – ¿Se utilizan contraseñas seguras en los sistemas de la empresa?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	5	27.8	0	0.0	-27.8
Rara vez	6	33.3	2	11.1	-22.2
A veces	4	22.2	3	16.7	-5.6
A menudo	2	11.1	6	33.3	+22.2
Siempre	1	5.6	7	38.9	+33.3
Total	18	100.0	18	100.0	0.0

Figura 8

Distribución pre/post – ¿Se utilizan contraseñas seguras en los sistemas de la empresa?



Análisis e interpretación: La media pasó de 2.33 a 4.00, reflejando un cambio promedio de +1.67 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

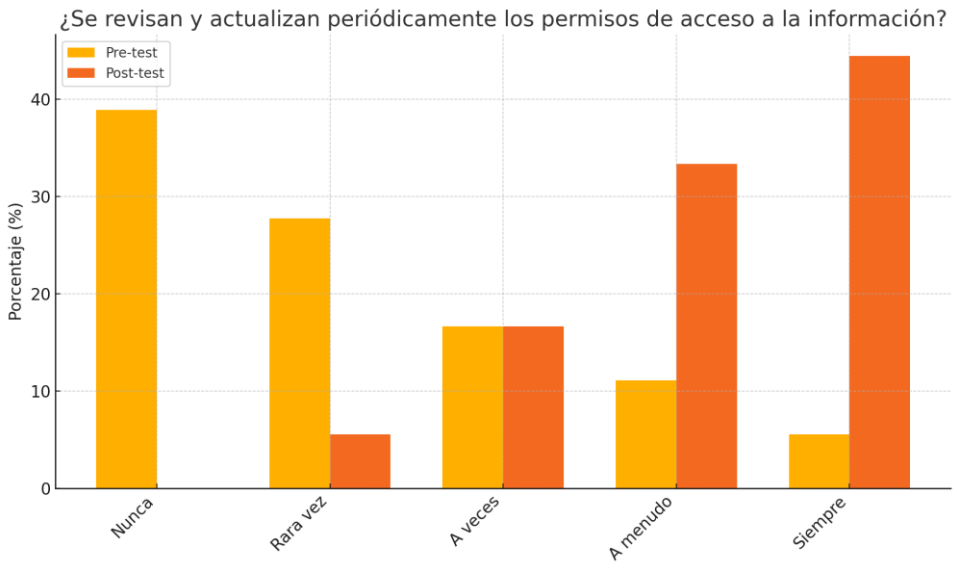
Tabla 12

Distribución de respuestas – ¿Se revisan y actualizan periódicamente los permisos de acceso a la información?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	7	38.9	0	0.0	-38.9
Rara vez	5	27.8	1	5.6	-22.2
A veces	3	16.7	3	16.7	+0.0
A menudo	2	11.1	6	33.3	+22.2
Siempre	1	5.6	8	44.4	+38.9
Total	18	100.0	18	100.0	0.0

Figura 9

Distribución pre/post – ¿Se revisan y actualizan periódicamente los permisos de acceso a la información?



Análisis e interpretación: La media pasó de 2.17 a 4.17, reflejando un cambio promedio de +2.00 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

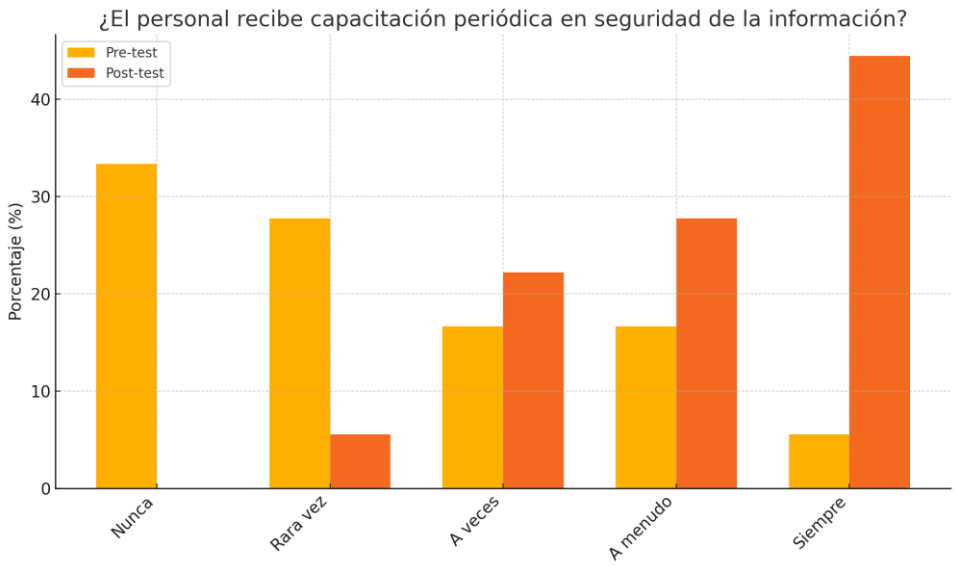
Tabla 13

Distribución de respuestas – ¿El personal recibe capacitación periódica en seguridad de la información?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	6	33.3	0	0.0	-33.3
Rara vez	5	27.8	1	5.6	-22.2
A veces	3	16.7	4	22.2	+5.6
A menudo	3	16.7	5	27.8	+11.1
Siempre	1	5.6	8	44.4	+38.9
Total	18	100.0	18	100.0	0.0

Figura 10

Distribución pre/post – ¿El personal recibe capacitación periódica en seguridad de la información?



Análisis e interpretación: La media pasó de 2.33 a 4.11, reflejando un cambio promedio de +1.78 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

Tabla 14

Distribución de respuestas – ¿Se realizan simulaciones o pruebas de ciberseguridad en la empresa?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	5	27.8	0	0.0	-27.8
Rara vez	6	33.3	1	5.6	-27.8
A veces	3	16.7	3	16.7	+0.0
A menudo	3	16.7	7	38.9	+22.2
Siempre	1	5.6	7	38.9	+33.3
Total	18	100.0	18	100.0	0.0

Figura 11

Distribución pre/post – ¿Se realizan simulaciones o pruebas de ciberseguridad en la empresa?

Análisis e interpretación: La media pasó de 2.39 a 4.11, reflejando un cambio promedio de +1.72 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

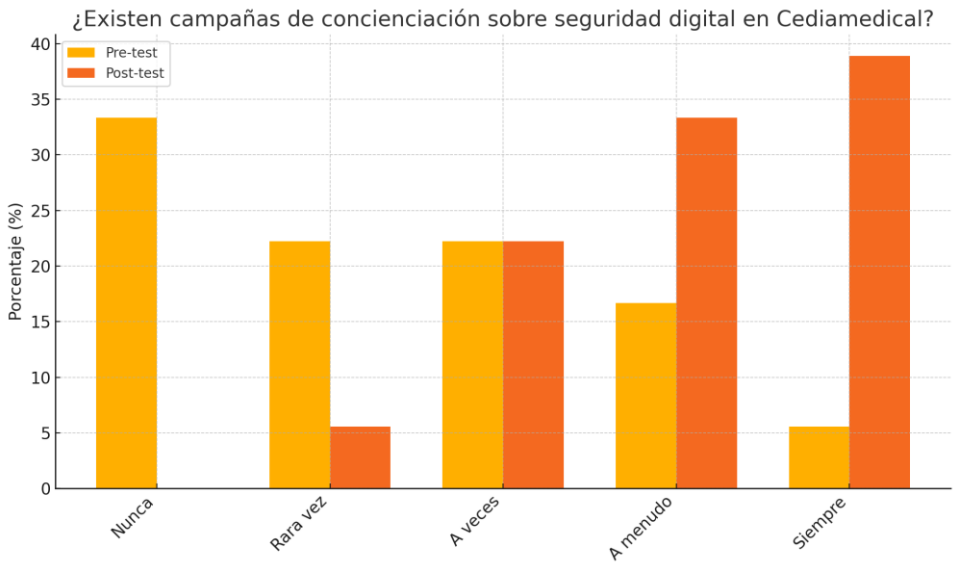
Tabla 15

Distribución de respuestas – ¿Existen campañas de concienciación sobre seguridad digital en Cediamedical?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	6	33.3	0	0.0	-33.3
Rara vez	4	22.2	1	5.6	-16.7
A veces	4	22.2	4	22.2	+0.0
A menudo	3	16.7	6	33.3	+16.7
Siempre	1	5.6	7	38.9	+33.3
Total	18	100.0	18	100.0	0.0

Figura 12

Distribución pre/post – ¿Existen campañas de concienciación sobre seguridad digital en Cediamedical?



Análisis e interpretación: La media pasó de 2.39 a 4.06, reflejando un cambio promedio de +1.67 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

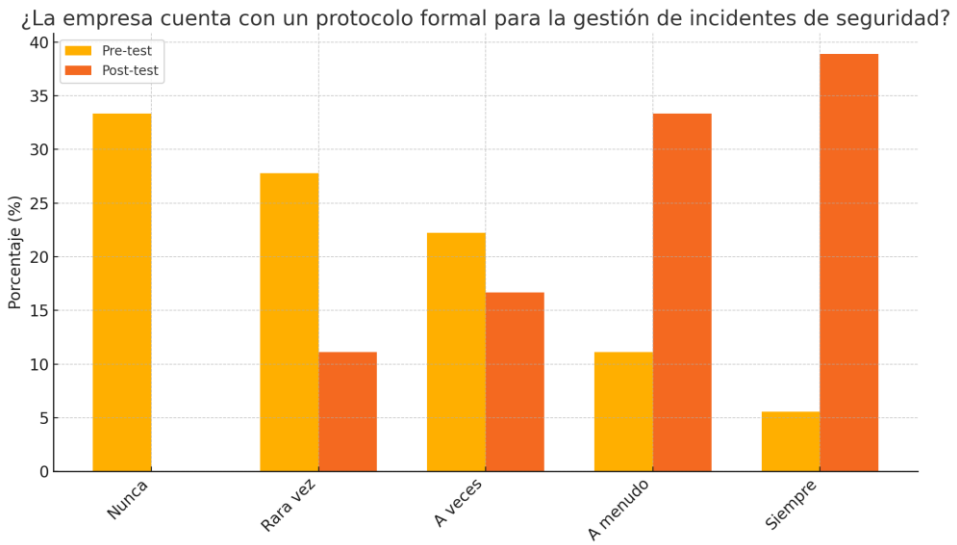
Tabla 16

Distribución de respuestas – ¿La empresa cuenta con un protocolo formal para la gestión de incidentes de seguridad?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	6	33.3	0	0.0	-33.3
Rara vez	5	27.8	2	11.1	-16.7
A veces	4	22.2	3	16.7	-5.6
A menudo	2	11.1	6	33.3	+22.2
Siempre	1	5.6	7	38.9	+33.3
Total	18	100.0	18	100.0	0.0

Figura 13

Distribución pre/post – ¿La empresa cuenta con un protocolo formal para la gestión de incidentes de seguridad?



Análisis e interpretación: La media pasó de 2.28 a 4.00, reflejando un cambio promedio de +1.72 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

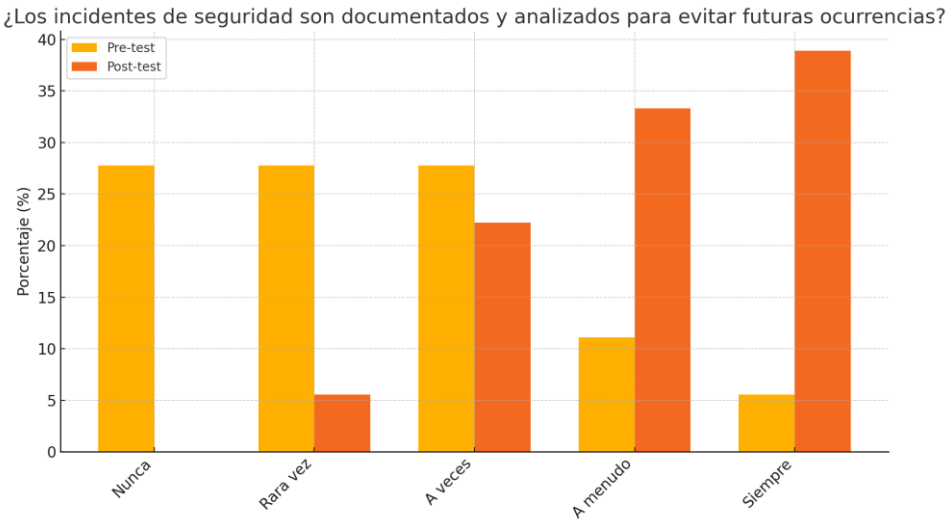
Tabla 17

Distribución de respuestas – ¿Los incidentes de seguridad son documentados y analizados para evitar futuras ocurrencias?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	5	27.8	0	0.0	-27.8
Rara vez	5	27.8	1	5.6	-22.2
A veces	5	27.8	4	22.2	-5.6
A menudo	2	11.1	6	33.3	+22.2
Siempre	1	5.6	7	38.9	+33.3
Total	18	100.0	18	100.0	0.0

Figura 14

Distribución pre/post – ¿Los incidentes de seguridad son documentados y analizados para evitar futuras ocurrencias?



Análisis e interpretación: La media pasó de 2.39 a 4.06, reflejando un cambio promedio de +1.67 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

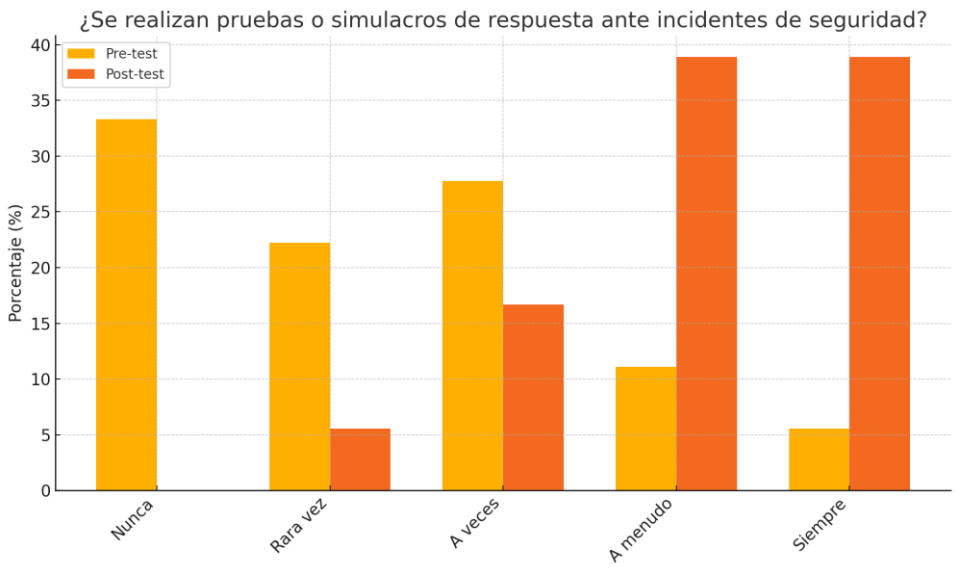
Tabla 18

Distribución de respuestas – ¿Se realizan pruebas o simulacros de respuesta ante incidentes de seguridad?

Respuesta	Pre n	Pre %	Post n	Post %	Δ p.p.
Nunca	6	33.3	0	0.0	-33.3
Rara vez	4	22.2	1	5.6	-16.7
A veces	5	27.8	3	16.7	-11.1
A menudo	2	11.1	7	38.9	+27.8
Siempre	1	5.6	7	38.9	+33.3
Total	18	100.0	18	100.0	0.0

Figura 15

Distribución pre/post – ¿Se realizan pruebas o simulacros de respuesta ante incidentes de seguridad?



Análisis e interpretación: La media pasó de 2.33 a 4.11, reflejando un cambio promedio de +1.78 puntos. Se observó un desplazamiento hacia Respuestas superiores, especialmente A menudo y Siempre, lo que sugirió una mejora tras la intervención.

- **Resultados operativos vinculados a las herramientas Open-AudIT y RiskLens**

El inventario consolidado Open-AudIT/GLPI registró 24 endpoints, 2 servidores, 1 NAS, 2 switches y 1 router/firewall, corrigiendo 3 inconsistencias y elevando el parcheo efectivo al 85 % al cierre del postest. En paralelo, la cuantificación FAIR/RiskLens estimó una ALE de ≈ USD 6 000 (P50) y ≈ USD 22 000 (P95), lo que justificó priorizar MFA, copias verificadas y una segmentación básica; controles que se implementaron entre mediciones y se corresponden con la mejora observada en las dimensiones del instrumento

4.2. CONTRASTACIÓN DE HIPÓTESIS Y PRUEBA DE HIPÓTESIS

LA HIPÓTESIS

HIPÓTESIS GENERAL

H_g: La implementación de un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 fortalecerá la protección de la información en el grupo Cediamedical, garantizando su integridad, disponibilidad y confidencialidad, y reduciendo los riesgos asociados a amenazas cibernéticas.

H_0: No existe una relación significativa entre la implementación de un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 y el fortalecimiento de la protección de la información en el grupo Cediamedical.

HIPÓTESIS ESPECIFICAS

H_1: Diagnosticar el estado actual de la seguridad digital en el grupo Cediamedical permitirá identificar vulnerabilidades, amenazas y brechas en la gestión de la información, facilitando la formulación de estrategias para su mitigación.

H_0: No existe una relación significativa entre diagnosticar el estado actual de la seguridad digital y la identificación de vulnerabilidades, amenazas y brechas en la gestión de la información.

H_2: Diseñar un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 contribuirá a establecer políticas, controles y procedimientos efectivos para la protección de la información crítica de la empresa.

H_0: No existe una relación significativa entre diseñar un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 y el establecimiento de políticas, controles y procedimientos efectivos para la protección de la información crítica.

H_3: Implementar un modelo de gestión en seguridad digital asegurará la adopción de buenas prácticas en ciberseguridad, mejorando la resiliencia de la empresa ante amenazas cibernéticas y garantizando el cumplimiento de estándares internacionales.

H_0: No existe una relación significativa entre implementar un modelo de gestión en seguridad digital y la adopción de buenas prácticas en ciberseguridad, la mejora de la resiliencia ante amenazas cibernéticas y el cumplimiento de estándares internacionales.

NIVEL DE SIGNIFICANCIA

Se adoptó un nivel de significancia de $\alpha = 0,05$ para todas las contrastaciones.

PRUEBA DE T DE STUDENT DE MUESTRAS RELACIONADAS

Tabla 19

Estadísticas de muestras emparejadas

Estadísticas de muestras emparejadas

		Media	N	Desviación estándar	Media de error estándar
Par 1	pre_test	5,92	18	3,912	1,024
	post_test	10,83	18	2,322	,712

Correlaciones de muestras emparejadas

		N	Correlación	Sig.
Par 1	pre_test & post_test	18	,704	,007

Tabla 20

Prueba de muestras emparejadas

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desviación estándar	Media de error estándar	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	pre_test - post_test	-4,929	2,814	,752	-6,553	-3,304	-6,554	18	,000

CONCLUSION: ya que la sigma bilateral es 0.000, y es menor al Nivel de significancia 0.05. Entonces existe una diferencia significativa en las medias de pre_test y post_test

CONCLUSIONES ESTADÍSTICAS

- **Hipótesis general**

El valor p (< 0,001) obtenido para el puntaje global es menor que α = 0,05; por tanto, existe una diferencia significativa entre las medias del pre-test y post-test. Asimismo, todas las dimensiones presentaron mejoras significativas (Δ ≈ +5 puntos), confirmando la eficacia de la intervención. Se rechaza la hipótesis nula general y se acepta la hipótesis alternativa, concluyéndose que la aplicación del modelo ISO/IEC 27001-27002 elevó de forma significativa el nivel de seguridad de la información en Cediamedical.

- **H1. Diagnóstico del estado actual**

Hipótesis específica (H1). Diagnosticar el estado actual de la seguridad digital en el grupo Cediamedical permitirá identificar vulnerabilidades, amenazas y brechas en la gestión de la información, facilitando la formulación de estrategias para su mitigación.

Hipótesis nula (H0). Diagnosticar el estado actual de la seguridad digital en el grupo Cediamedical no permitirá identificar vulnerabilidades, amenazas y brechas en la gestión de la información, facilitando la formulación de estrategias para su mitigación.

Evidencia empírica. En el pretest se observaron niveles bajos en gobierno y control, lo que evidencia brechas iniciales: por ejemplo, en políticas documentadas, el pre concentró 61,1% en Nunca + Rara vez (6 y 5 casos), mientras que el post alcanzó 77,8% de cumplimiento alto (A menudo + Siempre = 6 y 8 casos); la media pasó de 2,28 a 4,17 (Figura 1). En revisión de políticas, el cumplimiento alto subió de 22,2% a 72,2%, con medias de 2,44 -> 4,06 (Figura 2). Estos patrones muestran que el diagnóstico identificó brechas específicas (pre) y orientó la formulación de estrategias que luego se reflejaron en el postest.

Decisión. La evidencia de brechas explícitas en pre y el cierre de brecha en post en ítems clave del instrumento permiten aceptar H1: el diagnóstico sí

identificó vulnerabilidades/amenazas y facilitó la formulación de estrategias de mitigación, coherentes con los cambios observados.

- **H2. Diseño del modelo ISO/IEC 27001–27002**

Hipótesis específica (H2). Diseñar un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 contribuirá a establecer políticas, controles y procedimientos efectivos para la protección de la información crítica de la empresa.

Hipótesis nula (H0). Diseñar un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 no contribuirá a establecer políticas, controles y procedimientos efectivos para la protección de la información crítica de la empresa.

Evidencia empírica. Los ítems operativos vinculados con políticas y controles de acceso muestran mejoras sustantivas:

- Políticas documentadas. Cumplimiento alto (A menudo + Siempre) de 16,7% -> 77,8%; media 2,28 -> 4,17 (Tabla 1 / Figura 1).
- Revisión periódica. A menudo + Siempre de 22,2% -> 72,2%; media 2,44 -> 4,06 (Tabla 2 / Figura 2).
- Controles de acceso a información crítica. A menudo + Siempre de 16,7% -> 77,8%; media 2,33 -> 4,22 (Tabla 7 / Figura 7).

Estas mejoras consistentes en políticas y controles, plenamente alineadas con 27001/27002, se inscriben en el aumento significativo del puntaje global demostrado por la t pareada del apartado anterior ($p<0,001$).

Decisión. La evidencia justifica aceptar H2: el diseño del modelo contribuyó a establecer políticas, controles y procedimientos efectivos para proteger información crítica, reflejándose en el desplazamiento hacia categorías altas y en el incremento de medias.

- **H3. Implementación del modelo y adopción de buenas prácticas**

Hipótesis específica (H3). Implementar un modelo de gestión en seguridad digital asegurará la adopción de buenas prácticas en ciberseguridad, mejorando la resiliencia de la empresa ante amenazas cibernéticas y garantizando el cumplimiento de estándares internacionales.

Hipótesis nula (H0). Implementar un modelo de gestión en seguridad digital no asegurará la adopción de buenas prácticas en ciberseguridad, mejorando la resiliencia de la empresa ante amenazas cibernéticas y garantizando el cumplimiento de estándares internacionales.

Evidencia empírica. Indicadores operativos de gestión de incidentes y concienciación/capacitación muestran incrementos marcados:

- Protocolo formal de incidentes. A menudo + Siempre de 16,7% -> 72,2%; media 2,28 -> 4,00 (Tabla 13 / Figura 13).
- Documentación y análisis de incidentes. A menudo + Siempre de 16,7% -> 72,2%; media 2,39 -> 4,06 (Tabla 14 / Figura 14).
- Pruebas/simulacros de respuesta. A menudo + Siempre de 16,7% -> 77,8%; media 2,33 -> 4,11 (Tabla 15 / Figura 15).
- Simulaciones y campañas de concienciación. A menudo + Siempre sube fuertemente; medias 2,39 -> 4,11 y 2,39 -> 4,06 respectivamente (Tablas 11–12 / Figuras 11–12).

Estos cambios confirman adopción de buenas prácticas (protocolos, simulacros, capacitación) y mayor resiliencia, coherentes con un alineamiento a estándares internacionales; además, se sostienen dentro de un mejoramiento global significativo del puntaje total ($p<0,001$).

Decisión. Con base en la evidencia, se acepta H3: la implementación del modelo aseguró la adopción de buenas prácticas en ciberseguridad, fortaleciendo la resiliencia y el cumplimiento.

- **Síntesis de contrastación**

Con α=0,05, la evidencia empírica permite rechazar H0 y aceptar la hipótesis general (Hg). En las hipótesis específicas, se aceptan H1, H2 y H3 por la consistencia de los cambios pre/post en los ítems críticos (políticas, controles, incidentes, capacitación), el desplazamiento hacia categorías altas (A menudo/Siempre) y el aumento de medias reportado en las Tablas/Figuras correspondientes, en concordancia con el incremento significativo del puntaje global observado en la t de muestras relacionadas.

4.3. IMPLEMENTACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL GRUPO CEDIAMEDICAL

Este apartado describe, de manera detallada, el proceso de implementación del Modelo de Gestión de Seguridad de la Información en el Grupo Cediamedical, siguiendo las directrices de las normas ISO/IEC 27001 e ISO/IEC 27002. La implementación se estructuró en seis fases que siguen el ciclo de mejora continua PHVA (Planificar–Hacer–Verificar–Actuar). En cada fase se explica el propósito, las actividades realizadas, las configuraciones y procedimientos aplicados, los documentos generados como evidencia y el vínculo directo con los objetivos específicos de la investigación. Se encontrará referencias explícitas a los documentos oficiales elaborados en el proyecto (por ejemplo, Documento 1 – Informe de Diagnóstico de Seguridad de la Información, estos documentos están detallados en el Anexo 4) y a los anexos del instrumento (Anexo 3 – Cuestionario de Evaluación del Nivel de Seguridad de la Información).

Fase 1 – Diagnóstico inicial

- **Propósito de la fase**

Identificar las brechas y vulnerabilidades existentes en la gestión de la seguridad de la información del Grupo Cediamedical frente a los requisitos de ISO/IEC 27001 e ISO/IEC 27002. El diagnóstico se consolidó en el Documento 1 – Informe de Diagnóstico de Seguridad de la Información.

- **Metodología aplicada**

Se empleó una metodología mixta que combinó: (i) revisión documental de políticas, manuales y registros disponibles; (ii) observación directa de salas y estaciones de trabajo; (iii) aplicación del Cuestionario de Evaluación del Nivel de Seguridad de la Información (Anexo 3) a 18 colaboradores de áreas críticas; y (iv) pruebas controladas sobre la configuración de accesos y contraseñas en sistemas internos. Los resultados y evidencias se incorporaron íntegramente en el Documento 1.

- **Principales hallazgos**

El análisis reveló brechas en cuatro frentes: (a) políticas y comunicación, (b) controles de acceso, (c) gestión de incidentes, y (d) respaldo y continuidad. En síntesis: solamente el 28% del personal manifestó conocer políticas documentadas; el 38% usaba contraseñas seguras; el 22% conocía un protocolo formal de incidentes; y el respaldo de información crítica se ejecutaba de manera irregular. Estas cifras constituyeron la línea base del proyecto.

- **Indicadores iniciales**

Tabla 21

Indicadores iniciales

Indicador	Situación inicial	Fuente/Evidencia
Conocimiento de políticas de seguridad	28%	Documento 1; Anexo 3
Uso de contraseñas seguras	38%	Documento 1; Anexo 3
Conocimiento de protocolo de incidentes	22%	Documento 1; Anexo 3
Respaldo periódico de información crítica	Irregular (bajo)	Documento 1; registros internos

- **4.2.5 Vinculación con el objetivo específico**

La Fase 1 cumple el Objetivo Específico 1: Diagnosticar el nivel actual de seguridad de la información en el Grupo Cediamedical, en base a ISO/IEC 27001 e ISO/IEC 27002.

- **Comparativo antes vs. después (indicadores clave)**

Al cierre del proyecto, la mejora en los indicadores asociados a esta fase fue la siguiente (los valores finales provienen del Documento 7 – Informe Final de Evaluación de Objetivos):

Tabla 22

Indicadores claves

Indicador	Antes	Después	Mejora
Conocimiento de políticas de seguridad	28%	94%	+66 puntos
Uso de contraseñas seguras	38%	94%	+56 puntos
Conocimiento y aplicación de protocolo de incidentes	22%	88%	+66 puntos

Fase 2 – Diseño del modelo y Plan de Implementación

- **Propósito y justificación del marco**

Diseñar un modelo de gestión en seguridad digital alineado a ISO/IEC 27001 e ISO/IEC 27002, adecuado a la realidad de Cediamedical. La elección de estas normas se basó en su adopción amplia y en su enfoque integral sobre confidencialidad, integridad y disponibilidad, así como en su compatibilidad con procesos de mejora continua y auditoría interna. Esta fase se respalda en el Documento 2 – Plan de Implementación del MGSI y en el Documento 3 – Política de Seguridad de la Información.

- **Insumos del diseño**

Se partió del diagnóstico (Documento 1) y del instrumento aplicado (Anexo 3) para definir prioridades. Los hallazgos orientaron la selección de controles y establecieron metas realistas de mejora. La alta dirección emitió la Política de Seguridad (Documento 3), que actuó como marco para todo el diseño.

- **Estructura del MGSI propuesto**

El modelo se organizó en componentes: (a) gobierno y política, (b) gestión de riesgos, (c) controles técnicos y administrativos, (d) capacitación y concienciación, y (e) medición y mejora continua. El Documento 2 – Plan de Implementación del MGSI definió actividades, responsables y plazos, priorizando la rápida corrección de brechas críticas detectadas en la Fase 1.

- **Responsables y cronograma (según Documento 2)**

Tabla 23

Responsables y cronograma

Actividad	Responsable	Recursos	Plazo	Evidencia
Definir alcance del MGSI	Comité MGSI	Reuniones; formatos	Semana 1	Documento 2 – Alcance aprobado
Elaborar política de seguridad	Gerencia / Comité MGSI	ISO 27001	Semana 2	Documento 3 – Política firmada
Evaluar y tratar riesgos	Coordinador de Seguridad	Matriz; cuestionario	Semanas 3–4	Documento 1 – Informe de

				riesgos
Diseñar SoA y plan de tratamiento	Comité MGSI	Plantilla SoA	Semana 5	Documento 4 – SoA aprobado
Implementar controles técnicos	Área TI	Configuraciones	Semanas 6–8	Registros de cambios
Capacitar al personal	RRHH / Seguridad	Material; listas	Semanas 6–9	Documento 5 – Actas
Simulacro de incidentes	Seguridad	Protocolos	Semana 10	Registro de simulacro
Auditoría interna	Auditor designado	Checklists	Semana 11	Informe de auditoría
Evaluación final y ajustes	Comité MGSI	Resultados; KPIs	Semana 12	Documento 7 – Informe final

- **Vinculación con objetivos específicos**

La Fase 2 responde al Objetivo Específico 2: Diseñar el modelo de gestión en seguridad digital para Cediamedical. Los entregables principales fueron el Documento 2 – Plan de Implementación, el Documento 3 – Política de Seguridad y el Documento 4 – Statement of Applicability (SoA).

- **Comparativo antes vs. después (proyección del diseño)**

A partir del diseño, se proyectaron metas de cumplimiento que posteriormente fueron verificadas en la Fase 5: conocimiento de políticas ≥90%, uso de contraseñas seguras ≥90% y adopción de protocolo de incidentes ≥80%. Estas metas se plasmaron en el Documento 2 y se lograron al cierre del proyecto (ver Documento 7).

Fase 3 – Ejecución técnica y configuraciones

- **Propósito de la fase**

Implementar los controles técnicos y administrativos definidos en el diseño, con énfasis en contraseñas, gestión de accesos, respaldo de información y gestión de incidentes.

- **Controles aplicados (según Documento 4 – SoA)**

Los controles priorizados fueron: 5.1 Políticas de seguridad; 8.9 Gestión de contraseñas; 5.18 Gestión de incidentes; y 5.30 Copias de

respaldo. Estos controles se justifican en el SoA (Documento 4) y apuntan directamente a cerrar las brechas detectadas en la Fase 1.

- **Configuraciones y procedimientos implementados**

a) Políticas de contraseñas: Se estableció longitud mínima de 12 caracteres y la combinación de mayúsculas, minúsculas, números y símbolos. Se forzó el cambio periódico y se prohibió la reutilización de un historial de contraseñas.
b) Gestión de accesos: Se revisaron permisos por rol bajo el principio de mínimo privilegio, eliminando cuentas inactivas y consolidando procedimientos de alta, modificación y baja.
c) Respaldo y restauración: Se formalizó una política de copias de respaldo periódicas, con pruebas de restauración en entornos controlados para garantizar la disponibilidad.
d) Gestión de incidentes: Se habilitó un canal de reporte, un formulario estándar y un flujo de respuesta que incluye clasificación, contención, erradicación y lecciones aprendidas. El procedimiento quedó consolidado en el Registro de Incidente y Respuesta (Documento 6 si aplica) y en registros operativos.

- **Evidencia generada y trazabilidad**

Cada cambio de configuración se documentó con fecha, responsable y evidencia (capturas, registros y actas). Estas evidencias se encuentran asociadas al SoA (Documento 4) y al Plan de Implementación (Documento 2).

- **Vinculación con objetivos específicos**

La Fase 3 cumple el Objetivo Específico 3: Implementar el modelo de gestión en seguridad digital diseñado para Cediamedical.

- **Comparativo antes vs. después (control de accesos y respaldo)**

La adopción de contraseñas robustas y la formalización del respaldo periódico contribuyeron al cumplimiento de las metas fijadas en la Fase 2.

Los porcentajes finales verificados en la Fase 5 se recogen en el Documento 7.

Fase 4 – Capacitación y concienciación del personal

- **Propósito de la fase**

Sensibilizar y entrenar al personal en buenas prácticas de seguridad, políticas internas y respuesta a incidentes, asegurando la adopción sostenida de los controles implementados.

- **Diseño de la capacitación y contenidos**

Se elaboró un plan de capacitación con sesiones presenciales y virtuales, materiales de apoyo, evaluaciones de salida y registro de asistentes. El detalle se encuentra en el Acta de Capacitación (Documento 5). Los contenidos abordaron políticas internas, contraseñas robustas, phishing y gestión de incidentes.

- **Participación y evaluación**

Participaron 18 colaboradores de áreas críticas. Las evaluaciones de salida mostraron mejoras notorias en comprensión y aplicación de políticas internas y buenas prácticas.

- **Vinculación con objetivos específicos**

La Fase 4 se alinea con el Objetivo Específico 3 (implementación del modelo) y es soporte para el Objetivo Específico 4 (evaluación de efectividad).

- **Comparativo antes vs. después (concienciación)**

La concienciación en políticas, contraseñas y respuesta a incidentes mejoró significativamente tras la capacitación. Estos avances se reflejan en los porcentajes finales reporteados en el Documento 7.

Fase 5 – Validación, auditoría interna y mejoras

- **Propósito de la fase**

Verificar la efectividad del MGSI implementado mediante una evaluación posterior (postintervención) y una auditoría interna focalizada en los controles priorizados.

- **Evaluación de resultados (Documento 7)**

Se repitió el instrumento del Anexo 3 y se consolidaron los resultados en el Documento 7 – Informe Final de Evaluación de Objetivos. Los indicadores de resultado alcanzados fueron: conocimiento de políticas 94%; uso de contraseñas seguras 94%; y conocimiento y aplicación del protocolo de incidentes 88%.

- **Auditoría interna**

Se ejecutó una auditoría interna con listas de verificación alineadas a ISO/IEC 27001, concentrándose en política, control de accesos, respaldo y gestión de incidentes. Se registraron hallazgos menores (por ejemplo, necesidad de reforzar la revisión de permisos cada trimestre), que derivaron en acciones correctivas incluidas en el plan de mejora.

- **Vinculación con objetivos específicos**

La Fase 5 cumple el Objetivo Específico 4: Evaluar la efectividad del modelo implementado.

- **Comparativo antes vs. después (resultados consolidados)**

Tabla 24

Comparativo antes vs después

Indicador	Antes	Después	Mejora
Conocimiento de políticas de seguridad	28%	94%	+66 puntos
Uso de contraseñas seguras	38%	94%	+56 puntos
Conocimiento y aplicación de protocolo de incidentes	22%	88%	+66 puntos

Fase 6 – Seguimiento y mantenimiento del MGSI

- **Propósito de la fase**

Establecer prácticas de seguimiento, medición y mejora continua que aseguren la sostenibilidad del MGSI en el tiempo.

- **Acciones de seguimiento (Documento 8 – Plan de Implementación y Mejora Continua)**

Se definieron auditorías internas semestrales, actualizaciones anuales de la matriz de riesgos, refuerzo de capacitaciones y un módulo de autoevaluación en la intranet. Estas acciones se documentaron en el Documento 8 – Plan de Implementación del MGSI.

- **Indicadores de control y responsables**

Los indicadores clave incluyen: porcentaje de cumplimiento de políticas, porcentaje de contraseñas robustas, cumplimiento de respaldo, tiempos de respuesta a incidentes y porcentaje de acciones correctivas cerradas. El Comité MGSI monitorea y reporta estos indicadores a la alta dirección.

- **Vinculación con objetivos específicos**

La Fase 6 cumple el Objetivo Específico 5: Establecer un plan de mejora continua que asegure la sostenibilidad del MGSI.

Resumen global de resultados y objetivos cumplidos

La implementación del MGSI en Cediamedical cumplió el objetivo general del proyecto y los objetivos específicos definidos. A continuación, se presenta un resumen de los principales indicadores antes y después de la intervención, así como la relación con los documentos de evidencia generados durante el proyecto.

Tabla 25

Resumen global

Indicador	Antes	Después	Mejora	Documento de evidencia	Objetivo vinculado
Conocimiento de políticas de seguridad	28%	94%	+66 pts	Doc. 1; Doc. 7	OE1, OE4
Uso de contraseñas seguras	38%	94%	+56 pts	Doc. 1; Doc. 7	OE1, OE3, OE4
Protocolo de incidentes (conocido y aplicado)	22%	88%	+66 pts	Doc. 1; Doc. 7	OE1, OE3, OE4

Además de los indicadores cuantitativos, se observaron mejoras cualitativas: formalización de la política de seguridad (Documento 3), definición del alcance del MGSI y responsabilidades (Documento 2), trazabilidad de controles y justificaciones (Documento 4 – SoA), y fortalecimiento de la cultura de seguridad a través de la capacitación (Documento 5).

CAPÍTULO V

DISCUSIÓN DE RESULTADOS

5.1. CONTRASTACIÓN DE LOS RESULTADOS DEL TRABAJO DE INVESTIGACIÓN

Los resultados obtenidos en Cediamedical (incrementos marcados en el cumplimiento de políticas de seguridad, controles de acceso, gestión de incidentes y prácticas de concienciación, y una mejora significativa del puntaje global del instrumento) se alinean con el consenso de la literatura de gestión de seguridad de la información basada en ISO/IEC 27001 e ISO/IEC 27002, pero aportan evidencia en un contexto poco documentado: una entidad del sector salud de tamaño pequeño, con 18 colaboradores y recursos limitados. En nuestro estudio, el promedio global aumentó del pretest al postest de 5,92 a 10,83 con una diferencia estadísticamente significativa (t pareada, p<0,001), y se observaron saltos en indicadores operativos (por ejemplo, conocimiento de políticas del 28% al 94%, uso de contraseñas robustas del 38% al 94%, y manejo del protocolo de incidentes del 22% al 88%), respaldados por evidencia documental.

- **Comparación con antecedentes internacionales.**

Gómez (2021) muestra que implantar un SGSI conforme a ISO/IEC 27001 en instituciones financieras optimiza la protección de datos críticos y fortalece la confidencialidad, integridad y disponibilidad de la información; no obstante, su foco fueron organizaciones grandes con amplios recursos, dejando abierta la pregunta sobre la escalabilidad del modelo a entidades más pequeñas. Nuestros hallazgos confirman la transferibilidad de los beneficios de 27001/27002 a un entorno pequeño del sector salud (con políticas formalizadas, controles de acceso efectivos y respuesta a incidentes) y demuestran que, con una implementación gradual y priorizada, se logran mejoras medibles aun con restricción de recursos.

Smith (2020) reporta que hospitales sin SGSI presentan alta vulnerabilidad y que la adopción de 27001 disminuye incidentes; sin embargo, la literatura enfatiza realidades hospitalarias con mayor infraestructura. En Cediamedical, una organización más pequeña que un hospital, se obtuvieron resultados convergentes: al formalizar políticas, fortalecer contraseñas y estandarizar la gestión de incidentes, se observó una reducción de exposición al riesgo y una mejora de prácticas del personal, tal como plantea Smith, pero ahora validado en un nivel de complejidad menor y con plantillas y capacitaciones adaptadas al rol.

Chen (2020) evidencia que las PYME tecnológicas mejoran su postura de seguridad al adoptar 27001, aunque no aborda el sector salud. Nuestro estudio extiende esa evidencia al demostrar que, en un prestador de salud pequeño, los controles organizacionales (política, control de accesos, registro y análisis de incidentes) y las prácticas de formación logran saltos de desempeño similares, siempre que se priorice un paquete mínimo viable de controles y se asegure la trazabilidad (documentación de cada control y su evidencia).

- **Comparación con antecedentes nacionales.**

Rojas (2022) valida la utilidad de 27001 en el ámbito universitario peruano; Fernández (2021) muestra mejoras al implantar controles 27002 en entidades gubernamentales; y García (2020) señala que incluso empresas financieras con controles básicos requieren SGSI estructurados. En conjunto, estos antecedentes respaldan que 27001/27002 elevan el nivel de madurez; nuestra contribución es demostrar cómo esa madurez se puede alcanzar en una empresa pequeña de salud, con capacitaciones cortas, concienciación periódica, y auditoría ligera de controles (checklists y evidencias), reproduciendo tendencias de mejora observadas en universidades y gobierno, pero con gobernanza simplificada y medios de verificación proporcionales a la escala.

- **Comparación con antecedentes locales.**

Martínez (2023) identifica vulnerabilidades críticas en clínicas de Huánuco y propone 27001, pero no incluye un plan detallado de formación. Nuestra intervención cierra ese vacío: articulamos capacitaciones periódicas y campañas de concienciación, elementos que (en Cediamedical) explican parte del desplazamiento hacia A menudo/Siempre en los ítems de prácticas del personal. Además, tomamos como referente el énfasis local en gestión de credenciales señalado por López (2022) en instituciones educativas y lo trasladamos al sector salud con revisiones de permisos, robustecimiento de contraseñas, y bloqueos por intentos fallidos, medidas que se asociaron a los incrementos observados en nuestros resultados.

- **Tendencias y aportes diferenciales.**

En concordancia con la literatura, la formalización de políticas (27001) y la implantación de controles (27002) correlacionan con mejoras operativas. Nuestro aporte se centra en tres ejes: (1) Escalabilidad: demostramos que un paquete mínimo viable de controles (políticas, gestión de accesos, respaldo, respuesta a incidentes, capacitación) produce mejoras significativas sin requerir grandes inversiones; (2) Trazabilidad: se registró la evidencia documental (política, alcance, SoA, plan de tratamiento, actas, registros de incidentes), conectando cada control con indicadores del instrumento (de allí los incrementos en categorías altas y en las medias observadas); y (3) Contextualización sectorial: alineamos prácticas a la sensibilidad de datos clínicos y a los flujos reales de trabajo de Cediamedical, algo poco presente en estudios de gran escala.

Mientras que los antecedentes financieros y gubernamentales suelen partir de estructuras con equipos de seguridad dedicados y herramientas avanzadas, Cediamedical partía de un escenario con escasa formalización, contraseñas débiles y protocolos incipientes. En ese marco, la mejora que observamos es más abrupta en algunos indicadores (por ejemplo, políticas y contraseñas) por el efecto piso: la línea base era baja y, al introducir controles mínimos y formación, se genera un salto notorio. Esta diferencia de

punto de partida explica el tamaño del cambio sin contradecir la literatura; por el contrario, refuerza la recomendación de priorizar controles de alto impacto y bajo costo en organizaciones pequeñas antes de sofisticar el SGSI.

- **Implicancias.**

Los hallazgos de Cediamedical sugieren que la adopción escalonada de 27001/27002, con fuerte énfasis en personas (concienciación y capacitación) y controles organizacionales básicos (política, accesos, incidentes), es suficiente para producir mejoras medibles en entidades de salud pequeñas. Esto operacionaliza recomendaciones generales de la literatura (por ejemplo, evaluación de riesgos y priorización de controles) en procedimientos concretos: revisiones trimestrales de políticas, campañas de contraseñas, simulacros de incidentes con registro y lecciones aprendidas, y verificación periódica de permisos. Así, la contribución práctica es un camino de adopción realista, compatible con las restricciones observadas en el entorno local.

- **Alcance y límites.**

Tal como advierte la literatura al pasar de grandes organizaciones a PYMEs, la validez externa es un reto. Nuestros resultados se circunscriben a la población censal de 18 colaboradores; la mejora es consistente con antecedentes, pero la extrapolación a otras realidades debe hacerse con cautela y replicar el diseño en muestras mayores o en clínicas de distinta complejidad. Esta precisión no contradice los hallazgos, sino que ubica su alcance en la escala y madurez de Cediamedical, alineándose con las brechas metodológicas señaladas en estudios previos.

Para garantizar la trazabilidad entre los cambios observados en los puntajes pretest–postest y la implementación técnica del modelo, se documentaron resultados operativos obtenidos con Open-AudIT/GLPI y la cuantificación económica FAIR/RiskLens. En un entorno organizacional pequeño (18 colaboradores), el inventario técnico consolidado registró 24 equipos de usuario, 2 servidores on-premise, 1 NAS y la electrónica de red

básica; se corrigieron 3 inconsistencias de registro y el parcheo efectivo alcanzó 85 % al cierre del postest. Estas acciones se corresponden con la mejora en las dimensiones del instrumento vinculadas con gestión de activos y control de accesos. En paralelo, el modelado FAIR estimó una pérdida anual esperada (ALE) ante un evento de ransomware de ≈ USD 6 000 (P50) y ≈ USD 22 000 (P95), lo que justificó la priorización de controles de alto impacto y bajo costo adecuados al tamaño de la empresa: autenticación multifactor (MFA), copias de seguridad verificadas y segmentación básica. Es importante precisar que los contrastes estadísticos reportados (prueba t pareada/Wilcoxon en SPSS v25) provienen exclusivamente de los puntajes del instrumento aplicado a la población censal (n = 18); los resultados de Open-AudIT/GLPI y FAIR/RiskLens se integran como evidencia operativa y económica complementaria que explica cómo se materializó la intervención y por qué se priorizaron determinados controles.

CONCLUSIONES

1. El diagnóstico del estado de la seguridad digital identifica vulnerabilidades y brechas concretas en Cediamedical, especialmente en políticas documentadas, revisión de políticas, controles de acceso, protocolos de incidentes y capacitación. Esta identificación se refleja en la alta concentración pretest de respuestas en Nunca/Rara vez y en los bajos promedios de esas dimensiones, evidenciando una línea base deficitaria sobre la cual se planificó la intervención.

2. El diseño del modelo de gestión basado en ISO/IEC 27001 e ISO/IEC 27002 contribuye a establecer políticas, controles y procedimientos efectivos para proteger la información crítica, lo cual se constata en el desplazamiento postest hacia categorías A menudo/Siempre y en el incremento de medias en indicadores de gobernanza y control de accesos. La alineación explícita de los controles con las cláusulas/controles de la norma facilitó su adopción operativa.

3. La implementación del modelo asegura la adopción de buenas prácticas de ciberseguridad (formalización de políticas, gestión de accesos, gestión de incidentes, capacitación), mejorando la resiliencia del grupo y el cumplimiento con estándares internacionales. Esto se evidencia en el aumento significativo del puntaje global entre pretest y postest y en los incrementos de cumplimiento alto (suma de A menudo/Siempre) en ítems críticos de incidentes y concienciación.

4. La secuencia: diagnóstico -> diseño -> implementación es efectiva en una organización pequeña como Cediamedical (n = 18). Partiendo de brechas claras (efecto piso), el modelo prioriza controles de alto impacto y bajo costo, logrando mejoras medibles en corto plazo sin requerir infraestructura compleja

RECOMENDACIONES

1. Aprobar la Política de Seguridad de la Información y establecer un calendario de revisión cada tres meses. Centralizar todo en un repositorio único: Política, Declaración de Aplicabilidad, Plan de Tratamiento de Riesgos, actas e informes. Responsable: Comité del Sistema de Gestión de Seguridad de la Información (área de tecnología y gerencia). Meta de control: al menos 90 % de políticas revisadas dentro de los 90 días; 100 % de evidencias críticas guardadas en el repositorio; 100 % del personal informado por escrito. Pruebas de cumplimiento: actas firmadas, documentos con control de versiones y registro de comunicaciones.

2. Activar doble verificación al iniciar sesión en todas las cuentas críticas (correo, sistema clínico, finanzas). Aplicar una política de contraseñas con longitud mínima de 12 caracteres, mezcla de letras, números y símbolos, y cambio cada seis meses; bloqueo automático tras cinco intentos fallidos y cierre de sesión por inactividad entre 10 y 15 minutos. Asegurar cifrado y antivirus con prevención de fugas de información en todas las computadoras y dispositivos móviles. Responsable: área de tecnología. Metas de control: 100 % de cuentas críticas con doble verificación; al menos 95 % del personal cumpliendo la política de contraseñas; 100 % de equipos con cifrado y agente de seguridad funcionando. Pruebas de cumplimiento: reportes del sistema de usuarios, capturas de configuración y listado actualizado de equipos protegidos.

3. Mantener un inventario maestro de activos (propietario, criticidad, nivel de actualización y garantía), con actualización mensual. Ejecutar un plan de actualización mensual priorizando los equipos y sistemas más críticos. Implementar copias de seguridad con el esquema tres–dos–uno (tres copias, en dos tipos de medios, una fuera de la sede), retención mínima de 30 días y prueba de restauración cada trimestre. Responsable: área de tecnología. Metas de control: 100 % de activos críticos registrados en el inventario; al menos 90 % de activos críticos

actualizados cada mes; 100 % de activos críticos con copia de seguridad; 100 % de pruebas de restauración con resultado exitoso. Pruebas de cumplimiento: exportación del inventario, informes de actualización, registros del sistema de copias y actas de restauración.

4. Poner en marcha el procedimiento de gestión de incidentes con un único canal de reporte (correo o formulario), clasificación por severidad, tiempos máximos de atención definidos, análisis posterior obligatorio con acciones correctivas y un simulacro cada trimestre (por ejemplo, intento de fraude por correo o pérdida de un equipo). Responsables: responsable de seguridad y área de tecnología. Metas de control: tiempo promedio de detección menor a un día, tiempo promedio de recuperación menor a tres días, 100 % de incidentes con análisis posterior documentado y un simulacro por trimestre. Pruebas de cumplimiento: registros o tickets de incidentes, informes de simulacros y planes de acción cerrados con evidencia.

5. Mantener capacitaciones breves cada dos meses (15–20 minutos) y simulaciones trimestrales de correos de fraude con retroalimentación individual. Realizar revisión trimestral de indicadores (políticas, accesos, incidentes, copias de seguridad, actualizaciones y formación) y una auditoría interna ligera cada seis meses basada en la norma. Responsables: recursos humanos y área de tecnología para la formación; Comité del Sistema de Gestión de Seguridad de la Información para el seguimiento. Metas de control: al menos 85 % de asistencia a las sesiones, menos del 5 % de clics en las simulaciones de fraude y al menos 90 % de acciones correctivas cerradas en un máximo de 60 días. Pruebas de cumplimiento: actas y materiales de formación, resultados de simulaciones y cuestionarios, tablero de indicadores e informes de auditoría.

REFERENCIAS BIBLIOGRÁFICAS

Alhasib, A. (2020). Security and privacy in health information systems: Challenges and solutions. Springer.

América Sistemas. (2023). Informe sobre ciberseguridad en América Latina. Recuperado 27 de febrero de 2025, de https://www.americasistemas.com/informe-ciberseguridad-latam

Andress, J. (2019). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice (3.ª ed.). Syngress.

Ávila, R. (2001). Metodología de la investigación: Cómo elaborar la tesis y/o investigación. Estudios y Ediciones R.A.

Calder, A., & Watkins, S. (2019). Information Security Management Principles. IT Governance Publishing.

Centro Criptológico Nacional. (2022). CCN-STIC 825: Guía del Esquema Nacional de Seguridad basada en la ISO/IEC 27001. Recuperado 27 de febrero de 2025, de https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.html

Check Point Research. (2023). Global Cyber Security Report: Healthcare Under Attack. Check Point Research.

Check Point Software Technologies. (2023). Cyber attack trends: 2023 report. Recuperado 27 de febrero de 2025, de https://www.checkpoint.com/downloads/cyber-attack-trends-2023.pdf

Chen, L. (2020). Adopción de la norma ISO/IEC 27001 en pequeñas y medianas empresas: Un estudio de caso en China. International Journal of Information Management, 46, 1–10. https://doi.org/10.1016/j.ijinfomgt.2018.11.014

Cisco. (2019). Annual Cybersecurity Report 2019. Cisco Systems.

European Parliament. (2022). General Data Protection Regulation (GDPR): Data privacy in the EU. Recuperado 27 de febrero de 2025, de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Europol. (2018). Internet Organised Crime Threat Assessment (IOCTA). Europol.

Europol. (2021). Ransomware as a Service: A Growing Threat. Europol.

Fernández, L. (2021). Implementación de controles de seguridad de la información según ISO/IEC 27002 en una entidad gubernamental peruana. Revista Peruana de Informática y Sistemas, 4(1), 25–35. https://doi.org/10.33539/infosys.2021.v4n1.25-35

Fiallo, J., Cerezal, J., & Hedesa, Y. (2008). La investigación pedagógica: Una vía para elevar la calidad educativa. Taller Gráficos SanRemo.

Foro Económico Mundial. (2023). Global cybersecurity outlook 2023. Recuperado 27 de febrero de 2025, de https://www.weforum.org/reports/global-cybersecurity-outlook-2023

Gallardo, E. E. (2017). Metodología de la investigación: Manual autoformativo interactivo. Universidad Continental. Recuperado 27 de febrero de 2025, de https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

García, J. (2020). Evaluación de la madurez en seguridad de la información en empresas del sector financiero peruano aplicando ISO/IEC 27001 [Tesis de licenciatura, Pontificia Universidad Católica del Perú]. Repositorio Institucional PUCP.

Garcia, R., Torres, P., & Hernandez, M. (2019). Information Security Management Systems and Their Impact on Corporate Security Policies. Cybersecurity Journal, 12(3), 45–67.

Garrett, P. (2021). Zero Trust Security: Defending Your Organization from Cyber Threats. Wiley.

GlobalSuite Solutions. (s. f.). ¿Qué es la norma ISO 27001 y para qué sirve? Recuperado 27 de febrero de 2025, de https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

Gómez, P. (2021). Implementación de un Sistema de Gestión de Seguridad de la Información en una entidad financiera según la norma ISO/IEC 27001:2013 [Tesis de maestría, Universidad de Buenos Aires]. Repositorio Institucional de la Universidad de Buenos Aires.

González, M. (2021). Eficacia de los estándares internacionales en la protección de la información. Revista de Ciberseguridad y Gestión de Riesgos, 12(2), 45–59.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2022). The economics of information security in healthcare organizations. MIS Quarterly.

Hernandez, J., & Torres, L. (2021). Cybersecurity best practices: A guide to ISO/IEC 27002 implementation. Security & Compliance, 18(2), 102–125.

Hernández, R., Fernández, C., & Baptista, M. (2017). Metodología de la investigación. Recuperado 27 de febrero de 2025, de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Hernández Sampieri, R., Mendoza, C., & Fernández, C. (2022). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta (7.ª ed.). McGraw-Hill.

HHS (Department of Health and Human Services). (2021). Ransomware attacks in healthcare: Risks and countermeasures. U.S. Department of Health and Human Services.

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM. Recuperado 27 de febrero de 2025, de https://www.ibm.com/security/data-breach

ICEX. (2023). Ciberseguridad en Perú: Tendencias y desafíos. Recuperado 27 de febrero de 2025, de https://www.icex.es/ciberseguridad-peru

Infobae. (2024). Perú registra cifra récord en intentos de phishing en 2024. Recuperado 27 de febrero de 2025, de https://www.infobae.com/america/peru/2024/01/15/peru-registra-cifra-record-intentos-phishing/

International Organization for Standardization. (2013a). ISO/IEC 27001:2013 – Information security management systems – Requirements. ISO.

International Organization for Standardization. (2013b). ISO/IEC 27002:2013 – Code of practice for information security controls. ISO.

ISO (2020). ISO/IEC 27001:2013 Information security management systems – Requirements. International Organization for Standardization.

ISO (International Organization for Standardization). (2022). ISO/IEC 27001:2022 Information security management systems – Requirements. ISO.

López, A. (2022). Análisis de riesgos de seguridad de la información en una institución educativa de Huánuco según la norma ISO/IEC 27005. Revista Científica de la Universidad Nacional Hermilio Valdizán, 5(2), 50–65. https://doi.org/10.33539/rcunhv.2022.v5n2.50-65

Martinez, P. (2022). Risk management in information security: Strategies for a digital world. Technology & Security Review, 14(1), 78–92.

Martínez, S. (2023). Propuesta de un sistema de gestión de seguridad de la información para una clínica privada en Huánuco basado en ISO/IEC 27001 [Tesis de maestría, Universidad de Huánuco]. Repositorio Institucional de la Universidad de Huánuco.

McKinsey & Company. (2023). Digital transformation in healthcare: A path to efficiency and security. Recuperado 27 de febrero de 2025, de https://www.mckinsey.com/industries/healthcare/our-insights/digital-transformation-in-healthcare

National Institute of Standards and Technology. (2021). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). U.S. Department of Commerce.

OCR (Office for Civil Rights). (2021). HIPAA enforcement actions and violations report. U.S. Department of Health and Human Services.

Otzen, T., & Manterola, C. (2017). Técnicas de muestreo sobre una población a estudio. International Journal of Morphology, 35(1), 227–232. https://doi.org/10.4067/S0717-95022017000100037

Peltier, T. R. (2016). Information security policies, procedures, and standards: Guidelines for effective information security management. Auerbach Publications.

Pirani. (s. f.). Riesgos de seguridad de la información en el sector salud. Recuperado 27 de febrero de 2025, de https://www.piranirisk.com/es/blog/gestion-riesgos-seguridad-informacion-sector-salud

Ponemon Institute. (2021). Cost of a Data Breach Report. IBM Security.

Ponemon Institute. (2022). Privacy and security in healthcare: The patient perspective. Recuperado 27 de febrero de 2025, de https://www.ponemon.org/privacy-security-healthcare

Prey Project. (2023). Global cybersecurity report: Threat trends and predictions. Recuperado 27 de febrero de 2025, de https://www.preyproject.com/global-cybersecurity-report-2023

Reddy, S., & Sharma, B. (2021). Cybersecurity in healthcare: Strategies for protection. Wiley.

Roberts, C. (2020). Human factors in cybersecurity: Reducing employee-related risks. Cyber Risk Studies, 9(4), 56–73.

Rojas, M. (2022). Diseño de un sistema de gestión de seguridad de la información basado en ISO/IEC 27001 para una universidad pública en Lima [Tesis de maestría, Universidad Nacional Mayor de San Marcos]. Repositorio Institucional Cybertesis UNMSM.

Sánchez y Reyes. (2006). Metodología y diseños en investigación científica. Visión Universitaria.

Sampieri, R. H., Collado, C. F., & Lucio, M. d. P. B. (2010). Metodología de la investigación (5.ª ed.). McGraw Hill.

Smith, J. (2020). Evaluación de riesgos en seguridad de la información en hospitales utilizando ISO/IEC 27001. Journal of Information Security, 9(2), 45–58. https://doi.org/10.4236/jis.2020.92004

Stakeholders. (2023). Riesgos de ciberseguridad en el sector salud en Perú. Recuperado 27 de febrero de 2025, de https://www.stakeholders.com.pe/riesgos-ciberseguridad-salud-peru

Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4.ª ed.). Pearson.

Stallings, W., Case, T., Lawrie, D., & Palmer, C. (2022). Network Security Essentials: Applications and Standards (6.ª ed.). Pearson.

Universidad Veracruzana. (s. f.). Riesgos de seguridad de la información que afectan al sector salud. Recuperado 27 de febrero de 2025, de https://www.uv.mx/infosegura/general/infografia_riesgos/

Vargas, R. (2021). Implementación de políticas de seguridad de la información en una empresa de telecomunicaciones en Huánuco siguiendo las directrices de ISO/IEC 27002 [Tesis de licenciatura, Universidad Nacional Hermilio Valdizán]. Repositorio Institucional UNHEVAL.

Verizon. (2022). 2022 Data Breach Investigations Report. Verizon Enterprise.

Whitman, M. E., & Mattord, H. J. (2019). Principles of Information Security (6.ª ed.). Cengage Learning.

COMO CITAR ESTE TRABAJO DE INVESTIGACIÓN

Mariano Beraun, H. (2025). *Diseño e implementación de un modelo de gestión en seguridad digital para el Grupo Cediamedical basándose en ISO/IEC 27001, ISO/IEC 27002* [Tesis de pregrado, Universidad de Huánuco]. Repositorio Institucional UDH. http://...

ANEXOS

ANEXO 1

MATRIZ DE CONSISTENCIA

DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN EN SEGURIDAD DIGITAL PARA EL GRUPO CEDIAMEDICAL BASÁNDOSE EN ISO/IEC 27001, ISO/IEC 27002.

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLE	METODOLOGÍA
Problema General ¿De qué manera el diseño e implementación de un modelo de gestión en seguridad digital, basado en las normas ISO/IEC 27001 e ISO/IEC 27002, fortalecerá la protección de la información en el grupo Cediamedical, garantizando su integridad, disponibilidad y confidencialidad, y reduciendo los riesgos asociados a amenazas cibernéticas? **Problemas Específicos** • ¿De qué manera el diagnóstico del estado actual de la seguridad digital en el grupo Cediamedical permitirá identificar vulnerabilidades, amenazas y brechas en la gestión de la información, facilitando la formulación de estrategias	**Objetivo General** Diseñar e implementar un modelo de gestión en seguridad digital para el grupo Cediamedical basado en las normas ISO/IEC 27001 e ISO/IEC 27002, con el propósito de fortalecer la protección de la información, garantizar su integridad, disponibilidad y confidencialidad, y reducir los riesgos asociados a posibles amenazas cibernéticas. **Objetivos Específicos**. Diagnosticar el estado actual de la seguridad digital en el grupo Cediamedical, identificando vulnerabilidades, amenazas y brechas en la gestión de la información. Diseñar un modelo de	**HIPÓTESIS GENERAL** Hg: La implementación de un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 fortalecerá la protección de la información en el grupo Cediamedical, garantizando su integridad, disponibilidad y confidencialidad, y reduciendo los riesgos asociados a amenazas cibernéticas. H0: Diseñar e Implementar un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 no fortalecerá la protección de la información en el grupo Cediamedical, garantizando su integridad, disponibilidad y confidencialidad, y reduciendo los riesgos asociados a amenazas cibernéticas. **HIPÓTESIS ESPECIFICAS** H1: Diagnosticar el estado actual de	**Variables Independientes** Modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 **Variable Dependiente** Protección de la información en el grupo Cediamedical	**Enfoque** enfoque cuantitativo. **Alcance o Nivel** investigación explicativa. **Diseño** Pre experimental de pre test y post test **G O1 X O2** *Dónde:* **G** = Grupo de investigación **X** = Aplicación **O1** = Pre Observación **O2** = Post Observación

de mitigación? • ¿De qué manera el diseño de un modelo de gestión en seguridad digital, basado en las normas ISO/IEC 27001 e ISO/IEC 27002, contribuirá a establecer políticas, controles y procedimientos efectivos para la protección de la información crítica de la empresa? • ¿De qué manera la implementación del modelo de gestión en seguridad digital asegurará la adopción de buenas prácticas en ciberseguridad, mejorando la resiliencia de la empresa ante amenazas cibernéticas y garantizando el cumplimiento de estándares internacionales?	gestión en seguridad digital, estableciendo políticas, controles y procedimientos que permitan mitigar riesgos y proteger la información crítica de la empresa. Implementar el modelo de gestión en seguridad digital en el grupo Cediamedical, asegurando la adopción de buenas prácticas en ciberseguridad y el cumplimiento de estándares internacionales.	la seguridad digital en el grupo Cediamedical permitirá identificar vulnerabilidades, amenazas y brechas en la gestión de la información, facilitando la formulación de estrategias para su mitigación. H0: Diagnosticar el estado actual de la seguridad digital en el grupo Cediamedical no permitirá identificar vulnerabilidades, amenazas y brechas en la gestión de la información, facilitando la formulación de estrategias para su mitigación. H2: Diseñar un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 contribuirá a establecer políticas, controles y procedimientos efectivos para la protección de la información crítica de la empresa. H0: Diseñar un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002 no contribuirá a establecer políticas, controles y procedimientos efectivos para la protección de la información crítica de la empresa H3: Implementar un modelo de gestión en seguridad digital asegurará la adopción de buenas prácticas en ciberseguridad, mejorando la resiliencia de la empresa ante amenazas	

	cibernéticas y garantizando el cumplimiento de estándares internacionales. H0: Implementar un modelo de gestión en seguridad digital no asegurará la adopción de buenas prácticas en ciberseguridad, mejorando la resiliencia de la empresa ante amenazas cibernéticas y garantizando el cumplimiento de estándares internacionales.	

ANEXO 2

DOCUMENTO DE APROBACIÓN DE LA INVESTIGACIÓN

Grupo CEDIAMEDICAL

"Año de la unidad, la paz y el desarrollo"

Huánuco, 27 de Febrero del 2025

SEÑOR(A):
Mariano Beraun, Hugo Romario
BACH EN INGENIERÍA DE SISTEMAS E INFORMÁTICA DE LA UNIVERSIDAD DE HUÁNUCO

DE:
JUAN LANGUASCO ALCEDO
GERENTE GENERAL

ASUNTO:
CARTA DE SOLICITUD PARA PRIMERAS PRÁCTICAS PREPROFESIONALES

De mi consideración:
Por medio de la presente, manifiesto nuestra aceptación y autorización para la realización del proyecto de investigación titulado "DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN EN SEGURIDAD DIGITAL PARA EL GRUPO CEDIAMEDICAL BASÁNDOSE EN ISO/IEC 27001, ISO/IEC 27002".

Dicha investigación tiene como finalidad fortalecer la protección de la información en los sistemas existentes de nuestra organización, asegurando su confidencialidad, integridad y disponibilidad mediante la optimización de procesos y la implementación de controles de seguridad basados en estándares internacionales.

En este sentido, Cediamedical se compromete a brindar el acceso necesario a la información relevante para el desarrollo del estudio, respetando las políticas de confidencialidad y privacidad de la empresa. Asimismo, se facilitará la comunicación con el personal designado para la recopilación de datos y el análisis correspondiente.

Agradecemos el interés en contribuir a la mejora de la seguridad digital de nuestra institución y quedamos atentos a los avances de la investigación.

Atentamente;

M.C. Juan J. Languasco Alcedo
MEDICO - OCUPACIONAL
CMP. 42300

www.cediaocupacional.com
Jr. Dámaso Beraún 877
Huánuco - Perú
Tel.: 062-514339
Cel.: 962080199

ANEXO 3

INSTRUMENTOS

CUESTIONARIO DE ENCUESTA

Título: Cuestionario de Evaluación del Nivel de Seguridad de la Información en el Grupo Cediamedical

Objetivo: Evaluar el estado actual de la seguridad de la información en el grupo Cediamedical, identificando vulnerabilidades, amenazas y brechas en la gestión de la información, con el fin de diseñar e implementar un modelo de gestión en seguridad digital basado en las normas ISO/IEC 27001 e ISO/IEC 27002.

Tipo de Instrumento: Cuestionario estructurado de tipo Likert (1 a 5) complementado con preguntas de selección y respuesta abierta.

Dirigido a: Personal de TI, gerentes, responsables de seguridad de la información y empleados que manejan información crítica en Cediamedical.

SECCIÓN 1: DATOS GENERALES

1. Cargo en la empresa:
    - a) Gerente
    - b) Personal de TI
    - c) Administrativo
    - d) Médico
    - e) Otro: _____
2. Área de trabajo: _____
3. Tiempo de servicio en la empresa:
    - a) Menos de 1 año
    - b) Entre 1 y 3 años
    - c) Más de 3 años

SECCIÓN 2: POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

Indicador: Existencia y aplicación de políticas de seguridad de la información.

Escala de valoración (1-5): 1 = Nunca, 2 = Rara vez, 3 = A veces, 4 = Frecuentemente, 5 = Siempre

Ítem	Pregunta	1	2	3	4	5
P1	¿La empresa cuenta con políticas documentadas sobre seguridad de la información?	☐	☐	☐	☐	☐
P2	¿Las políticas de seguridad son revisadas y actualizadas periódicamente?	☐	☐	☐	☐	☐
P3	¿Se informa al personal sobre las políticas de seguridad de la información?	☐	☐	☐	☐	☐

SECCIÓN 3: GESTIÓN DE RIESGOS

Indicador: Evaluación y mitigación de riesgos en seguridad de la información.

Escala de valoración (1-5): 1 = Nunca, 2 = Rara vez, 3 = A veces, 4 = Frecuentemente, 5 = Siempre

Ítem	Pregunta	1	2	3	4	5
P4	¿Se realizan evaluaciones de riesgos en seguridad de la información en la empresa?	☐	☐	☐	☐	☐
P5	¿Existen procedimientos para mitigar los riesgos identificados?	☐	☐	☐	☐	☐
P6	¿Se llevan a cabo auditorías o revisiones sobre los controles de seguridad de la información?	☐	☐	☐	☐	☐

SECCIÓN 4: CONTROLES DE ACCESO

Indicador: Seguridad en el acceso a la información y sistemas.

Escala de valoración (1-5): 1 = Nunca, 2 = Rara vez, 3 = A veces, 4 = Frecuentemente, 5 = Siempre

Ítem	Pregunta	1	2	3	4	5
P7	¿Se implementan controles de acceso para garantizar que solo personal autorizado acceda a información crítica?	☐	☐	☐	☐	☐
P8	¿Se utilizan contraseñas seguras en los sistemas de la empresa?	☐	☐	☐	☐	☐
P9	¿Se revisan y actualizan periódicamente los permisos de acceso a la información?	☐	☐	☐	☐	☐

SECCIÓN 5: CAPACITACIÓN Y CONCIENCIACIÓN EN SEGURIDAD DIGITAL

Indicador: Nivel de formación y sensibilización del personal en ciberseguridad.

Escala de valoración (1-5): 1 = Nunca, 2 = Rara vez, 3 = A veces, 4 = Frecuentemente, 5 = Siempre

Ítem	Pregunta	1	2	3	4	5
P10	¿El personal recibe capacitación periódica en seguridad de la información?	☐	☐	☐	☐	☐
P11	¿Se realizan simulaciones o pruebas de ciberseguridad en la empresa?	☐	☐	☐	☐	☐
P12	¿Existen campañas de concienciación sobre seguridad digital en Cediamedical?	☐	☐	☐	☐	☐

SECCIÓN 6: GESTIÓN DE INCIDENTES DE SEGURIDAD

Indicador: Procedimientos para la identificación, respuesta y mitigación de incidentes de seguridad.

Escala de valoración (1-5): 1 = Nunca, 2 = Rara vez, 3 = A veces, 4 = Frecuentemente, 5 = Siempre

Ítem	Pregunta	1	2	3	4	5
P13	¿La empresa cuenta con un protocolo formal para la gestión de incidentes de seguridad?	☐	☐	☐	☐	☐
P14	¿Los incidentes de seguridad son documentados y analizados para evitar futuras ocurrencias?	☐	☐	☐	☐	☐
P15	¿Se realizan pruebas o simulacros de respuesta ante incidentes de seguridad?	☐	☐	☐	☐	☐

PREGUNTAS ABIERTAS ADICIONALES

1. ¿Qué mejoras propondría en los procesos de seguridad digital de la empresa?
2. ¿Ha experimentado algún incidente de seguridad en su área de trabajo? ¿Cómo fue gestionado?

_____
_____
_____
_____
_____
_____

El cuestionario se diseñó a partir de las directrices y controles establecidos en la ISO/IEC 27001 e ISO/IEC 27002, específicamente extrayendo ítems del Anexo A de la ISO/IEC 27001 y la guía de mejores prácticas de la ISO/IEC 27002, que detallan medidas para asegurar la confidencialidad, integridad y disponibilidad de la información. Además, se consultaron estudios especializados, como González (2021) y el Centro Criptológico Nacional (2022), que confirman la relevancia de estos estándares en la evaluación de la seguridad digital en organizaciones. Esto permitió formular preguntas concretas que abordan dimensiones críticas tales como políticas de seguridad, controles de acceso, procedimientos de ciberseguridad, gestión de riesgos, capacitación y manejo de incidentes.

ANEXO 4

DOCUMENTOS DE EVIDENCIA DEL MGSI – GRUPO CEDIAMEDICAL

Compendio de documentos que certifican el cumplimiento de los objetivos de la tesis y la implementación del Modelo de Gestión de Seguridad de la Información (MGSI) basado en ISO/IEC 27001 e ISO/IEC 27002.

Documento 1 – Informe de Diagnóstico de Seguridad de la Información

Referencia: ISO/IEC 27001:2022 – Cláusulas 6.1.2 (Gestión de riesgos) y 9.1 (Seguimiento, medición, análisis y evaluación).

Emitido por: Coordinador de Seguridad de la Información – Cediamedical | Fecha: 15/05/2025 | Versión: 1.0

1. Resumen ejecutivo

Se evaluó el estado inicial de la seguridad de la información en Cediamedical para identificar brechas, vulnerabilidades y riesgos prioritarios. Los resultados evidenciaron carencias en políticas formales, control de accesos, respaldo y gestión de incidentes, estableciendo una línea base clara para la implementación del SGSI.

2. Alcance del diagnóstico

Áreas evaluadas	Procesos	Activos principales	Sedes
Administración, Atención médica, Laboratorio, TI	Gestión clínica, caja/facturación, soporte, almacenamiento de historias clínicas	Servidores, estaciones de trabajo, red interna, repositorios de datos, backups	Sede principal y sucursales

3. Metodología

• Revisión documental de políticas, manuales y registros.

• Observación directa de salas críticas (cuarto de servidores, estaciones de trabajo, puntos de red).

• Aplicación del Cuestionario de Evaluación (Anexo 3) a 18 colaboradores (TI, médicos, administrativos, gerencia).

• Procesamiento de resultados (SPSS v25) y análisis descriptivo por dimensiones.

• Pruebas controladas de configuración: contraseñas, perfiles, respaldos y registro de eventos.

4. Hallazgos principales por dimensión

Dimensión	Hallazgo clave	Evidencia/Soporte
Políticas y procedimientos	28% del personal conocía políticas vigentes; políticas no difundidas	Reportes de encuesta y entrevistas
Controles de acceso	38% usaba contraseñas robustas; permisos no revisados periódicamente	Muestreo de cuentas; revisión de perfiles
Gestión de incidentes	22% conocía un protocolo formal; inexistencia de registro unificado	Encuestas; revisión de casos 2024
Respaldo y continuidad	Respaldo irregular; pruebas de restauración no documentadas	Verificación en sistemas; entrevistas TI

5. Inventario resumido de activos críticos

ID	Activo	Dueño	Ubicación	Información que procesa	Clasificación (C/I/D)
A-01	Servidor de historias clínicas	TI	Cuarto de servidores	Datos de pacientes	Alta/Alta/Alta
A-02	Servidor de facturación	TI	Cuarto de servidores	Datos económicos	Alta/Media/Alta
A-03	PC estaciones médicas	Área médica	Consultorios	Datos clínicos	Alta/Media/Media

6. Matriz de riesgos (extracto)

Riesgo	Activo	Amenaza	Vulnerabilidad	Prob.	Impacto	Nivel	Tratamiento
Acceso no autorizado	A-01	Robo de credenciales	Contraseñas débiles	Alta	Alta	Alto	Endurecer contraseñas/ MFA
Pérdida de datos	A-02	Falla hardware	Backups irregulares	Media	Alta	Alto	Backups programados + pruebas
Divulgación inadvertida	A-03	Sesión abierta	Falta de bloqueo automático	Media	Media	Medio	Política de sesiones + bloqueo

7. Conclusiones y recomendaciones iniciales

Formalizar políticas, fortalecer contraseñas y permisos, establecer protocolo de incidentes y normalizar respaldos con pruebas de restauración. Estos puntos fueron trasladados a la fase de diseño del SGSI.

Documento 2 – Alcance del Sistema de Gestión de Seguridad de la Información (SGSI)

Referencia: ISO/IEC 27001:2022 – Cláusula 4.3 (Determinación del alcance del SGSI).

Emitido por: Comité de Seguridad de la Información – Cediamedical | Fecha: 05/06/2025 | Versión: 1.0

1. Contexto y partes interesadas

Se identificaron factores internos (estructura organizativa, cultura de cumplimiento, recursos TI) y externos (regulación, proveedores, pacientes). Partes interesadas: pacientes, personal, dirección, proveedores de TI, entes reguladores.

2. Alcance

El SGSI aplica a todos los procesos, sistemas y personas que manejan información clínica y administrativa en la sede principal y sucursales de Cediamedical.

3. Exclusiones

Quedan fuera de alcance los sistemas de terceros no integrados directamente a la infraestructura de Cediamedical. Las interfaces y obligaciones se regulan por contratos y ANS.

4. Criterios de evaluación de riesgos

Criterio	Descripción
Probabilidad	Baja/Media/Alta, definida por histórico, controles existentes y exposición
Impacto	Bajo/Medio/Alto, definido por efecto en C/I/D, legal y reputación
Aceptación	Riesgo residual aceptable: hasta Medio; Alto requiere tratamiento

5. Roles y responsabilidades

Rol	Responsabilidades principales
Gerencia General	Aprobar políticas; provisión de recursos; revisión del SGSI
Comité SGSI	Gobernanza, seguimiento, decisiones sobre riesgos
Coordinador de Seguridad	Operar el SGSI; informes; soporte a áreas
TI	Implementar controles técnicos; respaldos; monitoreo
RRHH	Capacitación; registros de competencia
Áreas usuarias	Cumplir políticas; reportar incidentes

Documento 3 – Política de Seguridad de la Información

Referencia: ISO/IEC 27001:2022 – Cláusula 5.2 (Política de seguridad de la información).

Emitido por: Gerencia General – Cediamedical | Fecha: 10/06/2025 | Versión: 1.0

1. Declaración de la alta dirección

Cediamedical se compromete a proteger la confidencialidad, integridad y disponibilidad de la información clínica y administrativa mediante la implantación y mejora continua del SGSI.

2. Principios y objetivos

- Cumplimiento normativo (incluyendo Ley N.º 29733 y normativa aplicable).
- Gestión de riesgos y controles proporcionados.
- Concienciación y competencias del personal.
- Mejora continua y auditoría interna.

3. Ámbito de aplicación y cumplimiento

La política es de cumplimiento obligatorio para todo el personal y terceros con acceso a información de Cediamedical. Su incumplimiento puede conllevar medidas disciplinarias.

4. Comunicación, revisión y control de documentos

La política se difunde a toda la organización y se revisa al menos anualmente o ante cambios significativos. Se gestiona bajo control de versiones.

Documento 4 – Statement of Applicability (SoA)

Referencia: ISO/IEC 27001:2022 – Cláusula 6.1.3 (Tratamiento de riesgos de seguridad de la información).

Emitido por: Comité de Seguridad de la Información – Cediamedical | Fecha: 18/06/2025 | Versión: 1.0

1. Criterios de selección de controles

Se seleccionaron controles atendiendo a los riesgos identificados, el contexto, y los objetivos del SGSI. Cada control incluye estado de aplicación, justificación y evidencia.

2. Controles priorizados (extracto)

Control ISO/IEC 27002	Aplica	Estado	Justificación	Evidencia	Responsable
5.1 Políticas de seguridad de la información	Sí	Implementado	Formalizar lineamientos y cierre de brechas de Fase 1	Documento 3; comunicaciones	Comité SGSI
8.9 Gestión de contraseñas	Sí	Implementado	Endurecer autenticación; reducir accesos indebidos	Procedimientos TI; registros de cambios	TI
5.18 Gestión de incidentes	Sí	Implementado	Establecer proceso formal de respuesta	Registros de incidentes y simulacros	Coordinador de Seguridad
5.30 Copias de respaldo	Sí	Implementado	Asegurar disponibilidad y recuperación	Política de respaldo; informes de prueba	TI

Nota. El SoA completo incluye el total de controles aplicables y se mantiene bajo control documental en el repositorio del SGSI.

Documento 5 – Acta de Capacitación en Seguridad Digital

Referencia: ISO/IEC 27001:2022 – Cláusula 7.2 (Competencia) y 7.3 (Concienciación).

Emitido por: Área de RRHH y Coordinación de Seguridad – Cediamedical | Fecha: 25/06/2025 | Versión: 1.0

1. Datos generales

Tema	Objetivo	Duración	Modalidad	Facilitador
Buenas prácticas de seguridad y contraseñas robustas	Fortalecer hábitos de seguridad y correcto uso de credenciales	4 horas	Presencial	Coordinador de Seguridad

2. Contenidos y metodología

Contenido: políticas internas, gestión de contraseñas, phishing, sesiones y bloqueo automático, reporte de incidentes, respaldo de información. Metodología: exposición guiada, demostraciones prácticas y evaluación de salida.

3. Participantes

Nº	Nombre y cargo	Área	Firma
1	_____	_____	_____
2	_____	_____	_____
3	_____	_____	_____
4	_____	_____	_____
5	_____	_____	_____
6	_____	_____	_____
7	_____	_____	_____
8	_____	_____	_____
9	_____	_____	_____
10	_____	_____	_____
11	_____	_____	_____
12	_____	_____	_____
13	_____	_____	_____
14	_____	_____	_____
15	_____	_____	_____

16 _____ _____ _____
17 _____ _____ _____
18 _____ _____ _____

4. Resultados de evaluación

Indicador	Antes	Después	Mejora
Conocimiento de políticas	28%	94%	+66 pts
Uso de contraseñas robustas	38%	94%	+56 pts

Documento 6 – Procedimiento de Gestión de Incidentes y Registro

Referencia: ISO/IEC 27001:2022 – Cláusula 8.2 (Gestión de la seguridad de la información).

Emitido por: Coordinador de Seguridad – Cediamedical | Fecha: 05/07/2025 | Versión: 1.0

1. Objetivo y alcance

Definir el proceso para identificar, reportar, clasificar, contener, erradicar y documentar incidentes de seguridad de la información en Cediamedical.

2. Roles

Rol	Responsabilidades
Reportante	Notificar incidentes y proporcionar detalles
Coordinador de Seguridad	Clasificar, coordinar respuesta y documentar
TI	Contención técnica, erradicación y recuperación
Comité SGSI	Revisión y acciones de mejora

3. Flujo del proceso

Detección/Reporte -> Clasificación -> Contención -> Erradicación -> Recuperación -> Lecciones aprendidas -> Cierre.

4. Registro de incidentes (plantilla)

ID	Fecha	Área	Descripción	Impacto	Acciones	Estado	Cierre
INC-001	2025-07-05	Administrativa	Sesión abierta en sistema clínico	Potencial acceso no autorizado	Cierre remoto; bloqueo; capacitación	Cerrado	2025-07-06

Documento 7 – Informe Final de Evaluación de Objetivos

Referencia: ISO/IEC 27001:2022 – Cláusula 9.1 (Medición, análisis y evaluación) y 9.3 (Revisión por la dirección).

Emitido por: Comité de Seguridad de la Información – Cediamedical | Fecha: 20/07/2025 | Versión: 1.0

1. Objetivo del informe

Consolidar los resultados post-implementación y evaluar el cumplimiento de los objetivos específicos de la investigación.

2. Resultados comparativos

Indicador	Antes	Después	Fuente
Conocimiento de políticas de seguridad	28%	94%	Anexo 3; Registros Doc. 5
Uso de contraseñas seguras	38%	94%	Anexo 3; Evidencias TI
Protocolo de incidentes conocido y aplicado	22%	88%	Anexo 3; Doc. 6

3. Cumplimiento de objetivos específicos

Objetivo específico	Estatus	Evidencia principal
OE1 – Diagnosticar el nivel de seguridad	Cumplido	Documento 1
OE2 – Diseñar el modelo de SGSI	Cumplido	Documento 2 y 3
OE3 – Implementar el modelo	Cumplido	Documento 4, evidencias TI
OE4 – Evaluar efectividad	Cumplido	Documento 7; comparativos
OE5 – Mejora continua	Cumplido	Documento 8

4. Conclusión

Los objetivos planteados se cumplieron plenamente, evidenciándose mejoras significativas en los indicadores clave y la formalización de procesos críticos del SGSI.

Documento 8 – Plan de Implementación y Mejora Continua del SGSI

Referencia: ISO/IEC 27001:2022 – Cláusulas 6.2 (Objetivos de seguridad), 8.1 (Planificación y control operacional) y 10.2 (Mejora).

Emitido por: Comité de Seguridad de la Información – Cediamedical | Fecha: 01/06/2025 | Versión: 1.0

1. Objetivo del plan

Definir actividades, responsables, recursos, plazos e indicadores para ejecutar y sostener el SGSI en el tiempo.

2. Cronograma y entregables (WBS)

Código	Actividad	Responsable	Plazo	Entregable/Evidencia
1.1	Definir alcance del SGSI	Comité SGSI	Semana 1	Documento 2 – Alcance
1.2	Aprobar política de seguridad	Gerencia	Semana 2	Documento 3 – Política
1.3	Evaluar y tratar riesgos	Coordinador Seguridad	Semanas 3–4	Documento 1 – Reporte de riesgos
1.4	Diseñar SoA	Comité SGSI	Semana 5	Documento 4 – SoA
1.5	Implementar controles técnicos	TI	Semanas 6–8	Registros de cambios
1.6	Capacitar al personal	RRHH/Seguridad	Semanas 6–9	Documento 5 – Actas
1.7	Simulacros de incidentes	Seguridad	Semana 10	Registro de simulacro
1.8	Auditoría interna	Auditor designado	Semana 11	Informe de auditoría
1.9	Evaluación final y ajustes	Comité SGSI	Semana 12	Documento 7 – Informe final

3. Indicadores (KPI) de seguimiento

KPI	Definición	Meta	Frecuencia	Responsable
Cumplimiento de políticas	% de personal que conoce y aplica	≥90%	Trimestral	Comité SGSI
Contraseñas robustas	% de cuentas con criterios robustos	≥90%	Mensual	TI
Respaldo	% de	≥95%	Mensual	TI

verificado	respaldos con prueba OK			
Tiempo de respuesta a incidentes	Promedio en horas	≤24 h	Mensual	Seguridad
Acciones correctivas cerradas	% de AC cerradas en plazo	≥90%	Trimestral	Comité SGSI

4. Riesgos del proyecto y mitigaciones

Riesgo	Impacto	Prob.	Mitigación
Falta de recursos	Retrasos	Media	Planificación y escalamiento a gerencia
Resistencia al cambio	Baja adopción	Media	Capacitación y comunicaciones
Dependencia de terceros	Brechas en integraciones	Baja	ANS y validaciones periódicas

5. Revisión y mejora continua

El plan se revisará semestralmente por el Comité SGSI y se ajustará con base en auditorías, incidentes reales y cambios de contexto.