PIERRE ANGHELO MANUEL TELLO SAAVEDRA

Implementación de la norma ISO 27110 y la gestión de la ciberseguridad en la municipalidad distrital de Morales, 2025

Unidad de Investigación de la Facultad de Ingeniería de Sistemas e Informática

Detalles del documento

Identificador de la entrega
trn:oid:::3117:543491856

Fecha de entrega
29 dic 2025, 13:00 GMT-5

Fecha de descarga
29 dic 2025, 13:07 GMT-5

Nombre del archivo
INFORME FINAL DE PROYECTO DE TESIS - PIERRE TELLO 14-11-2025 (3) (3).docx

Tamaño del archivo
932.6 KB

108 páginas

22.009 palabras

127.250 caracteres

24% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

20% Fuentes de Internet
5% Publicaciones
19% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Fuentes principales

20% Fuentes de Internet
5% Publicaciones
19% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1 Internet
repositorio.unsm.edu.pe 7%

2 Internet
tesis.unsm.edu.pe 3%

3 Trabajos del estudiante
Universidad Privada Antenor Orrego on 2024-12-05 2%

4 Trabajos del estudiante
Universidad Nacional de San Martín on 2025-11-08 1%

5 Trabajos del estudiante
Universidad Nacional de San Martín on 2025-09-15 <1%

6 Internet
hdl.handle.net <1%

7 Internet
repositorio.ucv.edu.pe <1%

8 Internet
repositorio.ulasamericas.edu.pe <1%

9 Internet
dialnet.unirioja.es <1%

10 Internet
ve.scielo.org <1%

11 Internet
www.coursehero.com <1%

12 Trabajos del estudiante
Universidad Internacional de la Rioja on 2025-01-30 <1%

13 Trabajos del estudiante
Universidad San Marcos on 2025-03-31 <1%

14 Trabajos del estudiante
Universidad Andina Nestor Caceres Velasquez on 2025-12-02 <1%

15 Trabajos del estudiante
Universidad Andina Nestor Caceres Velasquez on 2025-09-05 <1%

16 Internet
repositorio.une.edu.pe <1%

17 Internet
repositorio.uct.edu.pe <1%

18 Trabajos del estudiante
Universidad San Marcos on 2025-12-13 <1%

19 Trabajos del estudiante
Universidad Tecnologica del Peru on 2023-07-12 <1%

20 Trabajos del estudiante
Consorcio CIXUG on 2019-11-10 <1%

21 Internet
pdfcookie.com <1%

22 Trabajos del estudiante
Universidad Privada San Juan Bautista on 2025-12-14 <1%

23 Trabajos del estudiante
Universidad Cesar Vallejo on 2025-07-30 <1%

24 Trabajos del estudiante
Universidad Nacional de San Martín on 2024-01-16 <1%

25 Trabajos del estudiante
Universidad del Bosque on 2024-11-09 <1%

26 Internet
ebuah.uah.es <1%

27 Trabajos del estudiante
Foundation University, Islmabad on 2025-09-19 <1%

28 Trabajos del estudiante
Universidad Nacional Santiago Antunez de Mayolo on 2025-11-29 <1%

29 Trabajos del estudiante
Universidad Privada San Juan Bautista on 2025-12-19 <1%

30 Internet
repositorioacademico.upc.edu.pe <1%

31 Trabajos del estudiante
Universidad Privada Antenor Orrego 2025 on 2025-07-18 <1%

32 Internet
www.globalstd.com <1%

33 Trabajos del estudiante
Bachillerato Alexander Bain, S.C on 2007-05-04 <1%

34 Internet
alicia.concytec.gob.pe <1%

35 Internet
cloud.google.com <1%

36 Internet
prezi.com <1%

37 Publicación
Abeer Saad Alsubaie, Alhanouf Khalid Alsharif, Fai Abdullah Almalki, Reham Same... <1%

38 Publicación
David Anibal Paz Panduro. "Impacto de los diarios digitales en la votación elector... <1%

39 Trabajos del estudiante
GIAC on 2004-10-13 <1%

40 Trabajos del estudiante
Universidad Cesar Vallejo on 2024-06-29 <1%

41 Trabajos del estudiante
Universidad Tecnológica Centroamericana UNITEC on 2025-12-27 <1%

42 Trabajos del estudiante
Universidad de San Martin de Porres on 2024-09-15 <1%

43 Trabajos del estudiante
consultoriadeserviciosformativos on 2024-02-05 <1%

44 Trabajos del estudiante
uncedu on 2025-07-04 <1%

45 Internet
www.paot.org.mx <1%

46 Trabajos del estudiante
Universidad Andina Nestor Caceres Velasquez on 2025-12-22 <1%

47 Trabajos del estudiante
Universidad Cesar Vallejo on 2025-07-16 <1%

48 Trabajos del estudiante
Universidad Privada de Tacna on 2021-01-13 <1%

49 Internet
busqueda.bvsalud.org <1%

50 Internet
esdeglibros.edu.co <1%

51 Internet
repositorio.ucam.edu <1%

52 Internet
repositorio.ulatina.ac.cr <1%

53 Internet
repositorio.unheval.edu.pe <1%

54 Internet
www.researchgate.net <1%

55 Trabajos del estudiante
CORPORACIÓN UNIVERSITARIA IBEROAMERICANA on 2024-12-02 <1%

56 Publicación
Germán Rojas-Cabezas, Ronald Mora-Esquivel, Nicolas Márquez, Susana Chacón-E... <1%

57 Trabajos del estudiante
Pontificia Universidad Catolica del Ecuador - PUCE on 2023-06-05 <1%

58 Trabajos del estudiante
Universidad Andina Nestor Caceres Velasquez on 2024-07-11 <1%

59 Trabajos del estudiante
Universidad Andina Nestor Caceres Velasquez on 2025-09-21 <1%

60 Trabajos del estudiante
Universidad Andina Nestor Caceres Velasquez on 2025-09-25 <1%

61 Trabajos del estudiante
Universidad Andina del Cusco on 2025-11-23 <1%

62 Trabajos del estudiante
Universidad Católica Nordestana on 2024-11-16 <1%

63 Trabajos del estudiante
Universidad Cesar Vallejo on 2019-02-25 <1%

64 Trabajos del estudiante
Universidad Internacional de la Rioja on 2024-12-14 <1%

65 Trabajos del estudiante
Universidad Mariano Gálvez de Guatemala on 2024-11-28 <1%

66 Trabajos del estudiante
Universidad Nacional Abierta y a Distancia, UNAD,UNAD on 2023-12-07 <1%

67 Trabajos del estudiante
Universidad Nacional Agraria de la Selva on 2025-12-18 <1%

68 Trabajos del estudiante
Universidad del Istmo de Panamá on 2024-12-02 <1%

69 Internet
ciencialatina.org <1%

70 Internet
freetrade.tamiu.edu <1%

71 Internet
proyectosti.muniate.gob.pe <1%

72 Internet
renati.sunedu.gob.pe <1%

73 Internet
repositorio.ujcm.edu.pe <1%

74 Internet
repositorio.unitec.edu <1%

75 Internet
revistas.unaat.edu.pe <1%

76 Trabajos del estudiante
ufidelitas on 2025-01-07 <1%

77 Internet
www.cinterfor.org.uy <1%

78 Internet
www.isaca.org <1%

79 Internet
www.netconsultingonline.com <1%

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENERÍA DE SISTEMAS E INFORMÁTICA

Tesis

Implementación de la norma ISO 27110 y la gestión de la ciberseguridad en la municipalidad distrital de Morales, 2025

Para optar el título profesional de Ingeniero de Sistemas e Informática

Autor:

Pierre Anghelo Manuel Tello Saavedra
https://orcid.org/0000-0002-3883-9712

Asesor:

Ing. MBA. John Clark Santa Maria Pinedo
https://orcid.org/0000-0002-8594-4865

Tarapoto, Perú

2025

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENERÍA DE SISTEMAS E INFORMÁTICA

Tesis

Implementación de la norma ISO 27110 y la gestión de la ciberseguridad en la municipalidad distrital de Morales, 2025

Para optar el título profesional de Ingeniero de Sistemas e Informática

Autor:

Pierre Anghelo Manuel Tello Saavedra

Sustentado y Aprobado el 19 de septiembre de 2025, ante el honorable jurado:

Presidente de Jurado Lic. Dr. Carlos Rodríguez Grández	**Secretario de Jurado** Ing. Dr. Jorge Damian Valverde Iparraguirre

Vocal del Jurado
Ing. Mg. Segundo Roger Ramírez Shupingahua

Asesor
Ing. MBA John Clark Santa María Pinedo

Tarapoto, Perú

2025

Declaratoria de autenticidad

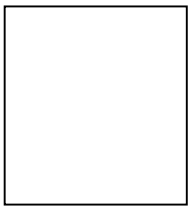
Yo, Pierre Anghelo Manuel Tello Saavedra, identificado con DNI N° 72865358, egresado de la Escuela Profesional de Ingeniería de Sistemas e Informática, de la Universidad Nacional de San Martín, con la tesis titulada: Implementación de la norma ISO 27110 y la gestión de la ciberseguridad en la municipalidad distrital de Morales, 2025.

Declaro bajo juramento que:

1. La tesis presentada es de mi autoría.
2. He respetado las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto, la tesis no ha sido plagiada ni total ni parcialmente.
3. La tesis no ha sido auto plagiada; es decir, no ha sido publicada ni presentada anteriormente para obtener algún grado académico previo o título profesional.
4. Los datos presentados en los resultados son reales, no han sido falseados, ni duplicados, ni copiados y por tanto los resultados que se presenten en la tesis se constituirán en aportes a la realidad investigada.

De considerar que el trabajo cuenta con una falta grave, como el hecho de contar con datos fraudulentos, demostrar indicios y plagio (al no citar la información con sus autores), plagio (al presentar información de otros trabajos como propios), falsificación (al presentar la información e ideas de otras personas de forma falsa), entre otros, asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad Nacional de San Martín.

Tarapoto, 19 de Setiembre de 2025



Pierre Anghelo Manuel Tello Saavedra
DNI N° 72865358

Ficha de identificación

Título: Implementación de la norma ISO 27110 y la gestión de la ciberseguridad en la municipalidad distrital de Morales, 2025	**Área de investigación:** Ingeniería y Tecnología. **Línea de investigación:** Estrategias de tecnologías de información y comunicación (TIC) y sistemas constructivos convencionales y no convencionales para el desarrollo sostenible. **Sublínea de investigación:** Inteligencia artificial y recuperación de la información **Grupo de investigación:** Gestión de TI, Automatización, IA, Análisis y Minería de Datos. **Tipo de investigación:** Básica ☐, Aplicada ☒, Desarrollo experimental ☐

Autor: Pierre Anghelo Manuel Tello Saavedra	Facultad de Ingeniería de Sistemas e Informática Escuela Profesional de Ingeniería de Sistemas e Informática https://orcid.org/0000-0002-3883-9712

Asesor: Ing. MBA. John Clark Santa María Pinedo	**Dependencia local de soporte:** Facultad de Ingeniería de Sistemas e Informática Escuela Profesional de Ingeniería de Sistemas e Informática Unidad o Laboratorio Ingeniería de Sistemas e Informática https://orcid.org/0000-0002-8594-4865

Dedicatoria

Dedico esta tesis, con profundo respeto y gratitud, a mis padres, quienes con su amor, esfuerzo y sacrificio me han enseñado el verdadero significado de la constancia y la responsabilidad. A ustedes, que nunca dejaron de creer en mí, incluso cuando yo dudaba, les entrego este logro como fruto de nuestra lucha compartida.

También dedico este trabajo a mi familia y seres queridos, cuyo apoyo incondicional fue mi sostén durante cada jornada de estudio, cada noche de desvelo y cada desafío superado.

Finalmente, dedico este logro a Dios, fuente de sabiduría, por darme la fortaleza para avanzar aun cuando el camino parecía incierto.

Pierre Anghelo Manuel Tello Saavedra

Agradecimiento

Agradezco en primer lugar a Dios, por concederme salud, perseverancia y lucidez a lo largo de este proceso académico.

Expreso mi sincero agradecimiento a la Universidad Nacional de San Martín, a la Facultad de Ingeniería de Sistemas e Informática y a todos los docentes que forjaron mi formación profesional con paciencia, rigor y vocación.

Agradezco de manera especial al Ing. John Clark Santa María Pinedo, mi asesor, por su guía, sus valiosas observaciones y su compromiso en el desarrollo de esta tesis.

A la Municipalidad Distrital de Morales, por permitirme acceder a la información necesaria y brindar las facilidades para ejecutar esta investigación.

Pierre Anghelo Manuel Tello Saavedra

Índice general

Índice de tablas

Índice de figuras

RESUMEN

Implementación de la Norma ISO 27110 y la Gestión de la Ciberseguridad en la Municipalidad Distrital de Morales, 2025

La presente investigación tuvo como objetivo determinar en qué medida la implementación de la norma ISO 27110 influye en la gestión de la ciberseguridad en la Municipalidad Distrital de Morales en 2025. Corresponde a un estudio de tipo aplicada, enfoque cuantitativo, método deductivo, nivel relacional y diseño no experimental de corte transversal. La población y muestra lo conformaron 30 trabajadores del área de TI y personal involucrado en el uso de TI de la entidad pública. Se aplicó la encuesta y se usó el cuestionario para la recolección de datos. Se ha encontrado una relación positiva entre la aplicación de la norma y la confidencialidad de la información (Rho = 0.662), fortaleciendo la protección de datos sensibles y reduciendo accesos no autorizados. Del mismo modo, la norma influye considerablemente en la integridad de la información (Rho = 0.764), asegurando su exactitud y confiabilidad, y en la disponibilidad de los datos (Rho = 0.782), garantizando su acceso oportuno y optimizando la continuidad operativa dentro de la municipalidad. Se llegó a concluir que, la implementación de la norma ISO 27110 en la Municipalidad Distrital de Morales ha demostrado tener un impacto significativo en la gestión de la ciberseguridad, mejorando en un 54.61 % la protección contra riesgos digitales.

Palabras clave: Norma ISO 27110, ciberseguridad, confidencialidad, integridad, disponibilidad

ABSTRACT

Implementation of ISO 27110 and cybersecurity management in the district municipality of Morales, 2025

The objective of this research was to determine the extent to which the implementation of ISO 27110 influences cybersecurity management in the District Municipality of Morales in 2025. It is an applied study with a quantitative approach, deductive method, relational level, and non-experimental cross-sectional design. The population and sample consisted of 30 IT workers and staff involved in the use of IT in the public entity. The survey was administered and the questionnaire was used for data collection. The survey was administered and the questionnaire was used for data collection. A positive relationship was found between the application of the standard and the confidentiality of information (Rho = 0.662), strengthening the protection of sensitive data and reducing unauthorized access. Similarly, the standard has a considerable influence on the integrity of information (Rho = 0.764), ensuring its accuracy and reliability, and on the availability of data (Rho = 0.782), guaranteeing timely access and optimizing operational continuity within the municipality. It was concluded that the implementation of the ISO 27110 standard in the District Municipality of Morales has had a significant impact on cybersecurity management, improving protection against digital risks by 54.61%.

Keywords: ISO 27110 standard, cybersecurity, confidentiality, integrity, availability

CAPÍTULO I
INTRODUCCIÓN A LA INVESTIGACIÓN

La ciberseguridad es una preocupación global debido al incremento exponencial de ciberataques. Según Check Point Software (2023), las instituciones públicas y privadas enfrentan más de 2,200 ataques por día a nivel mundial, destacándose como objetivos críticos las entidades gubernamentales y las infraestructuras esenciales. Además, el informe de INTERPOL (2020) evidenció que, durante la pandemia de COVID-19, se registró un aumento del 48% en actividades maliciosas, incluidas campañas de phishing y ransomware. Este panorama demuestra la importancia de adoptar estándares internacionales que ayuden a mitigar riesgos y a garantizar la continuidad operativa.

La norma ISO/IEC 27110 surge como una herramienta clave para estructurar marcos de ciberseguridad más sólidos. Según Djebbar y Nordström (2023), esta norma es especialmente pertinente para industrias clave, ya que ofrece una estructura cohesionada que mejora la interoperabilidad y la colaboración entre las partes interesadas. A medida que las amenazas evolucionan en complejidad, las normas técnicas mundiales facilitan la seguridad de la información y fomentan una estrategia cooperativa para la gestión de riesgos.

Por otro lado, la transformación digital global ha creado nuevos desafíos y oportunidades. Según el Foro Económico Mundial (2022), el costo de las brechas de seguridad cibernética alcanzó los 6 billones de dólares en 2021, lo que pone de manifiesto la necesidad urgente de enfoques integrales y efectivos. Watkins (2022) resalta que la implementación de normas como la ISO/IEC 27001 y la ISO/IEC 27110 no solo busca proteger activos informáticos, sino también fomentar una cultura organizacional orientada hacia la mejora continua en seguridad. Esto es particularmente importante en un entorno en el que la digitalización avanza a pasos agigantados y en el que las organizaciones deben ser resilientes frente a las amenazas emergentes.

En Perú, los esfuerzos por mejorar la ciberseguridad se han intensificado en los últimos años. En 2016, la Presidencia del Consejo de Ministros (PCM) estableció la obligatoriedad de implementar la Norma Técnica Peruana ISO/IEC 27001:2014 en entidades públicas, marcando un hito en la protección de datos estatales (PCM, 2016). Sin embargo, los desafíos persisten. Kim (2022) destaca que, en muchos países, la implementación de sistemas de gestión de seguridad de la información (ISMS) enfrenta barreras como la falta de recursos técnicos y financieros, una situación que también puede reflejarse en el caso peruano. De hecho, un estudio realizado por el Ministerio de

Transportes y Comunicaciones (MTC) en 2022 identificó que solo el 45% de las entidades cumple con estas normativas, evidenciando una implementación desigual y dejando al país vulnerable ante amenazas crecientes.

Asimismo, un informe de Kaspersky (2022) reveló que Perú fue el tercer país en Latinoamérica más afectado por ciberataques, contabilizando más de 17 millones de incidentes ese año. Este dato incluye ataques dirigidos específicamente a entidades públicas, subrayando la urgencia de adoptar marcos normativos como la ISO/IEC 27110 para fortalecer las capacidades de prevención y respuesta en el sector gubernamental. Djebbar y Nordström (2023) argumentan que la implementación efectiva de estas normativas no solo reduce riesgos, sino que también mejora la confianza de los ciudadanos y las partes interesadas en las instituciones gubernamentales.

En la región San Martín, la digitalización de los servicios gubernamentales ha avanzado considerablemente en los últimos años. Sin embargo, este progreso ha traído consigo desafíos relacionados con la seguridad de la información. Según un informe del Gobierno Regional de San Martín (2021), más del 60% de los municipios no cuentan con un plan de ciberseguridad formal, lo que aumenta su vulnerabilidad frente a posibles ataques. Este escenario refleja la urgente necesidad de políticas de ciberseguridad robustas que protejan los datos y sistemas utilizados en la administración pública local. En este sentido, la implementación de medidas de seguridad es fundamental, tal como lo subraya Kyranoudi et al. (2021), quienes identifican que la certificación en ciberseguridad es crucial para asegurar la protección de las cadenas de suministro, un componente clave en la administración pública.

Por su parte, un estudio realizado por la Universidad Nacional de San Martín (2023) destaca que las brechas en infraestructura tecnológica y la falta de personal capacitado son factores clave que limitan la implementación de medidas de seguridad. Esto coincide con lo planteado por Peng (2023), quien señala que la falta de una gobernanza adecuada en ciberseguridad puede generar vulnerabilidades significativas en los sistemas críticos. La implementación de normas internacionales, como la ISO/IEC 27110, puede servir como una medida eficaz para garantizar la continuidad operativa y salvaguardar los servicios esenciales que prestan las municipalidades.

La Municipalidad Distrital de Morales enfrenta grandes desafíos relacionados con la ciberseguridad debido a la creciente digitalización de sus servicios y la falta de un marco normativo robusto. La ausencia de estándares como la norma ISO/IEC 27110 incrementa la vulnerabilidad ante ciberataques, comprometiendo no solo la confidencialidad de la información, sino también la calidad y continuidad de los servicios

74

60

prestados a los ciudadanos. Por ello, resulta imperativo diseñar esta normativa, estableciendo un sistema integral que mitigue los riesgos asociados a amenazas cibernéticas y garantice un entorno seguro para las operaciones municipales.

En base a lo expuesto, se formuló el problema de investigación ¿En qué medida la implementación de la norma ISO 27110 influye en la gestión de la ciberseguridad en la Municipalidad Distrital de Morales en 2025? De tal manera que el objetivo general del estudio fue: Determinar en qué medida la implementación de la norma ISO 27110 influye en la gestión de la ciberseguridad en la Municipalidad Distrital de Morales en 2025. Consecuentemente, los objetivos específicos fueron: a) Determinar en qué medida la implementación de la norma ISO 27110 influye en la confidencialidad de la información en la Municipalidad Distrital de Morales en 2025. b) Determinar en qué medida la implementación de la norma ISO 27110 influye en la integridad de la información en la Municipalidad Distrital de Morales en 2025. Y c) Determinar en qué medida la implementación de la norma ISO 27110 influye en la disponibilidad de la información en la Municipalidad Distrital de Morales en 2025.

En ese sentido, se planteó como hipótesis general de la investigación: La implementación de la norma ISO/IEC 27110 influye significativamente en la mejora de la gestión de la ciberseguridad de la Municipalidad Distrital de Morales durante el año 2025.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes de la investigación

A nivel internacional, Kim (2022), El objetivo de la tesis fue investigar los estándares, regulaciones y marcos comunes de seguridad de la información, con un enfoque en la implementación y el mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI), cumpliendo con los requisitos internacionales y nacionales. La metodología utilizada incluyó una investigación teórica sobre el desarrollo y funcionamiento del SGSI, junto con un análisis comparativo de la norma internacional ISO/IEC 27002:2022 y la herramienta de auditoría de seguridad Katakri 2020. Los resultados obtenidos mostraron un sólido punto de referencia común para la seguridad de los sistemas de información, sustentado por ambas normativas, con algunas diferencias en el enfoque, áreas de atención y controles específicos. En conclusión, el estudio proporcionó una estrategia para mejorar un SGSI existente, ayudando a las organizaciones a alcanzar el cumplimiento de regulaciones adicionales y ofreciendo conocimientos valiosos sobre la gestión de seguridad de la información y las mejores prácticas del sector.

Djebbar & Nordström (2023), El objetivo de la investigación fue realizar un estudio comparativo entre tres normas de ciberseguridad ampliamente adoptadas: ETSI EN 303 645 v2.1.1, ISA/IEC 62443-3-3:2019 e ISO/IEC 27001:2022, con el fin de identificar las superposiciones y discrepancias entre ellas, facilitando así el proceso de selección de controles de seguridad adecuados. La metodología empleada consistió en un análisis exhaustivo de los estándares, teniendo en cuenta sus diferentes áreas de enfoque y adoptando un enfoque estratégico para optimizar los esfuerzos de cumplimiento y reducir la carga administrativa. Los resultados obtenidos evidenciaron una significativa superposición entre los tres estándares, lo cual puede ayudar a las organizaciones a entender mejor los requisitos y controles de seguridad comunes, mejorando la eficiencia de los esfuerzos de cumplimiento. En conclusión, este estudio proporciona información valiosa que simplifica el proceso de selección de normas y facilita el cumplimiento de las regulaciones, permitiendo a las organizaciones optimizar sus recursos y mejorar su ciberseguridad.

Rotim& Landeka (2024), El objetivo de este artículo fue proporcionar una comprensión clara del panorama normativo en ciberseguridad, destacando la importancia de la adopción de la Directiva NIS 2 en la Unión Europea para establecer un estándar

uniforme de ciberseguridad. La metodología utilizada consistió en analizar los marcos normativos, estándares y directrices relacionados con la Directiva NIS 2, con el fin de guiar a las entidades en la implementación efectiva de medidas de seguridad organizativas y técnicas. Los resultados mostraron que la adopción proactiva de la Directiva NIS 2 es crucial para fortalecer la resiliencia y seguridad del entorno digital en la UE. En conclusión, el artículo subraya que comprender y aplicar estos principios permite a las organizaciones protegerse de las crecientes ciberamenazas y contribuir a la seguridad colectiva del ecosistema digital europeo.

Martin (2023), El objetivo de este documento fue analizar las regulaciones de ciberseguridad a nivel internacional, regional y nacional, con el fin de identificar elementos aplicables a las actividades espaciales y determinar cómo garantizar la seguridad en el ciberespacio en relación con las actividades en el espacio ultraterrestre. La metodología empleada consistió en estudiar las interacciones entre ambos dominios y evaluar los riesgos asociados con los sistemas satelitales y la transmisión de datos. Los resultados revelaron un creciente riesgo de ciberataques contra satélites, lo que destaca la necesidad de fortalecer las medidas de seguridad en el espacio y evitar enfoques compartimentados en cuanto al ciberespacio y el espacio ultraterrestre. En conclusión, se subrayó la importancia de crear un marco regulatorio estructurado que involucre a todos los actores relevantes, con el objetivo de enfrentar de manera efectiva las ciberamenazas y garantizar la sostenibilidad y seguridad de las actividades espaciales a largo plazo.

Kyranoudi et al. (2021), El objetivo de este documento fue presentar los elementos básicos y los requisitos necesarios para la certificación de seguridad de los servicios de la cadena de suministro (SCS), destacando su importancia crítica para la competitividad, la prosperidad y la resiliencia del mercado único digital europeo. La metodología consistió en la identificación y análisis de las medidas de mitigación necesarias para garantizar la fiabilidad de las economías digitales. Los resultados evidenciaron que la certificación de la seguridad de los SCS es una herramienta clave para asegurar la estabilidad y protección de las cadenas de suministro en el contexto digital. En conclusión, se subrayó que implementar una certificación adecuada en este ámbito es esencial para fortalecer la seguridad de los servicios de la cadena de suministro y proteger las economías digitales a nivel europeo.

Donalds et al. (2022), El objetivo de este libro fue examinar la prevalencia, naturaleza, tendencias e impactos de los incidentes relacionados con la ciberseguridad en las economías del Sur Global, centrándose en los desafíos, amenazas y riesgos que

enfrentan las micro, pequeñas y medianas empresas (MIPYME) y los gobiernos en estas regiones. La metodología consistió en el análisis de conceptos, estrategias y marcos legislativos, además de proporcionar herramientas, técnicas y mejores prácticas basadas en evidencia para mejorar la resiliencia en términos de ciberseguridad. Los resultados destacaron la necesidad urgente de implementar marcos específicos de ciberseguridad adaptados a las realidades del Sur Global, con un enfoque particular en las MIPYME. En conclusión, se subrayó la importancia de promover la ciberseguridad y fortalecer las capacidades de las empresas y gobiernos en estas economías, proporcionando una agenda de investigación y estrategias de prevención para mejorar la protección frente a incidentes cibernéticos en el Sur Global.

Rodríguez & Rojas (2022), Este trabajo presenta los resultados de una investigación orientada a la creación de marcos de ciberseguridad, ofreciendo una guía para la implementación de marcos que aborden los aspectos esenciales de la seguridad informática. La guía describe de manera clara y accesible los conceptos necesarios para la creación de estos marcos, incluyendo recomendaciones sobre las categorías a implementar, la Implementación adecuada y ejemplos prácticos. Además, se hace referencia a las normas ISO/IEC, que ofrecen recomendaciones esenciales para crear estos marcos de acuerdo con el entorno específico de la empresa. La principal ventaja de la guía es su adaptabilidad, que permite la alineación con los marcos de ciberseguridad previamente establecidos dentro de las empresas, facilitando así el intercambio de información y conocimientos. El objetivo del manual es consolidar los instrumentos conceptuales necesarios para determinar las normas estandarizadas aplicables a diversas empresas, teniendo en cuenta sus especificidades en el procesamiento de la información. El objetivo es garantizar que todas las partes interesadas comprendan y participen en el desarrollo y la ejecución de marcos de ciberseguridad dentro de la organización. El manual sirve como documento de referencia para fines de desarrollo.

A nivel nacional, Valdospin et al. (2024), El objetivo de este estudio fue elaborar un modelo de gestión de política de privacidad para la consulta externa de usuarios en un hospital público de Ecuador, dada la creciente digitalización del sector sanitario público y los riesgos asociados a la gestión de datos sensibles. Se administró un cuestionario estructurado a 300 consumidores seleccionados mediante un muestreo probabilístico sistemático, como parte de un enfoque cuantitativo transversal con un alcance descriptivo-correlacional. Los resultados indicaron déficits significativos en todos los componentes evaluados, lo que demuestra que ninguno alcanzó la calificación mínima aprobatoria del 50 %. El componente más importante, la gestión de documentos, obtuvo

la calificación más alta, con un 28,4%. El análisis factorial reveló que tres elementos principales representaban el 88 % de la varianza: la protección de datos (28,7 %), el control de acceso (34,2 %) y el cumplimiento normativo (25,1 %). La crisis de confianza del sistema se reflejó en la calificación general de satisfacción de los usuarios, que fue de 3,2/10. Se propuso una reestructuración integral del paradigma de gestión, basada en estos tres factores, para garantizar la seguridad efectiva de los datos personales en el contexto hospitalario ecuatoriano.

Ángeles (2023), La investigación tuvo como objetivo principal determinar la influencia de la Gestión de la Ciberseguridad en la Concientización Digital de los usuarios administrativos de una empresa Outsourcing en Lima, 2023. Este fue un estudio aplicado que utilizó un diseño correlacional transversal y una metodología cuantitativa. Utilizando la herramienta Analyst STATS, se tomó una muestra de 151 usuarios con un nivel de confianza del 95 % y un margen de error del 5 % de la población de 250 usuarios administrativos. Se utilizó una encuesta en línea, aprobada por tres especialistas, para recopilar los datos. La gestión de la ciberseguridad tuvo un impacto moderado en la conciencia digital, según el análisis descriptivo que se llevó a cabo utilizando el cruce de tablas entre variables y dimensiones. Las pruebas estadísticas inferenciales indicaron una correlación positiva significativa entre las dos variables, evidenciada por un coeficiente Rho de Spearman de 0,847 y un nivel de significación de $p < 0,001$. En última instancia, se constató que la gestión de la ciberseguridad afecta significativamente a la conciencia digital.

Olivos (2024), La investigación tuvo como objetivo determinar la influencia de la gestión de riesgos y la ciberseguridad en la toma de decisiones del Sistema Nacional de Informática del Estado peruano en el año 2024. Con una muestra representativa de analistas de ciberseguridad del sistema, se utilizó un método cuantitativo con un diseño descriptivo transversal no experimental, basado en el marco de ciberseguridad elaborado por von Solms y van Niekerk y las teorías de gestión de riesgos de la norma ISO 31000. Los resultados mostraron que existían variaciones en la aplicación de las técnicas de ciberseguridad y gestión de riesgos por parte del sistema. No obstante, estos factores influyeron significativamente en el proceso de toma de decisiones, lo que pone de relieve la necesidad de mejorar estas competencias esenciales. Con el fin de garantizar un rendimiento fiable y seguro en el mundo digital moderno, se determinó que el Sistema Nacional de Información aún se enfrentaba a obstáculos significativos para integrar con éxito la gestión de riesgos y la ciberseguridad.

Chuqui (2024), La investigación tuvo como objetivo determinar la influencia de la ciberseguridad en la gestión de riesgos. Se utilizó un diseño correlacional causal no experimental de manera explicativa. La población del estudio estuvo compuesta por treinta trabajadores, y el método de recopilación de datos empleado fue una encuesta. Un análisis de regresión logística ordinal reveló que existía una relación suficiente entre las variables, con un valor de significación de 0,002 inferior a 0,05, lo que respaldaba la hipótesis general. Se determinó que la gestión de riesgos en la institución educativa de Callao en 2023 se veía significativamente afectada por la ciberseguridad, que representaba el 37,7 % de la variación en la gestión de riesgos.

Quispe & Felix (2022), El proyecto de investigación se puso en marcha debido a las pérdidas económicas y las violaciones de datos derivadas de una gestión inadecuada de la información y la pérdida de datos de clientes en varios departamentos de la organización. El estudio examinó la correlación entre la ciberseguridad y las TIC en Kiaratel S.A.C. con el fin de mejorar los protocolos de seguridad y mantener la lealtad de los clientes. El estudio utilizó un diseño transversal no experimental y una metodología cualitativa y descriptiva. De una población de 100 personas, se seleccionó a 40 mediante un muestreo probabilístico. En las encuestas se utilizaron doce preguntas sobre la gestión de la información y doce preguntas sobre la resiliencia de la ciberseguridad. Para examinar los datos se utilizó el software SPSS versión 23. Con un 82,5 % de confianza, los resultados demostraron una correlación significativa entre la ciberseguridad y la gestión de las TIC, lo que indica una estrecha relación entre ambos ámbitos en Kiaratel S.A.C. en 2022.

A nivel local, Ramos (2023), La presente investigación tuvo como objetivo estudiar los controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical Esta investigación empleó una metodología cuantitativa, un enfoque deductivo, un nivel descriptivo y un diseño longitudinal preexperimental. La muestra demográfica estuvo compuesta por 36 empleados de la empresa. Se utilizó un cuestionario como instrumento y una encuesta como método de recopilación de datos. Los resultados revelaron que, antes de implementar los controles críticos, la usabilidad de la información era inadecuada (61.1%), y después de los controles críticos, mejoró a adecuada (88.9%). La seguridad, que inicialmente era inadecuada (69.4%), también mejoró a adecuada (88.9%), y la fiabilidad, que antes era inadecuada (55.6%), pasó a ser adecuada (86.1%). Se determinó que el uso efectivo de la información por parte de Procesadora Tropical se ve significativamente afectado por controles cruciales de ciberseguridad. Con un valor p de 0,000, por debajo del umbral de significación permitido (0,05), esto se demostró mediante la prueba estadística paramétrica t de Student para

muestras relacionadas, lo que confirma el importante impacto de la gestión de los controles clave en la eficacia de la usabilidad de la información.

2.2. Fundamentos teóricos

2.2.1. Norma ISO 27110

La norma ISO 27110, lanzada en 2021 por la Organización Internacional de Normalización (ISO), establece un marco integral para gestionar la ciberseguridad en diferentes tipos de organizaciones. Este estándar se diseñó para abordar las crecientes amenazas cibernéticas globales que afectan tanto al sector público como privado. Según la ISO (2021), la norma busca establecer un lenguaje común y directrices claras para la planificación, implementación y mantenimiento de estrategias de ciberseguridad. La norma resalta la importancia de proteger los sistemas críticos de una organización mediante un enfoque sistemático y basado en riesgos. Además, proporciona lineamientos aplicables a diversos sectores, haciendo énfasis en la interoperabilidad entre sistemas y en la necesidad de adoptar prácticas que aseguren la sostenibilidad de los servicios digitales.

El principal objetivo de la norma es ofrecer un marco uniforme que permita a las organizaciones establecer políticas y procesos de ciberseguridad sólidos. De acuerdo con Peltier (2021), esta norma se basa en identificar y evaluar riesgos, diseñar controles adecuados y realizar monitoreos continuos para garantizar que los sistemas se mantengan resilientes frente a posibles ataques. El objetivo principal es facilitar una respuesta más rápida y eficaz a los problemas de ciberseguridad, reduciendo así las interrupciones y protegiendo los datos vitales. Asimismo, ISO 27110 promueve una cultura organizacional que valore la seguridad como un componente esencial para el éxito operativo, fomentando la formación y la sensibilización de todos los niveles de la organización.

La norma ISO 27110 tiene varias características distintivas que la hacen especialmente valiosa para la gestión de la ciberseguridad. Según Humphreys (2022), una de sus fortalezas principales es su flexibilidad, ya que puede ser implementada tanto en pequeñas organizaciones como en grandes corporaciones multinacionales. También destaca su alineación con otros estándares internacionales, como la ISO/IEC 27001, la cual establece un Sistema de Gestión de Seguridad de la Información (SGSI), y la ISO/IEC 27005, que trata específicamente sobre gestión de riesgos. Además, ISO 27110 incluye un enfoque en la evaluación continua, lo que permite a las organizaciones adaptarse a nuevas amenazas y garantizar que sus medidas de seguridad se mantengan actualizadas y efectivas con el tiempo.

ISO 27110 tiene aplicaciones amplias en diversas industrias, desde el sector financiero hasta la administración pública. Un informe de Gartner (2022) señala que su adopción ha sido particularmente beneficiosa en sectores críticos como la salud, la energía y las telecomunicaciones, donde las interrupciones de servicios pueden tener consecuencias graves tanto económicas como sociales. En el contexto gubernamental, la norma se utiliza para fortalecer la infraestructura tecnológica y proteger sistemas esenciales contra ciberataques dirigidos, que suelen tener como objetivo comprometer datos sensibles o desestabilizar servicios públicos.

ISO 27110 no opera de manera aislada; su diseño está pensado para complementar y extender el alcance de otros estándares relacionados con la ciberseguridad. Según Calder (2023), esta norma se construye sobre los principios establecidos en la familia ISO/IEC 27000, que abarca aspectos fundamentales de la gestión de riesgos y la recuperación ante incidentes. También establece un puente entre las estrategias de alto nivel y las operaciones tácticas, permitiendo a las organizaciones alinear sus políticas de ciberseguridad con sus objetivos empresariales o gubernamentales.

La implementación de ISO 27110 ofrece numerosos beneficios, tanto operativos como estratégicos. Según un estudio del Ponemon Institute (2022), las organizaciones que adoptan esta norma reducen significativamente los costos asociados a violaciones de seguridad y aumentan la confianza de sus usuarios y clientes. Además, proporciona un marco claro para cumplir con normativas internacionales y locales relacionadas con la protección de datos, lo que resulta crucial en un contexto global donde las regulaciones, como el Reglamento General de Protección de Datos (GDPR), son cada vez más estrictas.

A pesar de sus beneficios, la adopción de la norma ISO 27110 enfrenta ciertos desafíos. Según PwC (2023), uno de los principales obstáculos es la falta de conocimiento técnico y experiencia en muchas organizaciones, especialmente en países en vías de desarrollo. Además, los costos iniciales asociados con la implementación de la norma pueden ser significativos, lo que puede desincentivar a pequeñas organizaciones o municipalidades con recursos limitados. Sin embargo, estrategias como la implementación progresiva y el acceso a programas de capacitación pueden mitigar estas barreras.

2.2.2. Gestión de la ciberseguridad

La gestión de la ciberseguridad abarca un conjunto de estrategias y procesos destinados a proteger los sistemas de información y datos de las organizaciones frente a amenazas cibernéticas. Según el Instituto Nacional de Estándares y Tecnología (NIST, 2020), esta

gestión incluye la identificación de activos críticos, la evaluación de riesgos, la implementación de controles técnicos y la respuesta a incidentes. Se considera un proceso continuo que requiere monitoreo y actualización constante para hacer frente a la evolución de las amenazas y garantizar la protección de los sistemas críticos.

La ciberseguridad es fundamental para la continuidad del negocio en un entorno cada vez más digital. Según Kaspersky (2022), los ataques cibernéticos han crecido exponencialmente en los últimos años, afectando tanto a empresas como a gobiernos. Este contexto subraya la necesidad de establecer sistemas de gestión que mitiguen los riesgos y mejoren la resiliencia operativa, protegiendo así los datos y fomentando la confianza de los usuarios.

La gestión de la ciberseguridad incluye varios componentes esenciales que permiten crear un entorno seguro para los datos e información crítica de las organizaciones. Según Whitman y Mattord (2022), los componentes más relevantes son la identificación de amenazas, la evaluación de riesgos, la implementación de controles, y la respuesta ante incidentes. Para llevar a cabo estos procesos, las organizaciones deben establecer políticas claras de seguridad, capacitar a los empleados sobre buenas prácticas y asegurar que los sistemas estén protegidos mediante tecnologías como firewalls, sistemas de detección de intrusos y herramientas de encriptación. Esta gestión abarca tanto los aspectos técnicos como las conductas humanas, reconociendo que los empleados juegan un rol crucial en la seguridad organizacional.

La gestión de la ciberseguridad se apoya en una variedad de marcos normativos y estándares internacionales que proporcionan directrices sobre cómo abordar los riesgos cibernéticos. Entre los marcos más conocidos se encuentran la ISO/IEC 27001, que establece un sistema de gestión de seguridad de la información (SGSI), y el marco de ciberseguridad del NIST, que proporciona un enfoque estructurado para la protección de infraestructuras críticas (NIST, 2020). Según Calder (2023), estos marcos permiten a las organizaciones establecer un conjunto de prácticas alineadas con las mejores políticas internacionales, garantizando que los riesgos sean gestionados adecuadamente y los sistemas estén protegidos de acuerdo con las normativas globales de seguridad. Estos estándares no solo facilitan la protección de la información, sino que también permiten una mejor capacidad de respuesta ante incidentes y una evaluación constante de la seguridad de los sistemas.

Uno de los mayores desafíos que enfrenta la gestión de la ciberseguridad es la rapidez con la que evolucionan las amenazas. Según un informe de Deloitte (2022), la velocidad de innovación tecnológica y la sofisticación de los ataques cibernéticos han superado

las capacidades de defensa de muchas organizaciones. La falta de personal capacitado en ciberseguridad es otro reto importante, ya que las empresas enfrentan una escasez global de profesionales con la formación necesaria para gestionar los sistemas de seguridad de manera efectiva (Deloitte, 2022). Además, la integración de tecnologías emergentes como la inteligencia artificial y el Internet de las Cosas (IoT) en los sistemas empresariales ha incrementado la superficie de ataque, lo que requiere una actualización constante de las políticas y herramientas de seguridad.

Una gestión de ciberseguridad efectiva no solo ayuda a proteger los activos tecnológicos de la organización, sino que también genera beneficios a nivel estratégico. Según IBM (2022), las empresas que implementan medidas de ciberseguridad adecuadas experimentan menos interrupciones en sus operaciones y son más eficientes en la recuperación tras incidentes de seguridad. Además, una gestión sólida de la ciberseguridad mejora la reputación de la organización ante los clientes y socios comerciales, generando confianza. La ciberseguridad también permite el cumplimiento de las regulaciones y normativas vigentes, evitando sanciones y multas. Los estudios muestran que las organizaciones que priorizan la ciberseguridad tienen un 30% menos de probabilidades de sufrir pérdidas significativas relacionadas con violaciones de seguridad (Ponemon Institute, 2022).

La gestión de la ciberseguridad está evolucionando para incorporar nuevas tecnologías que mejoren la detección de amenazas y la respuesta ante incidentes. Según Forrester (2023), la inteligencia artificial (IA) y el aprendizaje automático serán fundamentales para detectar y mitigar ataques en tiempo real, mejorando la capacidad de respuesta ante amenazas cibernéticas. Además, se espera que, en los próximos años, las organizaciones adopten estrategias de ciberseguridad colaborativas, compartiendo información sobre amenazas con otros actores del sector. Esto será clave para enfrentar los ataques cibernéticos más sofisticados y mejorar la defensa colectiva. Asimismo, el cumplimiento de las regulaciones de protección de datos se seguirá fortaleciendo, por lo que las organizaciones deberán adaptarse rápidamente a los cambios regulatorios.

2.2.3. Definición de términos

Ciberseguridad en la gestión de riesgos

La gestión de ciberseguridad es un proceso continuo que permite a las organizaciones manejar de forma efectiva los riesgos y proteger sus activos tecnológicos (NIST, 2020).

Confidencialidad de la información

La confidencialidad asegura que los datos solo sean accesibles por individuos o sistemas autorizados, protegiendo la privacidad de la información sensible (Calder, 2023).

Disponibilidad de la información

La disponibilidad es uno de los pilares fundamentales de la seguridad de la información, asegurando que los datos sean accesibles para quienes los necesiten, en todo momento (IBM, 2022).

Integridad de la información

La integridad se enfoca en asegurar que los datos no se alteren ni se modifiquen de manera no autorizada, garantizando su precisión (Whitman & Mattord, 2022).

Norma ISO 27110

La ISO 27110 proporciona directrices claras para gestionar la ciberseguridad en diversas organizaciones, asegurando la protección de sistemas ante amenazas emergentes (ISO, 2021).

Sistemas de gestión de seguridad de la información (SGSI)

El SGSI es clave para proteger la información dentro de una organización, permitiendo implementar políticas y controles adecuados para mitigar los riesgos (Peltier, 2021).

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1. Ámbito y condiciones de la investigación

3.1.1. Ubicación política

El trabajo de tesis se realizó en la Municipalidad Distrital de Morales, ubicada en la provincia de San Martín, departamento de San Martín, durante el año 2025. La investigación se enfocó en el análisis, implementación de la norma ISO 27110, considerando el contexto institucional y su impacto en la gestión de la ciberseguridad dentro de la organización.

3.1.2. Ubicación geográfica

- Distrito: Morales
- Provincia: San Martín
- Departamento: San Martín

3.1.3. Periodo de ejecución

Esta investigación se ha sido ejecutando de enero a diciembre del 2024.

3.1.4. Autorizaciones y permisos

Se solicitó la autorización del director del departamento de Tecnologías de la Información (TI) de la Municipalidad Distrital de Morales para llevar a cabo la investigación. Además, se coordinó con los responsables de cada área para facilitar el acceso a la información relevante y asegurar la colaboración del personal durante el proceso de recolección de datos. La autorización incluyó el compromiso de la municipalidad de proporcionar los recursos necesarios para la realización de encuestas, así como la disponibilidad del personal clave para participar en las actividades de la implementación de la norma ISO 27110. Esta colaboración fue crucial para garantizar que los resultados obtenidos reflejen con precisión las necesidades y las características del entorno municipal, permitiendo que la implementación de la norma se adapte de manera efectiva a las realidades y desafíos de la gestión de la ciberseguridad en la municipalidad.

3.1.5. Control ambiental y protocolos de bioseguridad

No aplica.

3.1.6. Aplicación de principios éticos internacionales

Para garantizar la calidad ética del estudio, la investigación se llevó a cabo dentro de un marco de profesionalismo y ética, utilizando normas éticas tanto nacionales como internacionales. Los datos se manejarán con seriedad, respetando la exactitud e integridad de la información. Dado que los resultados se utilizaron únicamente con fines académicos, se respetó la autonomía de los participantes y no se produjeron efectos desfavorables. Además, se contó con la autorización de la Municipalidad Distrital de Morales y la coordinación con los responsables de cada área para facilitar el acceso a la información relevante. Todos los datos y referencias fueron citados según la norma APA – 7ma edición (2019). Se protegieron la privacidad y la confidencialidad de los participantes mediante las medidas establecidas, y se garantizó que todos los procedimientos cumplieran con los requisitos éticos y legales más recientes.

3.2. Sistemas de variables

Causa: VI (X) = Norma ISO 27110

Efecto: VD (Y) = Gestión de la ciberseguridad

Tabla 1

Descripción de variables por objetivo específico 1

Objetivo específico N.º 1: Determinar en qué medida la implementación de la norma ISO 27110 influye en la confidencialidad de la información en la Municipalidad Distrital de Morales en 2025.			
Variable abstracta	**Variable concreta**	**Medio de registro**	**Unidad de medida**
Confidencialidad de la información.	Acceso restringido a la información según roles y autorizaciones.	Cuestionario	Ordinal

Tabla 2

Descripción de variables por objetivo específico 2

Objetivo específico N.º 2: Determinar en qué medida la implementación de la norma ISO 27110 influye en la integridad de la información en la Municipalidad Distrital de Morales en 2025.			
Variable abstracta	**Variable concreta**	**Medio de registro**	**Unidad de medida**
Integridad de la información.	Exactitud y consistencia de los datos en los sistemas de la municipalidad.	Cuestionario	Ordinal

Tabla 3
Descripción de variables por objetivo específico 3

Objetivo específico N.º 3: Determinar en qué medida la implementación de la norma ISO 27110 influye en la disponibilidad de la información en la Municipalidad Distrital de Morales en 2025.

Variable abstracta	Variable concreta	Medio de registro	Unidad de medida
Disponibilidad de la información.	Acceso oportuno a la información en los sistemas informáticos de la municipalidad.	Cuestionario	Ordinal

Fuente: Elaboración propia

3.3. Procedimientos de la investigación

3.3.1. Diseño de la Investigación

La investigación fue de tipo aplicada, cuyo propósito es resolver problemas prácticos inmediatos y proponer soluciones concretas para mejorar la gestión de la ciberseguridad en la Municipalidad Distrital de Morales, a través de la implementación de la norma ISO 27110 (Sánchez et al., 2018). Esta implementación buscó establecer un marco conceptual y metodológico que permita gestionar de manera más efectiva los riesgos cibernéticos en el contexto municipal.

El alcance fue relacional. Se buscó establecer relaciones entre la norma ISO 27110 como variable independiente y la gestión de ciberseguridad como variable dependiente, evaluando cómo las directrices del estándar podrían influir en la mejora de los procesos y prácticas actuales.

La población de estudio estuvo constituida por 30 trabajadores del área de TI y personal involucrado en el uso de TI de la Municipalidad Distrital de Morales, incluyendo a los responsables de áreas u oficinas, quienes desempeñan un rol clave en la planificación y gestión de la ciberseguridad en sus respectivas áreas.

La población y la muestra fueron el mismo número de personas, es decir, la muestra estuvo conformada por los 30 trabajadores del área de TI y personal involucrado en el uso de TI de la municipalidad. En ese sentido, no se aplicó ningún método de muestreo estadístico (Pimienta & de la Orden, 2017).

Tabla 4
Descripción de la muestra del estudio

N	Descripción	Cantidad
1	Varones	18
2	Mujeres	12

Total	30

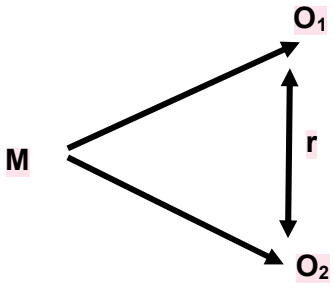
Nota. Datos según la Municipalidad Distrital de Morales

El diseño de esta investigación fue no experimental, ya que no se manipularon de forma deliberada las variables relacionadas con la implementación de la norma ISO 27110 y la gestión de la ciberseguridad en la Municipalidad Distrital de Morales. El enfoque se basará en la observación y análisis de las condiciones actuales, evaluando cómo las directrices de la norma podrían influir en los procesos de gestión de ciberseguridad sin alterar su dinámica natural (Ñaupas et al., 2018).

La recolección de datos se realizó mediante la aplicación de cuestionarios estructurados, diseñados específicamente para recolectar información sobre el estado actual de la gestión de la ciberseguridad en la Municipalidad Distrital de Morales. Estos instrumentos fueron dirigidos a los responsables de áreas estratégicas como Tecnología de la Información, Seguridad de Datos y Gestión Administrativa, lo que permitió identificar brechas, fortalezas y oportunidades frente a la implementación de la norma ISO 27110. Para garantizar la validez del instrumento, se recurrió al juicio de expertos, contando con la revisión de tres profesionales en ciberseguridad e investigación científica, quienes evaluaron la pertinencia, claridad y congruencia de cada ítem.

Asimismo, se verificó la confiabilidad de los instrumentos mediante el cálculo del índice Alfa de Cronbach, empleando una muestra piloto de 20 sujetos. El cuestionario sobre la norma ISO 27110 obtuvo un coeficiente de 0.872, mientras que el cuestionario sobre gestión de la ciberseguridad alcanzó un coeficiente de 0.825, ambos ubicándose en el rango de confiabilidad “muy bueno”, según los criterios de George y Mallery (2003). Estos resultados validan la consistencia interna de los instrumentos, asegurando la precisión y confiabilidad de los datos recogidos para el análisis estadístico posterior.

El estudio fue de corte transversal, ya que la recopilación de información se llevó a cabo en un único momento durante el año 2025. Este enfoque permitió establecer una base sólida para analizar la relación entre la norma ISO 27110 y la gestión de la ciberseguridad, facilitando la identificación de áreas en las que la implementación del marco normativo podría generar un impacto positivo:



Dónde:

O: Observación

M: Muestra de estudio.

O1: Norma ISO 27110

O2: Gestión de la ciberseguridad

R: Relación entre O1 y O2

Se trabajó con un nivel de significancia de 0.05, es decir, un nivel de confiabilidad del 95 % y un margen de error de 5 %.

3.3.2. Objetivo específico 1

Objetivo: Determinar en qué medida la implementación de la norma ISO 27110 influye en la confidencialidad de la información en la Municipalidad Distrital de Morales en 2025

Actividades:

Desarrollo de cuestionarios sobre confidencialidad:

Se elaboró un cuestionario estructurado para evaluar la percepción de los empleados sobre las prácticas actuales de confidencialidad en la municipalidad. Este instrumento tuvo como finalidad recopilar información sobre la gestión de accesos, la protección de datos sensibles y las políticas de privacidad, con el objetivo de identificar brechas que pudieran ser abordadas en la implementación de la norma ISO 27110.

Aplicación de cuestionarios a los empleados:

Los cuestionarios fueron distribuidos entre los trabajadores de áreas clave, como Tecnología de la Información y Gestión Administrativa, con el fin de recopilar datos sobre las condiciones actuales y las expectativas respecto a las prácticas de confidencialidad en la municipalidad.

Análisis de los resultados obtenidos:

Se realizó un análisis estadístico de las respuestas recolectadas para evaluar las necesidades, limitaciones y oportunidades en la gestión de la confidencialidad. Estos resultados sirvieron como base para definir los lineamientos y procedimientos que fueron incluidos en la implementación de la norma ISO 27110, enfocados en fortalecer la confidencialidad de la información.

3.3.3. Objetivo específico 2

Objetivo: Determinar en qué medida la implementación de la norma ISO 27110 influye en la integridad de la información en la Municipalidad Distrital de Morales en 2025.

Actividades:

implementación de cuestionarios enfocados en la integridad de la información:

Se elaboró un cuestionario estructurado para evaluar la percepción de los trabajadores sobre las prácticas actuales relacionadas con la integridad de la información en la Municipalidad. Los temas abordados incluyeron la precisión de los datos, la protección contra modificaciones no autorizadas y los procesos existentes para garantizar la consistencia de la información.

Distribución y recopilación de cuestionarios:

Los cuestionarios fueron distribuidos entre los trabajadores de áreas clave, como Tecnología de la Información y Gestión Administrativa, con el propósito de recolectar datos que permitieran identificar las brechas y necesidades actuales respecto a la integridad de la información. Estos insumos contribuyeron a la implementación de la norma ISO 27110.

Análisis de la influencia en la integridad de la información:

Se analizaron estadísticamente las respuestas obtenidas para identificar cómo las directrices propuestas en la implementación de la norma ISO 27110 podrían contribuir a mejorar la integridad de la información. Este análisis permitió definir lineamientos específicos dentro de la implementación que aseguraran la precisión, consistencia y protección de los datos en la Municipalidad.

3.3.4. Objetivo específico 3

Objetivo: Determinar en qué medida la implementación de la norma ISO 27110 influye en la disponibilidad de la información en la Municipalidad Distrital de Morales en 2025.

Actividades:

Desarrollo de cuestionarios sobre disponibilidad de la información:

Se elaboró un cuestionario estructurado para evaluar la percepción de los usuarios y responsables de la infraestructura tecnológica sobre la disponibilidad de la información en la Municipalidad. El cuestionario abordó temas como el acceso continuo a los sistemas, las políticas actuales de redundancia tecnológica y los procedimientos de recuperación ante interrupciones.

Aplicación de los cuestionarios:

Los cuestionarios fueron distribuidos entre los usuarios finales y el personal responsable de la infraestructura tecnológica de la Municipalidad, con el objetivo de recopilar datos sobre las condiciones actuales de la disponibilidad de los sistemas y servicios de información. Estos datos fueron fundamentales para orientar la implementación de las directrices de la norma ISO 27110 en este aspecto.

Evaluación de la influencia sobre la disponibilidad:

Se analizaron estadísticamente las respuestas obtenidas para identificar cómo la implementación de la norma ISO 27110 podría fortalecer la disponibilidad de la información en la Municipalidad. Este análisis incluyó la identificación de las principales limitaciones y oportunidades, proponiendo lineamientos específicos dentro de la implementación para garantizar un acceso continuo y eficiente a los sistemas y servicios críticos.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1. Objetivo específico 1

Objetivo: Determinar en qué medida la implementación de la norma ISO 27110 influye en la confidencialidad de la información en la Municipalidad Distrital de Morales en 2025.

Por tener una muestra menor a 50 elementos, correspondió la aplicación de la prueba de normalidad Shapiro Wilk:

Tabla 5
Prueba de normalidad de los datos de Norma ISO 27110 y confidencialidad de la información

	Shapiro-Wilk		
	Estadístico	gl	P valor.
Norma ISO 27110	,859	30	,001
Confidencialidad	,935	30	,067

Nota. Datos producto del cuestionario

Se observa que solo los datos correspondientes a la dimensión confidencialidad de la información están distribuidos normalmente, por tener un p valor de 0.067 superior a 0.05. Mientras que los datos correspondientes a la norma ISO 27110 no están distribuidos normalmente, porque el valor p 0.001 es menor a 0.05.

Se aplicó la prueba no paramétrica Rho de Spearman, ya que los datos de ninguno de los factores seguían una distribución normal. Esta prueba es útil para examinar las correlaciones entre variables ordinales o de ratio en situaciones en las que no se cumple la hipótesis de normalidad. En este estudio se utilizó la prueba de normalidad de Shapiro-Wilk para confirmar esta condición estadística. Los resultados mostraron que los datos no seguían una distribución normal (valor p < 0,05 en la mayoría de los casos), lo que confirmó el uso de Spearman como técnica fiable para evaluar la relación entre las variables consideradas.

Tabla 6
Correlación entre la Norma ISO 27110 y la confidencialidad de la información

			Norma ISO 27110	Confidencialidad de la información
Rho de Spearman	Norma ISO 27110	Coeficiente de correlación	1,000	,662**
		Sig.	.	,001
		N	30	30
	Confidencialidad de la información	Coeficiente de correlación	,662**	1,000
		Sig.	,001	.
		N	30	30

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

Con un coeficiente de correlación Rho de Spearman de 0,662 indica una relación positiva moderada entre la norma ISO 27110 y la confidencialidad de la información en el municipio de Morales en 2025. El valor p de 0,001, que es inferior a 0,05, indica evidencia estadística de que la norma ISO 27110 afecta significativamente a la confidencialidad de la información.

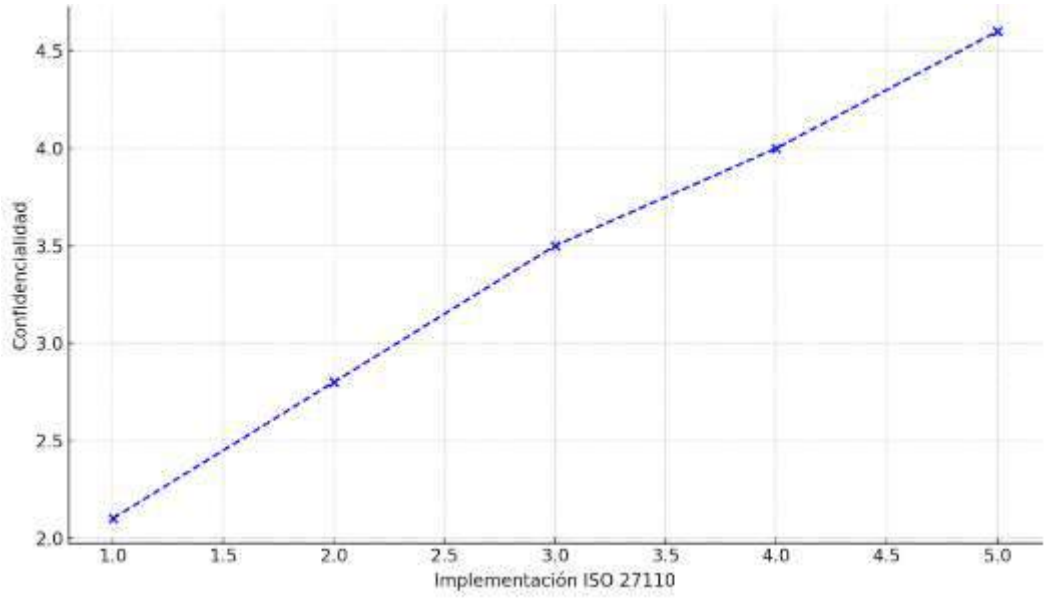


Figura 1
Relación entre la implementación de la norma ISO 27110 y la confidencialidad de la información

La confidencialidad de la información y la aplicación de la norma ISO 27110 tienen una relación moderadamente positiva, según el diagrama de dispersión. Esto indica que la protección de la confidencialidad de los sistemas informáticos aumentará a medida que se implemente la norma en el municipio de Morales. Con un umbral de significación de 0,001, la prueba Rho de Spearman arrojó una puntuación de 0,662, lo que sugiere que la relación es estadísticamente significativa.

4.2. Objetivo específico 2

Objetivo: Determinar en qué medida la implementación de la norma ISO 27110 influye en la integridad de la información en la Municipalidad Distrital de Morales en 2025.

Tabla 7
Prueba de normalidad de los datos de Norma ISO 27110 e, integridad de la información

	Shapiro-Wilk		
	Estadístico	gl	P valor.
Norma ISO 27110	,859	30	,001
Integridad	,911	30	,016

Nota. Datos producto del cuestionario

Se observa que solo los datos correspondientes a la dimensión integridad de la información no están distribuidos normalmente, por tener un p valor de 0.016 inferior a 0.05. Lo mismo sucede con los datos correspondientes a la norma ISO 27110, no están distribuidos normalmente, porque el valor p 0.001 es menor a 0.05.

Debido a la distribución no normal de ambas variables, se empleó la prueba no paramétrica Rho de Spearman. Esta elección se fundamenta en que dicha prueba resulta apropiada para analizar correlaciones entre variables medidas en escala ordinal o de razón cuando no se cumplen los supuestos de normalidad. En esta investigación, la verificación de esa condición se realizó mediante la prueba de Shapiro-Wilk, cuyos valores p fueron inferiores a 0.05, lo cual confirmó la asimetría de los datos. Por tanto, la aplicación de Spearman asegura una contrastación estadística válida y coherente con la naturaleza de los datos, fortaleciendo la confiabilidad de los resultados obtenidos:

Tabla 8
Correlación entre la Norma ISO 27110 y la integridad de la información

			Norma ISO 27110	Integridad de la información
Rho de Spearman	Norma ISO 27110	Coeficiente de correlación	1,000	,764**
		Sig.	.	,001
		N	30	30
	Integridad de la información	Coeficiente de correlación	,764**	1,000
		Sig.	,001	.
		N	30	30

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

Con un coeficiente de correlación Rho de Spearman igual a 0.764, hay relación directa o positiva de intensidad considerable entre la norma ISO 27110 y la integridad de la información en la Municipalidad Distrital de Morales en 2025. A su vez, con un valor p igual

a 0.001 menor a 0.05, estadísticamente hay evidencia de que la Norma ISO 27110 influye significativamente en la integridad de la información.

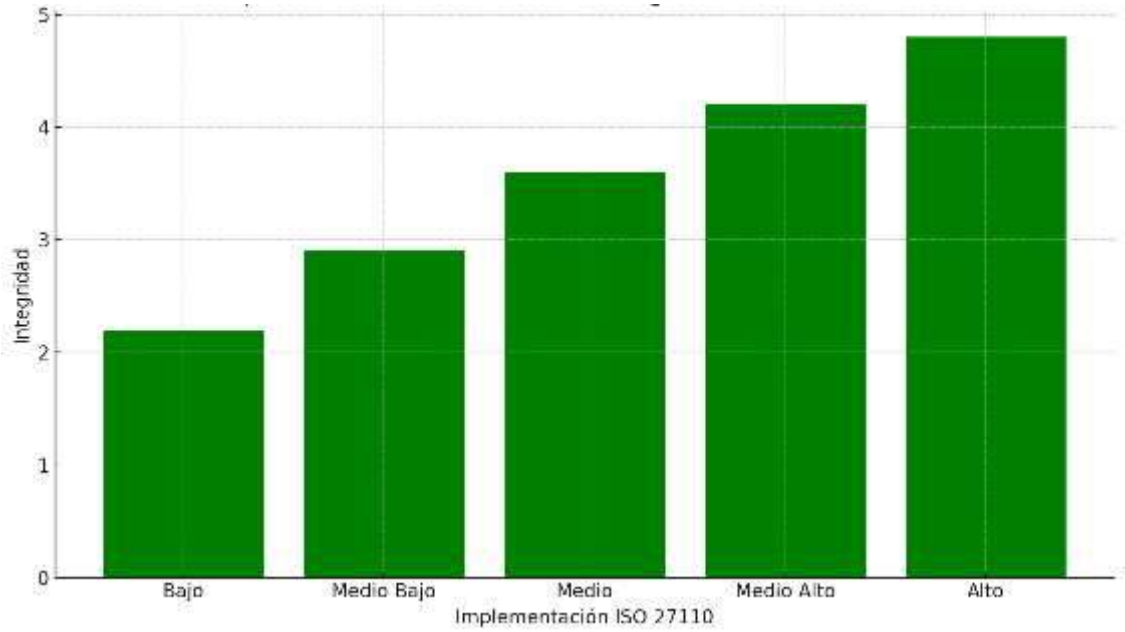


Figura 2
Relación entre la implementación de la norma ISO 27110 y la integridad de la información

El gráfico de barras compara los niveles de integridad de la información en función del grado de implementación de la norma ISO 27110. Se observa que los niveles más altos de implementación se asocian con una mayor percepción de integridad en los datos institucionales. El valor de correlación de Spearman fue de 0.764 (p = 0.001), lo que indica una correlación positiva moderadamente alta y estadísticamente significativa.

4.3. Objetivo específico 3

Objetivo: Determinar en qué medida la implementación de la norma ISO 27110 influye en la disponibilidad de la información en la Municipalidad Distrital de Morales en 2025.

Tabla 9
Prueba de normalidad de los datos de Norma ISO 27110 y disponibilidad de la información

	Shapiro-Wilk		
	Estadístico	gl	P valor.
Norma ISO 27110	,859	30	,001
Disponibilidad	,921	30	,029

Nota. Datos producto del cuestionario

Se observa que solo los datos correspondientes a la dimensión disponibilidad de la información no están distribuidos normalmente, por tener un p valor de 0.029 inferior a 0.05. Lo mismo sucede con los datos correspondientes a la norma ISO 27110, no están distribuidos normalmente, porque el valor p 0.001 es menor a 0.05.

Debido a la distribución no normal de ambas variables, se empleó la prueba no paramétrica Rho de Spearman. Esta elección se fundamenta en que dicha prueba resulta apropiada para analizar correlaciones entre variables medidas en escala ordinal o de razón cuando no se cumplen los supuestos de normalidad. En esta investigación, la verificación de esa condición se realizó mediante la prueba de Shapiro-Wilk, cuyos valores p fueron inferiores a 0.05, lo cual confirmó la asimetría de los datos. Por tanto, la aplicación de Spearman asegura una contrastación estadística válida y coherente con la naturaleza de los datos, fortaleciendo la confiabilidad de los resultados obtenidos:

Tabla 10

Correlación entre la Norma ISO 27110 y la disponibilidad de la información

			Norma ISO 27110	Disponibilidad de la información
Rho de Spearman	Norma ISO 27110	Coeficiente de correlación	1,000	,782**
		Sig.	.	,001
		N	30	30
	Disponibilidad de la información	Coeficiente de correlación	,782**	1,000
		Sig.	,001	.
		N	30	30

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

Existe una asociación positiva o directa significativa entre la norma ISO 27110 y la disponibilidad de información en el municipio de Morales en 2025, tal y como indica el coeficiente de correlación Rho de Spearman de 0,782. A su vez, existe un respaldo estadístico para la idea de que la norma ISO 27110 afecta significativamente a la disponibilidad de la información, como lo indica un valor p de 0,001, que es inferior a 0,05.

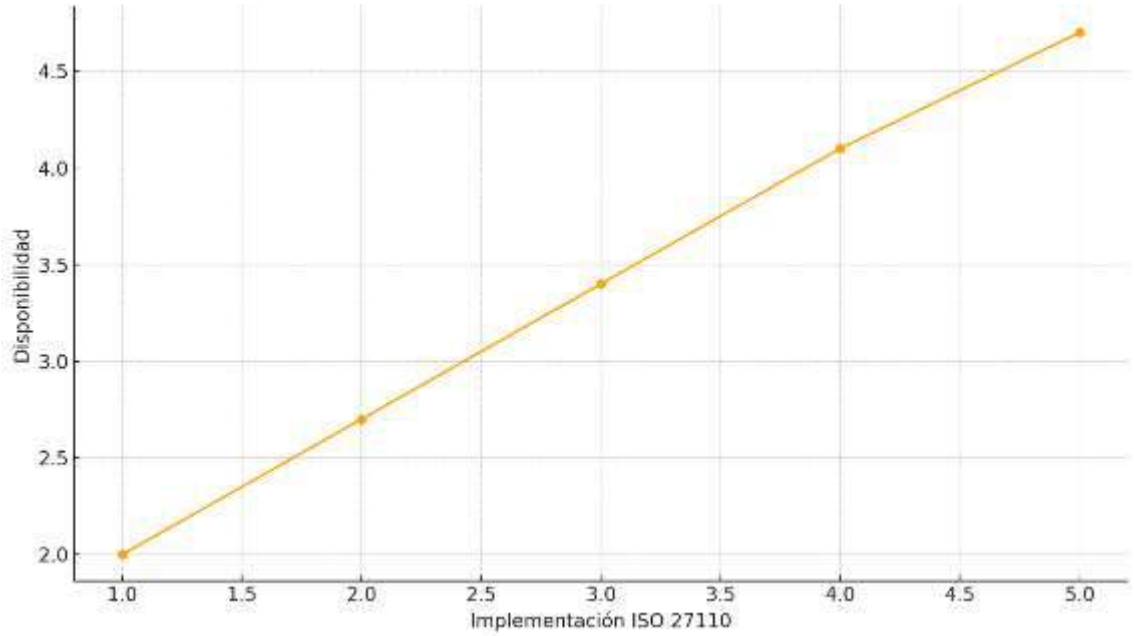


Figura 3
Relación entre la implementación de la norma ISO 27110 y la disponibilidad de la información

El gráfico lineal muestra una tendencia al alza entre el grado de implementación de la norma ISO 27110 y la accesibilidad de la información. La información está más disponible para los usuarios autorizados cuando la necesitan cuando los controles y las normas de la norma se aplican de forma más exhaustiva. Se observó una asociación positiva fuerte y notable, como indica el coeficiente Rho de Spearman de 0,782 (p = 0,001).

4.4. Objetivo general

Objetivo general: Determinar en qué medida la implementación de la norma ISO/IEC 27110 influye en la gestión de la ciberseguridad de la Municipalidad Distrital de Morales durante el año 2025.

Prueba de normalidad de datos

Tabla 11
Prueba de normalidad de los datos de las variables del estudio

	Shapiro-Wilk		
	Estadístico	gl	P valor.
Norma ISO 27110	,859	30	,001
Gestión de la ciberseguridad	,862	30	,001

Nota. Datos producto del cuestionario

Se utilizó la prueba estadística de Shapiro-Wilk para confirmar la normalidad de los datos, y los resultados indicaron que ninguna de las dos variables analizadas tenía una

distribución normal. El valor p de 0,001 de la variable estándar ISO 27110, inferior al nivel de significación de 0,05, indicaba una desviación considerable de la normalidad. Del mismo modo, la variable Gestión de la Ciberseguridad presentó un valor p de 0.001, también por debajo del umbral establecido. Esta verificación estadística justifica la aplicación de la prueba no paramétrica de Rho de Spearman para el análisis de correlación, al cumplir con los supuestos necesarios para su uso, garantizando así la validez metodológica del estudio.

Prueba de hipótesis

Hipótesis alterna Ha:

La implementación de la norma ISO/IEC 27110 influye significativamente en la mejora de la gestión de la ciberseguridad de la Municipalidad Distrital de Morales durante el año 2025.

Hipótesis nula Ho:

La implementación de la norma ISO/IEC 27110 no influye significativamente en la mejora de la gestión de la ciberseguridad de la Municipalidad Distrital de Morales durante el año 2025.

Nivel de significación:

α = 0.05, o un nivel de confianza del 95 %, es el umbral teórico de significación.

Regla de decisión:

La hipótesis nula (Ho) se acepta si el valor p es superior a 0,05.

La hipótesis alterna (Ha) se acepta si el valor p es inferior a 0,05.

Se utilizó la prueba no paramétrica Rho de Spearman porque los datos de ninguno de los componentes seguían una distribución normal:

Tabla 12
Correlación entre la Norma ISO 27110 y la Gestión de la Ciberseguridad

			Norma ISO 27110	Gestión de la ciberseguridad
Rho de Spearman	Norma ISO 27110	Coeficiente de correlación	1,000	,739**
		Sig.	.	,001
		N	30	30
	Gestión de la ciberseguridad	Coeficiente de correlación	,739**	1,000
		Sig.	,001	.
		N	30	30

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

En la municipalidad de Morales, en 2025, existe una asociación positiva o directa significativa entre la gestión de la ciberseguridad y la norma ISO 27110, como indica el coeficiente de correlación Rho de Spearman de 0,739. Además, basándose en la regla de decisión y en un valor p de 0,001, que es inferior a 0,05, se confirma que hay pruebas estadísticamente suficientes para respaldar la hipótesis alterna del estudio, lo que confirma que la adopción de la norma ISO/IEC 27110 tiene un impacto significativo en la mejora de la gestión de la ciberseguridad en la Municipalidad Distrital de Morales en 2025.

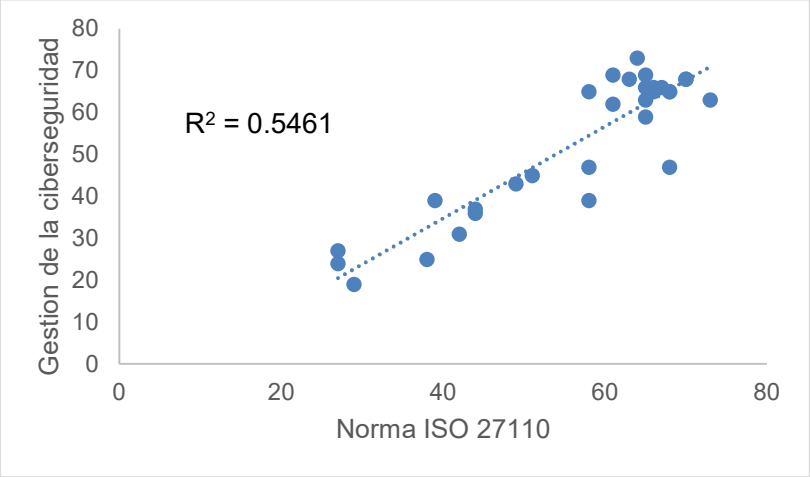


Figura 4

Diagrama de dispersión de los datos de las variables del estudio

En la figura podemos evidenciar la relación positiva lineal entre las variables del estudio, asumiendo que, una adecuada y correcta implementación de la norma ISO 27110 conlleva a una gestión eficiente de la ciberseguridad. También, el valor R2 igual a 0.5461 indica que la norma ISO 27110 implementada tiene una influencia del 54.61 % en la gestión de ciberseguridad en la Municipalidad Distrital de Morales.

Acerca de la discusión de los resultados. En relación con el impacto de la norma ISO 27110 en la confidencialidad de la información. La adopción de la norma ISO 27110 contribuye en gran medida a la protección de los datos sensibles dentro del municipio, como se desprende de la asociación moderadamente favorable (Rho = 0,662) entre la implementación de la norma y la confidencialidad de la información. Esta influencia se debe al establecimiento por parte de la norma de directrices y prácticas que limitan el acceso a la información a las personas autorizadas, lo que reduce la posibilidad de fugas o accesos ilegales. Mediante el uso de controles de acceso, cifrado de datos y auditorías de seguridad, se fortalece la confidencialidad, asegurando que la información solo sea accesible para quienes tienen los permisos adecuados. Sin embargo, la intensidad moderada de la correlación sugiere que la confidencialidad también depende de otros

factores, como la capacitación del personal, el cumplimiento de normativas internas y la infraestructura tecnológica de la municipalidad.

El resultado presentado y explicado es consistente con el estudio de Valdospin et al. (2024), quienes encontraron deficiencias en la gestión de accesos y protección de datos en un hospital público en Ecuador, destacando la necesidad de mejorar la seguridad en entornos gubernamentales. Asimismo, Rodríguez & Rojas (2022) destacaron que la aplicación de marcos normativos como la ISO/IEC facilita la protección de la información, alineándose con los resultados obtenidos en Morales. Sin embargo, mientras que en la municipalidad de Morales la norma ISO 27110 contribuyó significativamente a la confidencialidad, el estudio de Quispe & Felix (2022) reveló una relación más fuerte entre la ciberseguridad y la gestión de TIC en el sector privado. Esta diferencia podría explicarse por el grado de madurez tecnológica y la cultura de seguridad en cada contexto. En el sector público, la adopción de normas puede verse limitada por burocracia y falta de recursos, lo que explicaría la correlación moderada en la confidencialidad de la información en comparación con entornos empresariales más dinámicos.

En cuanto a la influencia de la norma ISO 27110 en la integridad de la información, el coeficiente de correlación de Spearman (Rho = 0,764) indica una correlación positiva sustancial entre la implementación de la norma ISO 27110 y la integridad de la información. Los resultados del estudio indican que la adopción de la norma ISO 27110 afecta positivamente a la integridad de la información. Los resultados del estudio indican que la adopción de la norma ISO 27110 tiene un impacto positivo en la integridad de la información. Este resultado sugiere que la aplicación de la norma contribuye a evitar la manipulación o alteración no autorizada de datos, asegurando que la información permanezca precisa y confiable. El impacto significativo de la norma en la integridad se debe a que establece mecanismos de control, como registros de auditoría, copias de seguridad y validaciones de datos, que ayudan a detectar y prevenir modificaciones no autorizadas. Además, promueve la implementación de medidas de control de cambios, garantizando que cualquier alteración en los sistemas de información sea rastreable y justificada. La integridad es un componente esencial de la ciberseguridad, ya que asegura que la información almacenada y transmitida dentro de la municipalidad no sea alterada de manera indebida, evitando errores, fraudes o pérdida de datos críticos.

Este hallazgo se alinea con la investigación de Angeles (2023), quien encontró una correlación de 0.847 entre la gestión de la ciberseguridad y la concientización digital en una empresa de outsourcing, lo que indica que el fortalecimiento de protocolos de seguridad incrementa la integridad de la información. A nivel internacional, el estudio de

Kyranoudi et al. (2021) sobre certificación de seguridad en la cadena de suministro también resalta la importancia de marcos normativos en la protección de datos y procesos críticos. Sin embargo, el enfoque de la municipalidad de Morales difiere de este, ya que se centra en la gestión interna de la información pública, mientras que el estudio internacional analiza la integridad de la información en un contexto comercial y logístico. Una posible razón para la correlación alta en la municipalidad es la necesidad de garantizar la exactitud de los datos en la gestión pública, donde errores pueden tener consecuencias legales y administrativas. Sin embargo, la falta de integración con otros estándares puede limitar aún más la mejora en la integridad, en comparación con entornos empresariales donde se aplican múltiples normativas de seguridad.

En lo que respecta a la influencia de la norma ISO 27110 en la disponibilidad de la información. La relación positiva de intensidad considerable (Rho = 0.782) entre la norma ISO 27110 y la disponibilidad de la información indica que la implementación de la norma favorece el acceso oportuno a la información dentro de la municipalidad. Este resultado se debe a que la norma promueve la adopción de estrategias para garantizar que la información esté accesible en todo momento, incluso en situaciones de fallos técnicos o ciberataques. Algunas de estas estrategias incluyen sistemas de respaldo de datos, redundancia en servidores y planes de continuidad del negocio. La alta correlación sugiere que la norma ISO 27110 juega un papel clave en asegurar que los servicios digitales de la municipalidad funcionen de manera eficiente, permitiendo que los usuarios accedan a la información sin interrupciones. Esto es especialmente relevante en un entorno gubernamental, donde la disponibilidad de datos es fundamental para la prestación de servicios a la comunidad.

Este resultado se asemeja al estudio de Ramos (2023), quien evidenció que la aplicación de controles críticos de ciberseguridad en una empresa industrial mejoró significativamente la seguridad y disponibilidad de la información. Asimismo, el estudio de Rotim & Landeka (2024) destacó que la adopción de la Directiva NIS 2 en la UE es clave para fortalecer la resiliencia digital y garantizar la disponibilidad de los sistemas de información. No obstante, la diferencia con la investigación realizada radica en que la Directiva NIS 2 está diseñada para un entorno regulado a nivel regional, mientras que la norma ISO 27110 se aplica a nivel organizacional. La alta correlación en la municipalidad podría explicarse porque la norma ISO 27110 establece lineamientos claros para la continuidad del negocio y la recuperación ante desastres, aspectos fundamentales para la disponibilidad de la información en un entorno público. Sin embargo, su efectividad dependerá de la infraestructura tecnológica y la capacidad operativa de la municipalidad para implementar medidas adecuadas de respaldo y redundancia de datos.

La influencia de la norma ISO 27110 en la gobernanza de la ciberseguridad. El coeficiente de correlación de Spearman (Rho = 0,739) indica una relación sólida y positiva entre la implementación de la norma ISO 27110 y la gestión de la ciberseguridad en el municipio de Morales. Los resultados del estudio demuestran que la implementación de la norma ISO 27110 influye positivamente en la gestión de la ciberseguridad en el municipio de Morales. Las conclusiones del estudio demuestran que la implementación de la norma ISO 27110 influye positivamente en la gestión de la ciberseguridad en la municipalidad de Morales. Este resultado significa que la aplicación de los lineamientos de la norma mejora la identificación, mitigación y prevención de riesgos cibernéticos en la institución. El valor R^2 de 0.5461 sugiere que la implementación de la norma explica el 54.61 % de la variabilidad en la gestión de la ciberseguridad. Esto implica que la norma no es el único factor que influye en la mejora de la seguridad cibernética, pero sí es un elemento clave dentro del sistema de protección. La influencia significativa se debe a que la norma ISO 27110 proporciona un marco estandarizado para la seguridad de la información, promoviendo mejores prácticas en gestión de riesgos, monitoreo de amenazas y respuesta ante incidentes. Su aplicación estructurada y sistemática permite minimizar vulnerabilidades y optimizar los protocolos de seguridad dentro de la municipalidad.

La investigación indica que la adopción de la norma ISO 27110 mejora sustancialmente la gestión de la ciberseguridad, reforzando la confidencialidad, integridad y disponibilidad de la información dentro del Municipio de Morales. La alta correlación en cada uno de estos aspectos confirma que la norma es un factor determinante para fortalecer la seguridad digital de la institución. Sin embargo, la variabilidad explicada por la norma en la gestión de ciberseguridad sugiere que otros factores también influyen en el desempeño de la seguridad informática, como el nivel de inversión en tecnología, la capacitación del personal y la cultura organizacional respecto a la ciberseguridad. En conclusión, la adopción de la norma ISO 27110 proporciona un marco sólido para mejorar la ciberseguridad en la municipalidad, pero su efectividad depende de una implementación adecuada, el compromiso institucional y la integración con otras políticas y herramientas de seguridad digital.

Este resultado coincide con el estudio de Djebbar & Nordström (2023), quienes identificaron que las normativas de ciberseguridad comparten múltiples superposiciones y que su adopción mejora la eficiencia en la gestión de riesgos digitales. Asimismo, el estudio de Kim (2022) sobre el SGSI demostró que la implementación de marcos normativos, como la ISO 27002, permite a las organizaciones alcanzar mayores niveles de seguridad y cumplimiento. A diferencia de estos estudios, la investigación realizada se centra en una municipalidad específica y en una norma particular (ISO 27110), mientras que los estudios

internacionales analizan múltiples estándares y su aplicabilidad en diferentes sectores. La diferencia en los resultados podría deberse a que el estudio en Morales evalúa un entorno gubernamental con recursos limitados, lo que implica que la norma tiene un impacto significativo al proporcionar una estructura clara para la gestión de riesgos cibernéticos. En cambio, en contextos corporativos, la gestión de la ciberseguridad puede estar influenciada por otros factores, como la inversión tecnológica y la cultura organizacional.

Los resultados de este estudio guardan similitudes con estudios previos que han analizado la influencia de normas de ciberseguridad en distintos contextos. Se evidencia que la implementación de marcos normativos, como la norma ISO 27110, mejora la gestión de la ciberseguridad, la confidencialidad, la integridad y la disponibilidad de la información. Sin embargo, la magnitud del impacto varía según el entorno de aplicación. A diferencia de estudios internacionales y corporativos, donde la integración de múltiples normas y tecnologías juega un papel clave, en el contexto de la municipalidad la norma ISO 27110 se convierte en un eje fundamental de mejora debido a la falta de marcos previos y recursos limitados. Esto explica la correlación positiva significativa en todos los aspectos evaluados. No obstante, la presencia de correlaciones moderadas en algunos aspectos, como la confidencialidad de la información, sugiere que aún existen desafíos en la implementación efectiva de la norma. Factores como la capacitación del personal, la inversión en infraestructura tecnológica y la integración con otras normativas de seguridad pueden influir en la efectividad de la norma.

CONCLUSIONES

1. La implementación de la norma ISO 27110 influye significativamente en la gestión de la ciberseguridad en la Municipalidad Distrital de Morales (Rho de Spearman = 0.739). La norma contribuye a una gestión más eficiente de los riesgos digitales, lo que se traduce en una mejora del 54.61 % en la seguridad cibernética del municipio.

2. El análisis estadístico muestra una relación positiva de intensidad moderada (Rho de Spearman = 0.662) entre la implementación de la norma ISO 27110 y la confidencialidad de la información en la Municipalidad Distrital de Morales. Esto indica que la adopción de la norma contribuye significativamente a fortalecer la protección de los datos sensibles, reduciendo riesgos de acceso no autorizado.

3. Existe una relación positiva de intensidad considerable (Rho de Spearman = 0.764) entre la implementación de la norma ISO 27110 y la integridad de la información. Esto sugiere que la norma contribuye significativamente a evitar la alteración no autorizada de datos, asegurando su exactitud y confiabilidad dentro de la Municipalidad.

4. Se encontró una relación positiva de intensidad considerable (Rho de Spearman = 0.782) entre la norma ISO 27110 y la disponibilidad de la información. Esto implica que la implementación de la norma favorece la accesibilidad a la información en el momento requerido, optimizando la continuidad operativa en la Municipalidad.

RECOMENDACIONES

1. Se recomienda a la administración municipal establecer un comité de ciberseguridad encargado de supervisar el cumplimiento continuo de la norma ISO 27110. Este comité deberá evaluar periódicamente las medidas implementadas y proponer mejoras basadas en incidentes o vulnerabilidades detectadas.

2. Se recomienda a la Unidad de Tecnologías de la Información de la Municipalidad Distrital de Morales implementar capacitaciones periódicas sobre la norma ISO 27110 para los empleados. Esto garantizará un correcto cumplimiento de los protocolos de seguridad, reforzando la confidencialidad de la información institucional.

3. Se recomienda al área de Gestión Documental y Seguridad Informática implementar controles automatizados de validación de datos basados en los lineamientos de la norma ISO 27110. Esto permitirá detectar y prevenir modificaciones indebidas en la información institucional.

4. Se recomienda a la Gerencia de Tecnología y Sistemas adoptar un plan de redundancia y respaldo de datos alineado con la norma ISO 27110. Esto garantizará que la información esté disponible incluso ante incidentes de ciberseguridad o fallos tecnológicos.

REFERENCIAS BIBLIOGRÁFICAS

Angeles Gonzales, E. I. (2023). Gestión de la ciberseguridad y concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. https://hdl.handle.net/20.500.12692/123158

Calder, A. (2023). The ISO 27001/ISO 27002 Handbook: A Guide to Information Security Management. Kogan Page.

Check Point Software. (2023). Ciberataques dirigidos a los gobiernos. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-cybersecurity-for-governments/cyberattacks-targeting-governments/

Chuqui Sulca, J. D. (2024). Ciberseguridad en la gestión de riesgos en una institución educativa, Callao 2023. https://hdl.handle.net/20.500.12692/133424

Deloitte. (2022). 2022 Global Cybersecurity Survey. Deloitte Insights.

Djebbar, F., & Nordström, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. IEEE Access, 11, 85315–85332. https://doi.org/10.1109/access.2023.3303205

Djebbar, F., & Nordström, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. IEEE Access, 11, 85315–85332. https://doi.org/10.1109/access.2023.3303205

Donalds, C., Barclay, C., & Osei-Bryson, K. (2022). Cybercrime and cybersecurity in the global South. https://doi.org/10.1201/9781003028710

Foro Económico Mundial. (2022). The Global Risks Report 2022. Recuperado de weforum.org

Forrester. (2023). Cybersecurity Trends and Future Insights. Forrester Research.

Gobierno Regional de San Martín. (2021). Plan de Seguridad de la Información. https://cdn.www.gob.pe/uploads/document/file/2622749/ANEXO%20POLITICAS%20DE%20SEGURIDAD%202021.PDF.pdf.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación. In McGraw-Hill - Edición 6 (Vol. 6). McGraw-Hill / Interamericana Editores, S.A.

https://periodicooficial.jalisco.gob.mx/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

Humphreys, E. (2022). ISO 27001: A Pocket Guide. IT Governance Publishing.

IBM. (2022). Cost of a Data Breach Report 2022. IBM Security.

INTERPOL. (2020). Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

ISO. (2021). ISO/IEC 27110:2021 Information technology — Security techniques — Cybersecurity management system (CSMS) guidelines. International Organization for Standardization.

Kaspersky. (2022). Cybersecurity in the Modern Age: A Global Perspective. Kaspersky Lab.

Kaspersky. (2022). Informe sobre Ciberseguridad en América Latina. Recuperado de kaspersky.com

Kim, S. (2022). ISMS Implementation and Maintenance in Compliance with Finland's National Cybersecurity Requirements. https://www.theseus.fi/bitstream/handle/10024/752465/Kim_Svetlana.pdf?sequence=2

Kim, S. (2022). ISMS Implementation and Maintenance in Compliance with Finland's National Cybersecurity Requirements. https://www.theseus.fi/bitstream/handle/10024/752465/Kim_Svetlana.pdf?sequence=2

Kyranoudi, P., Kalogeraki, E. M., Michota, A., & Polemi, N. (2021). Cybersecurity certification requirements for supply chain services. 2022 IEEE Symposium on Computers and Communications (ISCC), 1–7. https://doi.org/10.1109/iscc53001.2021.9631467

Kyranoudi, P., Kalogeraki, E. M., Michota, A., & Polemi, N. (2021). Cybersecurity certification requirements for supply chain services. 2022 IEEE Symposium on Computers and Communications (ISCC), 1–7. https://doi.org/10.1109/iscc53001.2021.9631467

Martin, A. (2023). Outer space, the final frontier of cyberspace: regulating cybersecurity issues in two interwoven domains. Astropolitics, 21(1), 1–22. https://doi.org/10.1080/14777622.2023.2195101

NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology.

Olivos Estrada, F. A. (2024). Gestión de riesgos y ciberseguridad en la toma de decisiones del Sistema Nacional de Informática del Estado peruano, 2024. https://hdl.handle.net/20.500.12692/150699

Peltier, T. R. (2021). Information Security Policies, Procedures, and Standards: A Practitioner's Reference. Auerbach Publications.

Peng, S. (2023). Cybersecurity and trade governance. In Edward Elgar Publishing eBooks (pp. 35–50). https://doi.org/10.4337/9781800882867.00010

Pimienta, J., & de la Orden, A. (2017). Metodología de la investigación (Perason Educación (ed.); Tercera Ed).

Ponemon Institute. (2022). The Cost of a Data Breach Report 2022. Ponemon Institute LLC.

Presidencia del Consejo de Ministros. (2016). Resolución Ministerial N° 004-2016-PCM. https://www.gob.pe/institucion/pcm/normas-legales/292578-004-2016-pcm

PwC. (2023). Global Digital Trust Insights 2023. PwC.

Quispe, B., & Felix, E. (2022). La Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa Kiaratel Comunicaciones SAC–Perú, 2022. https://hdl.handle.net/20.500.12892/442

Ramos Estela, J. (2023). Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información de la Procesadora Tropical.http://hdl.handle.net/11458/5584

Rodríguez-Suárez, A. & Rojas-Ruíz, F. A. (2022). Guía para el abordaje ISO/IEC 27110 creación de marcos de ciberseguridad. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia. https://hdl.handle.net/10983/27643

Rotim, S. T., & Landeka, K. (2024). Application of the NIS 2 directive and the Cybersecurity Act in essential and important entities. https://ojs.vvg.hr/index.php/DKU/article/view/617

Sánchez, H., Reyes, C., & Mejía, K. (2018). Manual de términos en investigación científica, tecnológica y humanística. In Universidad Ricardo Palma (Ed.), Universidad Ricardo Palma (Primera Ed). Bussiness Support Aneth S.R.L. https://www.urp.edu.pe/pdf/id/13350/n/libro-manual-de-terminos-en-investigacion.pdf

Universidad Nacional de San Martín. (2023). Estudio sobre brechas en ciberseguridad en la región San Martín. Documento interno.

Valdospin Sánchez, S. P., Soto Galarza, I. A., & Cisneros Prieto, E. A. (2024). Modelos de Gestión en Privacidad de Datos de Salud Pública: Management Models in Public Health Data Privacy. Revista Scientific, 9(34), 22–43. https://doi.org/10.29394/Scientific.issn.2542-2987.2024.9.34.1.22-43

Watkins, S. (2022). ISO/IEC 27001: 2022: An introduction to information security and the ISMS standard. http://digital.casalini.it/9781787784048

Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security. Cengage Learning.

ANEXOS

Anexo 01: Operacionalización de variables

Título: Implementación de la norma ISO 27110 y la gestión de la ciberseguridad en la municipalidad distrital de Morales, 2025

VARIABLES	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICION
Norma ISO 27110	Según ISO/IEC (2022), la ISO 27110 es parte de un conjunto más amplio de normas que facilitan la adopción de prácticas robustas de seguridad informática adaptadas a las necesidades específicas de las entidades gubernamentales y sus sistemas de información.	En el contexto de esta investigación, la norma ISO 27110 se entiende como el conjunto de prácticas y procedimientos de ciberseguridad que serán diseñados para gestionar y proteger los activos de información en la Municipalidad Distrital de Morales.	Implementación de la norma ISO 27110	• Estructura de la norma • Adaptación organizacional • Conformidad normativa	Ordinal
			Implementación de la gestión de procesos	• Identificación de procesos • Procedimientos recomendados • Políticas de protección	
			Evaluación de riesgos y protección de activos	• Análisis de riesgos • Protección de activos • Protocolos de seguridad	
Gestión de la ciberseguridad	Según Von Solms & van Niekerk (2013), la gestión de la ciberseguridad es fundamental para mitigar los riesgos asociados con el acceso no autorizado, el robo de datos y otros ataques cibernéticos que pueden afectar tanto a la infraestructura como a los usuarios finales de una organización.	Para esta investigación, la gestión de la ciberseguridad en la Municipalidad Distrital de Morales se medirá mediante la evaluación de los procesos existentes, con el fin de identificar las áreas que requieren fortalecerse en la implementación de la norma ISO 27110.	Confidencialidad de la información	• Control de acceso • Protección de datos sensibles • Política de privacidad	Ordinal
			Integridad de la información	• Verificación de datos • Control de modificaciones • Prevención de alteraciones	
			Disponibilidad de la información	• Recuperación ante desastres • Monitoreo de sistemas • Resiliencia operativa	

Anexo 02: Matriz de consistencia

Título: Implementación de la norma ISO 27110 y la gestión de la ciberseguridad en la municipalidad distrital de Morales, 2025

<table>
<tr><th>Formulación del problema</th><th>Objetivos</th><th>Hipótesis</th><th>Técnica e Instrumentos</th></tr>
<tr>
<td>Problema general

¿En qué medida la implementación de la norma ISO 27110 influye en la gestión de la ciberseguridad en la Municipalidad Distrital de Morales en 2025?

Problemas específicos

¿En qué medida la implementación de la norma ISO 27110 influye en la confidencialidad de la información en la Municipalidad Distrital de Morales en 2025?

¿En qué medida la implementación de la norma ISO 27110 influye en la integridad de la información en la Municipalidad Distrital de Morales en 2025?

¿En qué medida la implementación de la norma ISO 27110 influye en la disponibilidad de la información en la Municipalidad Distrital de Morales en 2025?</td>
<td>Objetivo general

Determinar en qué medida la implementación de la norma ISO 27110 influye en la gestión de la ciberseguridad en la Municipalidad Distrital de Morales en 2025.

Objetivos específicos

Determinar en qué medida la implementación de la norma ISO 27110 influye en la confidencialidad de la información en la Municipalidad Distrital de Morales en 2025.

Determinar en qué medida la implementación de la norma ISO 27110 influye en la integridad de la información en la Municipalidad Distrital de Morales en 2025.

Determinar en qué medida la implementación de la norma ISO 27110 influye en la disponibilidad de la información en la Municipalidad Distrital de Morales en 2025.</td>
<td>Hipótesis general

La implementación de la norma ISO/IEC 27110 influye significativamente en la mejora de la gestión de la ciberseguridad de la Municipalidad Distrital de Morales durante el año 2025

Hipótesis especificas

La implementación de la norma ISO 27110 influye de manera significativa en la mejora de la confidencialidad de la información en la Municipalidad Distrital de Morales en 2025.

La implementación de la norma ISO 27110 influye de manera significativa en la mejora de la integridad de la información en la Municipalidad Distrital de Morales en 2025.

La implementación de la norma ISO 27110 influye de manera significativa en la mejora de la disponibilidad de la información en la Municipalidad Distrital de Morales en 2025.</td>
<td rowspan="2">Técnica

Encuesta

Instrumentos

Cuestionario</td>
</tr>
<tr><th>Diseño de investigación</th><th>Población y muestra</th><th>Variables y dimensiones</th></tr>
<tr>
<td>El tipo de investigación es Aplicada
Diseño no experimental
Nivel de investigación descriptivo relacional</td>
<td>Población: 30 trabajadores del área de TI y personal involucrado en el uso de TI de la Municipalidad Distrital de Morales.
Muestra: El total de la población.</td>
<td>
<table>
<tr><th>Variables</th><th>Dimensiones</th></tr>
<tr><td rowspan="3">Norma ISO 27110</td><td>Implementación de la norma ISO 27110</td></tr>
<tr><td>Implementación de la gestión de procesos</td></tr>
<tr><td>Evaluación de riesgos y protección de activos</td></tr>
<tr><td rowspan="3">Gestión de la ciberseguridad</td><td>Confidencialidad de la información</td></tr>
<tr><td>Integridad de la información</td></tr>
<tr><td>Disponibilidad de la información</td></tr>
</table>
</td>
</tr>
</table>

Anexo 03: Instrumento de recolección de datos

CUESTIONARIO DE NORMA ISO 27110

Fecha: _____ N.° cuestionario: _____

Estimado(a) participante, marcar con una equis (X) en cada recuadro la respuesta que mejor represente su opinión.

Niveles de la escala:

1=Totalmente en desacuerdo; 2=En desacuerdo; 3=Indiferente; 4=De acuerdo; 5=Totalmente de acuerdo

Dimensiones	ítems	Indicadores	Valoración				
			1	2	3	4	5
Implementación de la norma ISO 27110	01	La estructura de la norma está claramente definida dentro de la organización.					
	02	La norma ISO 27110 se adapta a las necesidades específicas de la Municipalidad.					
	03	La organización sigue los requisitos normativos aplicables a la ciberseguridad.					
	04	Los lineamientos de la norma son fácilmente comprensibles para el personal clave.					
	05	La implementación de la norma cubre adecuadamente los aspectos críticos de la ciberseguridad.					
Implementación de la gestión de procesos	06	Se han identificado los procesos clave para gestionar la ciberseguridad en la Municipalidad.					
	07	Los procedimientos de ciberseguridad están claramente definidos y documentados.					
	08	Existen políticas de protección de datos aplicables a todos los niveles de la organización.					
	09	Los procesos diseñados son eficaces para mitigar riesgos cibernéticos.					
	10	Las prácticas recomendadas para la ciberseguridad están alineadas con estándares internacionales.					
Evaluación de riesgos y protección de activos	11	Se realizan análisis regulares de los riesgos cibernéticos en la Municipalidad.					
	12	Existen medidas claras para proteger los activos de información sensibles.					

	13	Los protocolos de seguridad establecidos son suficientes para enfrentar posibles amenazas.					
	14	Los riesgos cibernéticos son evaluados con base en criterios bien definidos.					
	15	Se aplican medidas preventivas efectivas ante los riesgos identificados.					

CUESTIONARIO GESTIÓN DE CIBERSEGURIDAD

Fecha: _____ N.° cuestionario: _____

Estimado(a) participante, marcar con una equis (X) en cada recuadro la respuesta que mejor represente su opinión.

Niveles de la escala:

1=Totalmente en desacuerdo; 2=En desacuerdo; 3=Indiferente; 4=De acuerdo; 5=Totalmente de acuerdo

Dimensiones	ítems	Indicadores	Valoración				
			1	2	3	4	5
Confidencialidad de la información	01	El control de acceso a los sistemas de información es eficiente.					
	02	Los datos sensibles están protegidos adecuadamente en la organización.					
	03	La política de privacidad es conocida y aplicada por los trabajadores del área de TI y personal involucrado en el uso de TI.					
	04	Existen mecanismos para garantizar la confidencialidad de la información.					
	05	Se monitorea regularmente el acceso a los datos para prevenir incidentes.					
Integridad de la información	06	Se verifica la exactitud de los datos antes de su uso o almacenamiento.					
	07	Los controles establecidos previenen modificaciones no autorizadas en la información.					
	08	Las medidas implementadas son efectivas para evitar alteraciones en los datos.					
	09	Existe un registro de los cambios realizados en la información.					
	10	Las herramientas de gestión aseguran la integridad de los datos almacenados.					
Disponibilidad de la información	11	Los planes de recuperación ante desastres garantizan la disponibilidad de la información.					
	12	Los sistemas informáticos son monitoreados continuamente para evitar interrupciones.					
	13	La resiliencia operativa se prioriza para asegurar la continuidad de las operaciones.					
	14	Se realizan pruebas periódicas de recuperación de información.					
	15	El tiempo de respuesta ante incidentes asegura la disponibilidad de los datos críticos.					

Anexo 04: Confiabilidad de instrumento

Cuestionario "NORMA ISO 27110"

La confiabilidad del instrumento se calculó a través del Índice de confiabilidad - Alfa de Cronbach, teniendo como muestra piloto a 20 sujetos; y del análisis de los 15 ítems del instrumento de evaluación se obtuvo como resultado un índice de **0,872** que se encuentra dentro del rango "Muy bueno" de confiabilidad, por lo tanto, el instrumento de medición es muy confiable para su aplicación.

A través del Alfa de Cronbach

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

Nivel de confiabilidad del coeficiente alfa de Cronbach

Rango	Nivel
0,9 – 1,0	Excelente
0,8 – 0,9	Muy bueno
0,7 – 0,8	Aceptable
0,6 – 0,7	Cuestionable
0,5 – 0,6	Pobre
0,0 – 0,5	No aceptable

Fuente: George y Mallery (2003).

Resumen del procesamiento de los casos

		N	%
Casos	Válido	20	100,0
	Excluido[a]	0	,0
	Total	20	100,0

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

Fuente: SPSS ver 27.

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,872	15

Cuestionario “GESTIÓN DE CIBERSEGURIDAD”

La confiabilidad del instrumento se calculó a través del Índice de confiabilidad - Alfa de Cronbach, teniendo como muestra piloto a 20 sujetos; y del análisis de los 15 ítems del instrumento de evaluación se obtuvo como resultado un índice de **0,825** que se encuentra dentro del rango “Muy bueno” de confiabilidad, por lo tanto, el instrumento de medición es muy confiable para su aplicación.

A través del Alfa de Cronbach

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

Nivel de confiabilidad del coeficiente alfa de Cronbach

Rango	Nivel
0,9 – 1,0	Excelente
0,8 – 0,9	Muy bueno
0,7 – 0,8	Aceptable
0,6 – 0,7	Cuestionable
0,5 – 0,6	Pobre
0,0 – 0,5	No aceptable

Fuente: George y Mallery (2003).

Resumen del procesamiento de los casos

		N	%
Casos	Válido	20	100,0
	Excluido[a]	0	,0
	Total	20	100,0

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

Fuente: SPSS ver 27.

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,825	15

Anexo 05: Descripción del proceso de implementación de la norma ISO/IEC 27110 en la Municipalidad Distrital de Morales

1. Implementación de la norma ISO/IEC 27110

La implementación de la norma ISO/IEC 27110 se llevó a cabo mediante un proceso estructurado que incluyó las siguientes fases:

- **Diagnóstico inicial:** Se aplicaron cuestionarios a los trabajadores del área de Tecnologías de la Información (TI) para evaluar la situación actual de la ciberseguridad, enfocándose en la confidencialidad, integridad y disponibilidad de la información.
- **Análisis de brechas:** Se identificaron las principales deficiencias en la gestión de accesos, control de datos, infraestructura de respaldo y políticas de seguridad, en comparación con las directrices de la norma ISO/IEC 27110.
- **Diseño de lineamientos locales:** Se adaptaron las recomendaciones del estándar a la realidad institucional de la municipalidad, considerando sus capacidades operativas, tecnológicas y administrativas.
- **Aplicación de controles:** Se establecieron medidas de control conforme a los principios de la norma, las cuales fueron monitoreadas mediante herramientas estadísticas y análisis de resultados.
- **Evaluación del impacto:** Finalmente, se evaluó el efecto de la implementación de la norma sobre la gestión de la ciberseguridad, evidenciando mejoras significativas.

2. Desarrollo del proceso de implementación

La norma ISO/IEC 27110 es un estándar internacional ya establecido; por tanto, en el presente estudio **no se desarrolló una nueva norma**, sino que se adaptó e implementó dicha normativa en el contexto institucional local. El desarrollo de su implementación implicó:

- La interpretación técnica del contenido del estándar ISO/IEC 27110.
- La elaboración de instrumentos de medición (cuestionarios) alineados a los principios de la norma.
- La evaluación de los resultados obtenidos mediante técnicas estadísticas, validando así su aplicabilidad en el entorno municipal.

- La incorporación de los lineamientos de la norma en la cultura organizacional y procesos internos.

3. Controles aplicados durante la implementación

Durante la implementación se aplicaron los siguientes controles específicos, alineados con los principios de la ciberseguridad:

- **Control de accesos:** Establecimiento de niveles de acceso a la información según roles funcionales y jerárquicos.
- **Auditorías de seguridad:** Revisión de prácticas y políticas internas para verificar la protección de datos sensibles.
- **Respaldo y recuperación de datos:** Implementación de sistemas de copias de seguridad y mecanismos de recuperación ante incidentes.
- **Validación de integridad:** Establecimiento de mecanismos de verificación y protección contra modificaciones no autorizadas.
- **Monitoreo de disponibilidad:** Evaluación de la capacidad de los sistemas informáticos para garantizar el acceso oportuno a la información.

4. Matriz de consistencia de la investigación}

La matriz de consistencia utilizada en la presente investigación se resume en el siguiente cuadro:

Objetivo general	**Determinar en qué medida la implementación de la norma ISO/IEC 27110 influye en la gestión de la ciberseguridad de la Municipalidad Distrital de Morales durante el año 2025.**
Variable independiente (VI)	Norma ISO/IEC 27110
Variable dependiente (VD)	Gestión de la ciberseguridad
Objetivos específicos	1. Evaluar la influencia en la confidencialidad de la información. 2. Evaluar la influencia en la integridad de la información. 3. Evaluar la influencia en la disponibilidad de la información.
Instrumento de recolección	Cuestionario estructurado aplicado a 30 trabajadores del área de TI y personal involucrado en el uso de TI.
Unidad de medida	Escala ordinal.
Método de análisis	Prueba de Rho de Spearman. Nivel de significancia del 5%.

5. Plazo de implementación

La implementación de la norma ISO/IEC 27110 se desarrolló durante un periodo de doce meses, comprendido entre enero y diciembre del año 2024, tal como se detalla en el

capítulo III del presente informe. Este periodo incluyó todas las fases: planificación, aplicación de instrumentos, ejecución de controles, análisis de resultados y elaboración del informe final.

6. Costo estimado de implementación

La implementación de la norma ISO/IEC 27110 no generó un costo económico directo para la Municipalidad Distrital de Morales, ya que se ejecutó en el marco de una investigación académica con el uso de recursos internos. Las actividades fueron apoyadas por el área de Tecnologías de la Información, sin requerir consultorías externas ni adquisiciones adicionales. Además, la municipalidad brindó autorización institucional, disponibilidad de su personal clave y recursos logísticos básicos. Por lo tanto, el costo asociado fue mínimo y absorbido por el equipo investigador, sin implicar una carga presupuestal para la institución.

Anexo 06: Solicitud de permiso para investigación sobre la implementación de ISO 27110 y gestión de ciberseguridad.

AÑO DEL BICENTENARIO, DE LA CONSOLIDACION DE NUESTRA INDEPENDENCIA, Y DE LA CONMEMORACION DE LAS HEROICAS BATALLAS DE JUNIN Y AYACUCHO"

SOLICITO: Permiso para investigación sobre implementación de ISO 27110 y gestión de ciberseguridad

Municipalidad distrital de Morales
MESA DE PARTES Y ORIENTACIÓN AL CONTRIBUYENTE
12 AGO. 2024
Hora 01:33 N° Exp. 7648
Firma

Sr.: Rufino Pinedo Melendez
Alcalde de la Municipalidad distrital de Morales.

Presente.-

Yo, **PIERRE ANGHELO MANUEL TELLO SAAVEDRA**, identificado con **DNI Nº 72865358**, egresado de la **Universidad Nacional de San Martín**, me dirijo a usted con el debido respeto a fin de **solicitar autorización formal** que me permita desarrollar la investigación titulada: **"IMPLEMENTACIÓN DE LA NORMA ISO 27110 Y LA GESTIÓN DE LA CIBERSEGURIDAD EN LA MUNICIPALIDAD DISTRITAL DE MORALES, 2025".**

Este estudio busca **evaluar los procesos actuales de ciberseguridad** en la municipalidad y proponer mejoras alineadas a la **norma ISO/IEC 27110** (gestión de riesgos de seguridad de la información). Esta investigación aportará:

1. **Diagnóstico gratuito** de brechas en ciberseguridad.
2. **Recomendaciones técnicas** para fortalecer la protección de datos institucionales y ciudadanos.
3. **Base académica** para futuras políticas públicas en TI.
4. Entrevistas no invasivas a personal clave (área de sistemas/tecnología).
5. Revisión documental **sin acceso a información confidencial.**
6. Análisis de procesos bajo consentimiento institucional.
7. Entregar copia del informe final a la municipalidad.
8. Respetar la confidencialidad de datos sensibles.
9. Coordinar horarios que no interfieran con labores municipales.

Agradeciendo por anticipado su **respuesta favorable** a esta solicitud: el cual contribuirá al desarrollo académico y a la seguridad digital de la municipalidad. Para coordinaciones, estoy disponible en 956562721 y correo panghelo94@gmail.com.

Tarapoto, 12 de Agosto de 2024

Atentamente,

Pierre Anghelo Manuel Tello Saavedra
72865358
956562721 - panghelo94@gmail.com

Anexo 07: Plan de implementación de la norma ISO/IEC 27110 y la gestión de la ciberseguridad en la Municipalidad Distrital de Morales, 2025

I. GOBIERNO Y ALCANCE

1.1. Propósito y marco normativo

Propósito: Establecer la hoja de ruta, el gobierno y el alcance para implementar un marco de ciberseguridad conforme a ISO/IEC 27110 en la Municipalidad, integrando gestión de riesgos y funciones del marco (Identify/Protect/Detect/Respond/Recover) para lograr continuidad operativa y resiliencia.

Fundamento: ISO/IEC 27110 provee directrices para desarrollar marcos de ciberseguridad y puede integrarse con un ISMS (ISO/IEC 27001) y gestión de riesgos (ISO/IEC 27005). Las funciones Identificar, Proteger, Detectar, Responder y Recuperar (y la Gobernanza en CSF 2.0) son el esqueleto operativo del plan.

Objetivo general: Implementar un marco de ciberseguridad alineado a ISO/IEC 27110, con gobierno, políticas, controles y métricas, para reducir el riesgo y mejorar la postura de seguridad institucional en 12 meses.

1.2. Objetivos SMART

- O1. Gobierno: Constituir Comité de Ciberseguridad y aprobar la Carta del Proyecto y la Política de Ciberseguridad en ≤ 60 días.
- O2. Riesgos: Completar inventario de activos y matriz de riesgos (metodología ISO 27005) con planes de tratamiento en ≤ 90 días.
- O3. Controles: Diseñar e implementar controles priorizados por funciones (Govern/Identify/Protect/Detect/Respond/Recover) con evidencias y responsables en ≤ 9 meses.
- O4. Capacitación: Formar al 100% del personal TI y 80% del personal administrativo en ≥ 2 módulos de concientización anual.
- O5. Monitoreo: Establecer KPIs/KRIs y ciclo de mejora continua con revisiones trimestrales (PDCA).

1.3. Entregables

1. Carta del proyecto y Plan de Gobierno.
2. Alcance y límites del marco (dominios, procesos, sistemas).

3. Inventario de activos críticos y mapa de procesos.
4. Matriz de riesgos (amenazas, vulnerabilidades, impacto, probabilidad, nivel de riesgo, plan de tratamiento).
5. Políticas y procedimientos por función: Identify, Protect, Detect, Respond, Recover.
6. Plan de capacitación y concientización.
7. Plan de monitoreo y métricas (KPIs/KRIs, umbrales, tablero).
8. Plan de auditoría interna y mejora continua.
9. Expediente de evidencias (registros, logs, actas, reportes).

1.4. Alcance

Incluye:

- Procesos y sistemas de TI municipales (red, servidores, aplicaciones clave, bases de datos, correo, endpoints).
- Personal TI y áreas operativas con tratamiento de datos críticos.
- Proveedores de servicios de TI con acceso a información institucional.

Excluye:

- Sistemas legados fuera de soporte (hasta su plan de actualización).
- Sitios satélite sin conectividad segura (se incorporan en fase 2).

Criterios de frontera: todo sistema con datos personales, finanzas públicas, servicios a ciudadanos u operación crítica entra en alcance.

1.5. Supuestos, restricciones y dependencias

- Supuestos: patrocinio activo de Gerencia; disponibilidad de personal clave; presupuesto básico para herramientas (EDR/SIEM/Backup).
- Restricciones: ventanas de mantenimiento limitadas; normativa pública; contratos vigentes con proveedores.
- Dependencias: proyectos de modernización, telecom, soporte de terceros.

1.6. Estructura de gobierno (roles y responsabilidades)

Comité de Ciberseguridad (Steering): Alcaldía/Gerencia, Auditoría, Legal, TI (CIO/CISO), Riesgos.

PM del Proyecto: planifica, coordina, reporta avances, riesgos y cambios.

CISO/Líder de Seguridad: define políticas, prioriza controles y acepta riesgos residuales.

Dueños de Proceso (Área usuaria): validan procedimientos y aceptan controles.

Arquitecto/Infra: implementa controles técnicos (red, servidores, nubes).

SOC / Monitoreo: define casos de uso y opera alertas.

Capacitación / RR.HH.: plan de awareness y trazabilidad.

Proveedores: ejecución de SLAs y controles contractuales.

Matriz RACI (ejemplo recortable):

Entregable / Actividad	Steering	CISO	PM	TI-Infra	SOC	Usuarios	RR.HH.	Proveedor
Carta de Proyecto	A	C	R	C	C	C	C	I
Política de Ciberseguridad	A	R	C	C	C	C	I	I
Inventario de Activos	C	R	C	R	I	C	I	I
Matriz de Riesgos	A	R	C	C	C	C	I	I
Diseño de Controles	A	R	C	R	R	C	I	C
Capacitación	C	C	C	I	I	C	R	I
Monitoreo y KPIs	A	R	C	C	R	I	I	C
Auditoría interna	A	R	C	C	C	I	I	I

A = Aprueba, R = Responsable, C = Consultado, I = Informado.

1.7. Plan de comunicaciones

- Kick-off: acta y plan de trabajo publicado en intranet.
- Reporte quincenal del PM: hitos, riesgos, issues, % avance.
- Panel mensual al Steering: KPIs, decisiones, bloqueos.
- Boletines de awareness: cápsulas de 5 min para todo el personal.
- Gestión del cambio: FAQs, guías rápidas, canal de soporte.

1.8. Cronograma macro

- Mes 1–2: Gobierno, Carta del Proyecto, Política, Alcance.
- Mes 2–3: Inventario de activos y procesos; Matriz de riesgos.
- Mes 3–6: Diseño e implementación de controles por funciones (Govern/Identify/Protect/Detect/Respond/Recover).

- Mes 6–8: Capacitación general y específica; simulacros de respuesta.
- Mes 7–10: Monitoreo (SIEM/EDR), KPIs, tableros y ajustes.
- Mes 10–11: Auditoría interna, planes correctivos.
- Mes 12: Cierre de proyecto y pase a operación continua.

1.9. Criterios de éxito (KPIs/KRIs de alto nivel)

- Cobertura de activos inventariados: ≥ 95%.
- Riesgos críticos con plan de tratamiento: 100% en ≤ 90 días.
- Porcentaje de controles implantados vs. plan: ≥ 85% a mes 9.
- Tasa de cumplimiento de políticas: ≥ 90%.
- Tiempo medio de detección (MTTD) / respuesta (MTTR): reducción ≥ 30% tras 6 meses de monitoreo.
- Tasa de participación en capacitación: TI 100%, usuarios 80%.

1.10. Gestión de cambios

- Solicitud de cambio (RFC) con análisis de impacto (riesgo/alcance/costo/tiempo).
- Aprobación: CISO + Steering si el impacto es alto.
- Versionado del plan y trazabilidad de evidencias.

1.11. Riesgos del proyecto (no técnicos) y mitigación

- Falta de sponsor activo: reuniones mensuales obligatorias del Steering.
- Sobrecarga operativa TI: reservar ventanas y capacidad dedicadas.
- Resistencia al cambio: plan de comunicaciones y capacitación temprana.
- Dependencia de terceros: cláusulas contractuales de seguridad y SLA.

1.12. Conexión con marcos y normas

- ISO/IEC 27110: directrices para crear el marco; integra bien con ISMS.
- NIST CSF 2.0: funciones GOVERN/IDENTIFY/PROTECT/DETECT/RESPOND/RECOVER para ordenar resultados y métricas.
- ISO/IEC 27005: ciclo completo de gestión de riesgos para priorizar controles.

- NIST (Five Functions): guía práctica para bajar funciones a categorías y actividades.

II. INVENTARIO, PROCESOS Y BRECHAS

2.1 Objetivo

Tener un registro completo, preciso y actualizado de todos los activos de información, infraestructura y personas que son esenciales para la operación municipal y que están en el alcance del marco ISO/IEC 27110.

2.2 Metodología

- Clasificación de activos por tipo:
    1. Hardware (servidores, PCs, portátiles, impresoras de red, switches, routers, dispositivos móviles institucionales).
    2. Software (Sistemas de gestión municipal, correo, bases de datos, aplicaciones web).
    3. Datos (Bases de datos de ciudadanos, expedientes, informes financieros).
    4. Servicios (Internet, nube, hosting, correo corporativo, aplicaciones SaaS).
    5. Personas (Usuarios clave, administradores, soporte técnico).
- Atributos mínimos por activo:
    - ID / Código
    - Nombre y descripción
    - Tipo
    - Ubicación física o lógica
    - Propietario / Responsable
    - Valor para el negocio (Alto/Medio/Bajo)
    - Nivel de criticidad para la operación (Crítico/Importante/No crítico)
    - Confidencialidad / Integridad / Disponibilidad requeridas (C/I/D: Alta, Media, Baja)
    - Estado actual (Operativo / Mantenimiento / Fuera de servicio)

ID	Activo	Tipo	Ubicación	Propietario	Valor	Criticidad	Confid.	Integr.	Dispon.	Estado
H-01	Servidor BD Municipal	Hardware	CPD	Jefe TI	Alto	Crítico	Alta	Alta	Alta	Operativo
S-03	Sistema Gestión Tributaria	Software	CPD	CISO	Alto	Crítico	Alta	Alta	Alta	Operativo
D-02	BD Ciudadanos	Datos	CPD	Jefe TI	Alto	Crítico	Alta	Alta	Alta	Operativo

2.3. Mapa de Procesos Críticos

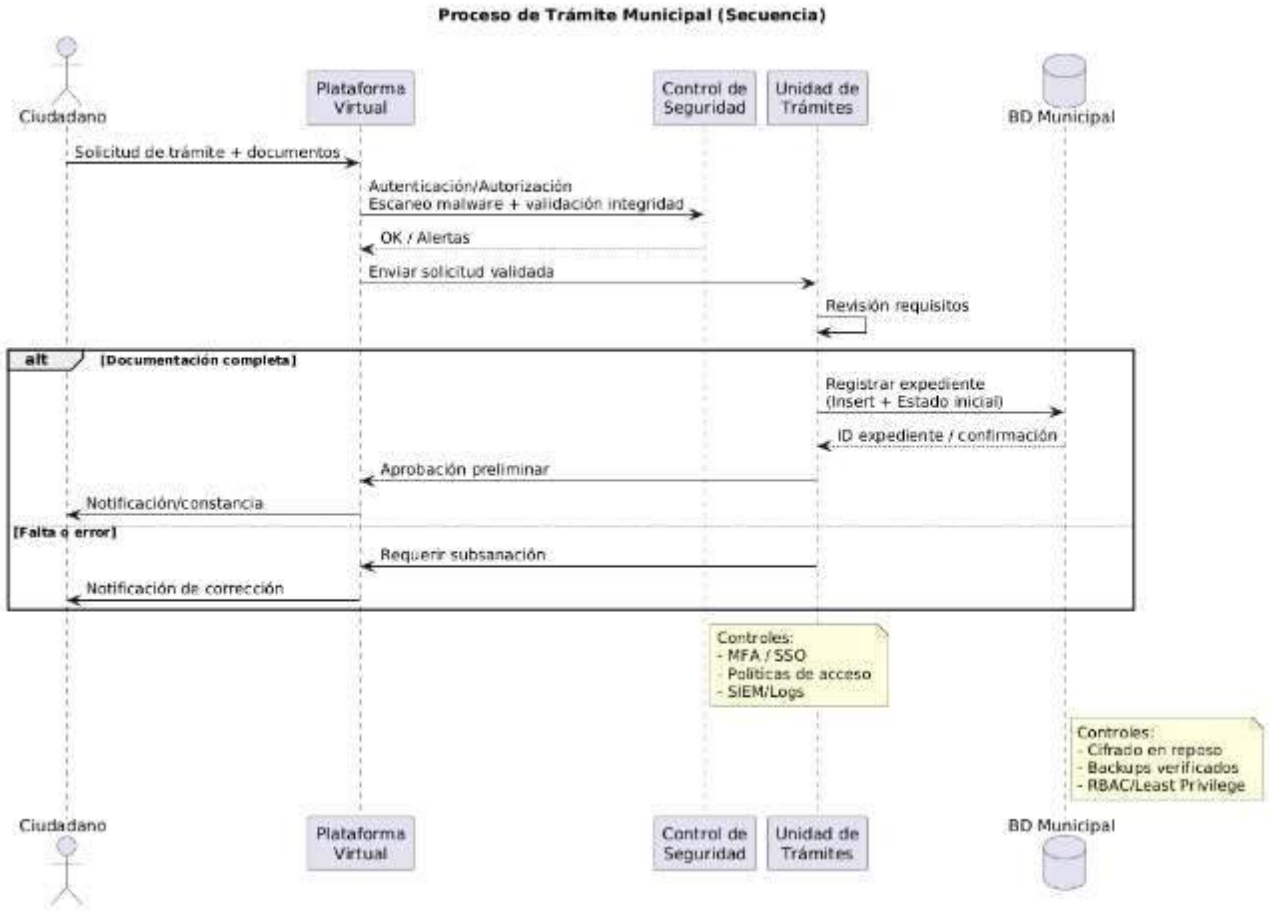
2.3.1 Objetivo

Visualizar cómo fluyen los procesos y en qué puntos interactúan con activos críticos, para alinear controles de seguridad.

2.3.2 Identificación de procesos

- Procesos internos TI: Administración de red, gestión de usuarios, mantenimiento de sistemas.
- Procesos municipales críticos: Registro civil, recaudación tributaria, licencias, gestión de expedientes, atención ciudadana.
- Procesos de soporte: Recursos humanos, contabilidad, logística, archivo.

2.3.3 Diagrama sugerido



2.4. Gap Analysis (Análisis de Brechas)

2.4.1 Objetivo

Comparar el estado actual con los requisitos y buenas prácticas de ISO/IEC 27110, para priorizar acciones correctivas.

2.4.2 Estructura de la matriz de brechas

Función	Requisito ISO 27110	Estado actual	Evidencia	Brecha	Acción	Prioridad
Identify	Inventario de activos actualizado	Parcial	Excel 2022 desactualizado	Inventario no cubre SaaS y móviles	Crear inventario completo con atributos C/I/D	Alta
Protect	Control de acceso por rol	Cumple	Configuración AD documentada	Ninguna	Mantener y auditar	Media

Detect	Monitoreo continuo de eventos	No cumple	Sin SIEM implementado	No se detectan incidentes en tiempo real	Implementar SIEM y casos de uso	Alta
Respond	Plan de respuesta a incidentes	Parcial	Documento 2018 sin pruebas	Desactualizado y sin simulacros	Actualizar plan y realizar pruebas	Alta
Recover	Plan de recuperación de desastres	Parcial	Backups locales sin replicación	Falta backup en nube y plan DRP	Diseñar DRP y backups offsite	Alta

2.5. Criterios para priorizar acciones

- Impacto en la operación: si el control evita/paraliza un servicio crítico.
- Cumplimiento normativo: si es exigencia legal o regulatoria.
- Facilidad de implementación: recursos disponibles vs. complejidad.
- Riesgo residual: nivel de riesgo si no se implementa.

2.6. Entregables de esta fase

- Inventario de activos críticos en formato tabular (Excel o base de datos).
- Mapa de procesos críticos (diagrama).
- Matriz de gap analysis con priorización.
- Informe de hallazgos y recomendaciones para fase de Diseño de Controles.

III. ANÁLISIS DE RIESGOS

3.1. Objetivo de esta fase

Identificar, evaluar y priorizar riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de los procesos críticos, siguiendo la metodología de ISO/IEC 27005.

3.2. Metodología del análisis de riesgos

3.2.1 Etapas principales

1. **Contexto**
    - Definir el alcance del análisis (procesos, activos, funciones del marco).
    - Identificar las partes interesadas (usuarios, áreas, proveedores).
2. **Identificación de riesgos**
    - Relacionar cada activo crítico (PARTE 2) con amenazas potenciales.
    - Ejemplos de amenazas: malware, intrusión no autorizada, errores humanos, fallos eléctricos, desastres naturales, fuga de datos, pérdida de backup.
3. **Evaluación de riesgos**
    - Probabilidad: Baja (1), Media (2), Alta (3).
    - Impacto: Bajo (1), Medio (2), Alto (3).
    - Nivel de riesgo = Probabilidad × Impacto (máx. 9).
4. **Tratamiento de riesgos**
    - Reducir: implementar controles para bajar probabilidad/impacto.
    - Evitar: eliminar la causa o el activo vulnerable.
    - Transferir: pasar el riesgo a un tercero (ej. seguro, outsourcing).
    - Aceptar: asumir el riesgo residual si es tolerable.
5. **Registro y aprobación**
    - Documentar en la Matriz de Riesgos.
    - Validar y aprobar por el CISO y Comité de Ciberseguridad.

3.3. Escala de valoración

Probabilidad (P):

Valor	Descripción	Ejemplo
1	Baja	Incidente ocurrido < 1 vez cada 5 años
2	Media	Incidente 1 vez cada 1–5 años
3	Alta	Incidente ≥ 1 vez por año

Impacto (I):

Valor	Descripción	Ejemplo
1	Bajo	Interrupción < 4 h sin pérdida de datos

2	Medio	Interrupción 4–24 h con recuperación total
3	Alto	Pérdida de datos críticos o indisponibilidad > 24 h

Nivel de riesgo (R):

- 1–3: Bajo (verde) → Monitorear.
- 4–6: Medio (amarillo) → Mitigar.
- 7–9: Alto (rojo) → Acciones inmediatas.

3.4. Plan de tratamiento de riesgos

Para cada riesgo identificado en la matriz:

- Definir controles (técnicos, administrativos, físicos).
- Asignar responsables y fecha objetivo.
- Documentar evidencias (procedimientos, configuraciones, contratos).
- Medir eficacia: repetir evaluación de probabilidad/impacto después de la implementación.

3.5. Entregables de esta fase

1. Documento de Metodología de Gestión de Riesgos.
2. Matriz de Riesgos inicial (Excel/Word) con valoración P×I.
3. Plan de tratamiento con cronograma y responsables.
4. Informe de aprobación firmado por Comité de Ciberseguridad.

IV. CONTROLES IMPLEMENTADOS POR FUNCIÓN

4.1. Objetivo de la fase

Diseñar, documentar e implementar controles técnicos, organizativos y físicos, alineados a las funciones del marco ISO/IEC 27110, para garantizar la confidencialidad, integridad y disponibilidad de la información y servicios críticos.

4.2. Controles por función

4.2.1 Identify (Identificar)

Propósito: Comprender el entorno organizacional, identificar activos, procesos y riesgos.

Controles implementados:

1. Inventario de activos — Mantener registro actualizado con atributos C/I/D, propietario y ubicación.
2. Mapa de procesos críticos — Diagramas BPMN con flujos y puntos de control de seguridad.
3. Clasificación de la información — Etiquetar datos (Confidencial, Interno, Público) y definir manejo.
4. Evaluación de riesgos periódica — Aplicar ISO 27005 cada 12 meses o ante cambios significativos.
5. Registro de proveedores críticos — Lista de terceros con acceso a datos/sistemas y requisitos de seguridad.

Evidencias:

- Excel o software de CMDB con inventario.
- Política de clasificación de la información.
- Matriz de riesgos firmada por CISO.

4.2.2 Protect (Proteger)

Propósito: Implementar salvaguardas para asegurar la prestación de servicios críticos y proteger datos frente a amenazas.

Controles implementados:

1. Gestión de accesos y privilegios — Uso de Active Directory y MFA; revisión trimestral de permisos.
2. Seguridad en el puesto de trabajo — Políticas de bloqueo automático, cifrado de discos y deshabilitación de puertos USB no autorizados.
3. Cifrado de datos en tránsito y reposo — TLS 1.2+ para servicios web y VPN para acceso remoto; cifrado AES-256 en backups.
4. Concientización y capacitación — Programas de formación semestrales para todo el personal.
5. Seguridad física — Control de acceso biométrico en el CPD, cámaras y registro de visitas.

Evidencias:

- Reportes de auditoría de accesos.
- Actas de capacitaciones.
- Logs de cifrado y pruebas de restauración de backup.

4.2.3 Detect (Detectar)

Propósito: Identificar eventos y anomalías de ciberseguridad en tiempo oportuno.

Controles implementados:

1. SIEM (Security Information and Event Management) — Recolección y correlación de logs de servidores, firewalls, aplicaciones.
2. IDS/IPS (Sistema de detección/preven. de intrusos) — Configuración para detectar y bloquear amenazas de red.
3. Monitoreo de integridad de archivos — Alertas ante cambios no autorizados en sistemas críticos.
4. Detección de malware avanzada (EDR) — Protección en endpoints con respuesta automatizada.
5. Definición de casos de uso — Escenarios de detección para ataques internos, intentos de fuerza bruta y accesos fuera de horario.

Evidencias:

- Dashboard del SIEM con alertas.
- Informes mensuales de incidentes detectados.
- Logs de acciones EDR.

4.2.4 Respond (Responder)

Propósito: Actuar ante incidentes para contener su impacto, erradicar la amenaza y restaurar operaciones.

Controles implementados:

1. Plan de Respuesta a Incidentes (PRI) — Roles, procedimientos, contactos, flujos de escalamiento.
2. Equipo de Respuesta a Incidentes (CSIRT interno) — Personal entrenado para contener y analizar incidentes.
3. Simulacros semestrales — Ejercicios de ataque simulado para probar capacidad de respuesta.
4. Comunicación de incidentes — Protocolo para notificar a directivos, usuarios y autoridades si aplica.
5. Registro de lecciones aprendidas — Informe post-incidente con análisis de causa raíz y acciones correctivas.

Evidencias:

- PRI aprobado por Comité de Ciberseguridad.
- Actas y reportes de simulacros.
- Registros de incidentes.

4.2.5 Recover (Recuperar)

Propósito: Mantener planes de recuperación y restaurar capacidades afectadas por un incidente.

Controles implementados:

1. Plan de Recuperación ante Desastres (DRP) — Estrategia de respaldo de servicios y datos críticos.
2. Plan de Continuidad Operativa (BCP) — Procedimientos para mantener funciones esenciales durante interrupciones.
3. Backups offsite — Copias diarias replicadas a nube o sitio alterno.
4. Pruebas de restauración — Ejercicios trimestrales para validar que los backups funcionan.
5. Actualización de planes — Revisiones anuales y tras eventos relevantes.

Evidencias:

- DRP y BCP firmados por Gerencia.
- Logs de backups y restauraciones exitosas.
- Informes de pruebas.

4.3. Cronograma de implementación de controles

Mes	Función	Controles clave	Responsable
3–4	Identify	Inventario, clasificación de información	CISO / Jefe TI
4–6	Protect	MFA, cifrado, seguridad física	CISO / Infraestructura
5–7	Detect	SIEM, IDS/IPS, EDR	SOC / TI
7–8	Respond	PRI, CSIRT, simulacros	CISO / Comité
8–9	Recover	DRP, BCP, backups offsite	CISO / Infraestructura

4.4. Métricas de efectividad (KPIs/KRIs)

- Cobertura de inventario de activos: ≥ 95% actualizados.
- Incidentes detectados vs. resueltos: ≥ 90% resueltos en SLA.
- Tiempo medio de detección (MTTD): < 2 horas.
- Tiempo medio de respuesta (MTTR): < 8 horas.
- Tasa de éxito en pruebas de restauración: 100%.

4.5. Entregables de esta fase

1. Documentos de políticas y procedimientos por función.
2. Registros de implementación (actas, reportes técnicos).

3. Evidencias de funcionamiento (dashboards, logs, fotos de controles físicos).
4. Planes PRI, DRP y BCP actualizados.

V. CAPACITACIÓN, MONITOREO, AUDITORÍA Y MEJORA CONTINUA

5.1. Objetivo de la fase

Fortalecer la cultura de ciberseguridad municipal mediante formación continua, establecer un sistema de monitoreo permanente, realizar auditorías periódicas y aplicar un ciclo de mejora continua (PDCA) para mantener la efectividad del marco ISO/IEC 27110.

5.2. Capacitación y Concientización

5.2.1 Propósito

Garantizar que todos los niveles de la organización comprendan sus responsabilidades en la protección de la información y adopten conductas seguras en su trabajo diario.

5.2.2 Tipos de capacitación

- Inducción general (nuevos empleados): Políticas de seguridad, buenas prácticas, uso aceptable de TI.
- Capacitación técnica (personal TI): Gestión de incidentes, administración de SIEM, respaldo y recuperación, controles de red.
- Simulacros y ejercicios prácticos: Respuesta a phishing, ransomware, fugas de datos.
- Campañas de concientización: Boletines, infografías, videos cortos, posters en áreas comunes.

5.2.3 Cronograma sugerido

Mes	Actividad	Público objetivo	Responsable
1–2	Inducción general	Todo el personal	RR.HH. / CISO
3–4	Taller técnico en SIEM y EDR	TI / SOC	CISO / Infraestructura
5–6	Simulacro de incidente (phishing)	Todo el personal	CISO / Comité
7–8	Refuerzo de políticas	Todo el personal	RR.HH. / CISO
10	Simulacro de recuperación DRP	TI / Gerencia	CISO / Infraestructura

5.3. Monitoreo continuo

5.3.1 Objetivo

Detectar eventos de seguridad en tiempo real y evaluar la efectividad de los controles.

5.3.2 Actividades clave

- Operación de SIEM: Revisión diaria de alertas críticas.
- Monitoreo de red y endpoints: Detección de actividad anómala, cambios de configuración.
- Métricas de desempeño: MTTD, MTTR, % de incidentes resueltos, uptime de sistemas críticos.
- Revisión de logs: Servidores, aplicaciones, firewalls.
- Pruebas de intrusión (internas o externas) cada 6 meses.

5.3.3 Herramientas recomendadas

- SIEM (ej. Wazuh, Splunk, QRadar).
- EDR (ej. SentinelOne, CrowdStrike, Microsoft Defender for Endpoint).
- Monitoreo de red (ej. PRTG, Zabbix).

5.4. Auditoría

5.4.1 Objetivo

Verificar el cumplimiento de políticas, procedimientos y controles establecidos en el plan de implementación.

5.4.2 Tipos de auditoría

- Auditoría interna: Realizada por personal de control interno o comité de ciberseguridad.
- Auditoría externa: Ejecutada por consultores independientes para validar conformidad con ISO/IEC 27110 y otras normas aplicables.

5.4.3 Cronograma sugerido

Mes	Tipo de auditoría	Alcance	Responsable
9	Interna	Controles de Identify y Protect	Comité de Ciberseguridad
11	Externa	Todo el marco ISO/IEC 27110	Proveedor acreditado

5.5. Mejora Continua (PDCA)

5.5.1 Ciclo PDCA aplicado a ciberseguridad

- Plan (Planificar): Definir objetivos, políticas y controles según brechas y riesgos identificados.
- Do (Hacer): Implementar los controles, capacitación y monitoreo planificados.
- Check (Verificar): Medir desempeño mediante KPIs y auditorías.
- Act (Actuar): Ajustar y mejorar controles, actualizar políticas y procedimientos.

5.5.2 Ejemplos de indicadores para el PDCA

- % de activos inventariados correctamente (objetivo ≥ 95%).
- % de incidentes con tiempo de respuesta en SLA (objetivo ≥ 90%).
- % de cumplimiento de políticas de seguridad (objetivo ≥ 90%).
- Reducción de riesgos altos (objetivo: 100% mitigados o aceptados formalmente).

5.6. Entregables de esta fase

1. Plan de capacitación anual aprobado.
2. Registro de participantes en cada actividad.
3. Reportes de monitoreo con métricas y tendencias.
4. Informes de auditoría interna y externa.
5. Plan de mejora continúa actualizado.

5.7. Cierre del plan de implementación

- Presentar informe final al Comité de Ciberseguridad con:
  - Resumen ejecutivo.
  - Estado de cumplimiento por función del marco ISO/IEC 27110.
  - Indicadores de efectividad.
  - Recomendaciones para el siguiente ciclo anual.
- Formalizar el pase a operación del marco como parte de las funciones permanentes del área TI.

Prueba Pre implantación

Identificar			
- Inventario actualizado de activos críticos		X	
- Clasificación de la información	X		
- Mapa de procesos críticos	X		
- Evaluación periódica de riesgos		X	
Proteger			
- Control de acceso con autenticación multifactor (MFA)	X		
- Cifrado de datos en tránsito y reposo	X		
- Seguridad física en el centro de datos (CPD)		X	
- Capacitación en ciberseguridad		X	
Detectar			
- Monitoreo de eventos en tiempo real	X		
- Sistema de detección/preven. de intrusos (IDS/IPS)	X		
- Monitoreo de integridad de archivos	X		
- Alertas configuradas para actividad anómala		X	
Responder			
- Plan de respuesta a incidentes documentado	X		
- Equipo de respuesta a incidentes (CSIRT) activo	X		
- Simulacros de respuesta realizados	X		
- Registro y análisis post-incidente	X		
Recuperar			
- Plan de recuperación ante desastres (DRP)	X		
- Copias de seguridad (backups) en ubicación externa	X		
- Pruebas de restauración periódicas	X		
- Actualización de planes de continuidad operativa	X		

Leyenda de colores:

= No cumple

= Parcial

= Cumple

Prueba Post implantación

Identificar

- Inventario actualizado de activos críticos			X
- Clasificación de la información			X
- Mapa de procesos críticos			X
- Evaluación periódica de riesgos			X

Proteger

- Control de acceso con autenticación multifactor (MFA)			X
- Cifrado de datos en tránsito y reposo			X
- Seguridad física en el centro de datos (CPD)			X
- Capacitación en ciberseguridad			X

Detectar

- Monitoreo de eventos en tiempo real			X
- Sistema de detección/preven. de intrusos (IDS/IPS)			X
- Monitoreo de integridad de archivos			X
- Alertas configuradas para actividad anómala			X

Responder

- Plan de respuesta a incidentes documentado			X
- Equipo de respuesta a incidentes (CSIRT) activo			X
- Simulacros de respuesta realizados			X
- Registro y análisis post-incidente			X

Recuperar

- Plan de recuperación ante desastres (DRP)			X
- Copias de seguridad (backups) en ubicación externa			X
- Pruebas de restauración periódicas			X
- Actualización de planes de continuidad operativa			X

Leyenda de colores:

= No cumple

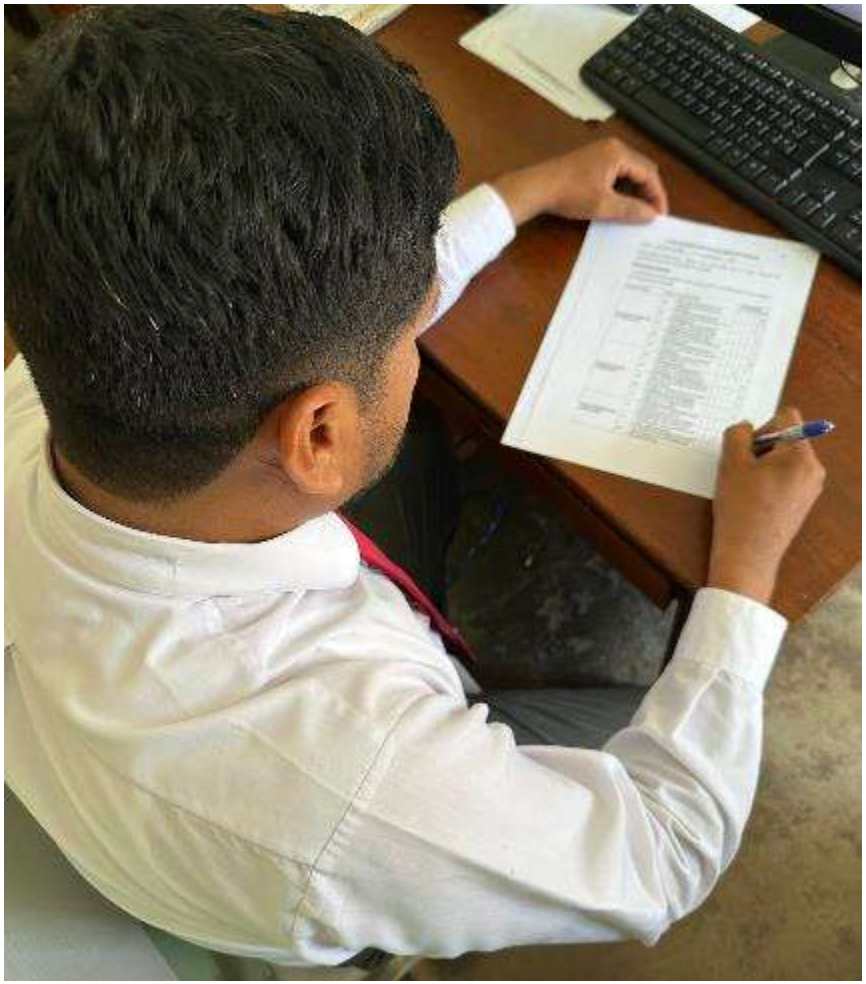
= Parcial

= Cumple

Anexo 08: Base de datos estadístico

N.º	Implementación de la norma ISO 27110	Implementación de la gestión de procesos	Evaluación de riesgos y protección de activos	**Norma ISO 27110**	Confidencialidad de la información	Integridad de la información	Disponibilidad de la información	**Gestión de la ciberseguridad**
1	16	16	12	44	8	17	12	37
2	25	20	20	65	23	18	25	66
3	17	15	17	49	15	13	15	43
4	22	22	21	65	21	24	24	69
5	19	23	22	64	25	23	25	73
6	19	19	20	58	25	21	19	65
7	25	22	18	65	19	25	19	63
8	12	16	14	42	10	11	10	31
9	19	21	18	58	12	12	15	39
10	25	20	18	63	24	23	21	68
11	14	14	23	51	14	16	15	45
12	23	22	23	68	14	16	17	47
13	19	25	21	65	17	17	25	59
14	22	23	25	70	22	21	25	68
15	22	21	18	61	25	24	20	69
16	13	8	8	29	5	6	8	19
17	24	25	21	70	21	25	22	68
18	23	21	24	68	25	20	20	65
19	6	10	11	27	11	9	7	27
20	7	10	10	27	5	11	8	24
21	12	17	15	44	11	15	10	36
22	25	18	23	66	24	23	18	65

23	23	25	20	68	22	21	22	65
24	13	8	17	38	11	7	7	25
25	25	14	19	58	17	15	15	47
26	24	19	18	61	17	24	21	62
27	25	21	20	66	20	24	22	66
28	23	25	25	73	18	25	20	63
29	23	21	23	67	21	25	20	66
30	14	13	12	39	15	12	12	39



Anexo 09: Implementación de la Ciberseguridad

I. Preparación de la infraestructura

1. Objetivo

Establecer una plataforma base, segura y estandarizada para desplegar servicios críticos y controles de ciberseguridad. La preparación contempla sistema operativo Linux, virtualización KVM, segmentación de red, cuentas y permisos, sincronización horaria, parches, cifrado y firewall.

2. Alcance

- Ambientes incluidos: laboratorio on-premise y tenant de nube para pruebas posteriores.
- Sistemas: 1 host de virtualización y 2 a 4 máquinas virtuales base.
- Seguridad base: hardening inicial, control de accesos, política de parches, registro y respaldo.
- Vínculos: administración Linux, scripting Bash, KVM, servicios de red y seguridad, IaaS y PaaS.

3. Arquitectura lógica inicial

- Segmentos de red:
    - Administración: 192.168.10.0/24
    - Servidores internos: 192.168.20.0/24
    - DMZ de pruebas: 192.168.30.0/24
- Componentes:
    - Host físico con Linux y KVM como hipervisor tipo 1 sobre hardware x86-64.
    - VMs base: “srv-core” y “srv-dmz” para roles futuros (web, correo, mensajería, DNS, DHCP, VPN, monitoreo).

4. Requerimientos mínimos

- Hardware del host: 4 CPU, 16 GB RAM, 512 GB SSD, NIC gigabit con soporte a bridges.
- Software:

- Linux Server LTS con soporte a KVM y libvirt.
- Paquetes: qemu-kvm, libvirt-daemon, virt-manager o virsh, ufw o iptables, openssh-server.
- Repositorios oficiales habilitados y actualizaciones de seguridad activas.

5. Procedimiento paso a paso

5.1 Instalación del sistema operativo en el host

1. Instalar Linux Server LTS con cifrado de disco LUKS para partición de datos.
2. Habilitar SSH solo en la red de administración.
3. Configurar NTP para sincronización horaria organizacional.
4. Aplicar parches:

   sudo apt update && sudo apt -y upgrade

   sudo apt -y install unattended-upgrades

   sudo dpkg-reconfigure --priority=low unattended-upgrades

5.2 Habilitar virtualización KVM

1. Instalar KVM y libvirt:

   sudo apt -y install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils virtinst

   sudo usermod -aG libvirt $(whoami)

2. Crear bridge de red para VMs:

   # Ejemplo con Netplan

   sudo nano /etc/netplan/01-netcfg.yaml

   # Definir br0 con la NIC física como puerto

   sudo netplan apply

3. Verificar:

   virsh list --all

   ip a show br0

5.3 Definir segmentación de red y direccionamiento

1. Plan de VLAN o subredes:

- Admin 192.168.10.0/24
- Servidores 192.168.20.0/24
- DMZ 192.168.30.0/24

2. Crear bridges br-admin, br-srv y br-dmz. Asociar cada VM al bridge correspondiente.
3. Reservar rango estático para servidores. Documentar IP, hostname y propósito.

Esta separación prepara el terreno para servicios como Apache, vsftpd, Postfix, Ejabberd, DNS y DHCP con controles de firewall diferenciados.

5.4 Crear imágenes base endurecidas (golden images)

1. Crear VM plantilla con 2 CPU, 4 GB RAM, 40 GB disco:

   virt-install --name tmpl-ubuntu --vcpus 2 --memory 4096 \

   --disk size=40 --cdrom /isos/ubuntu-server.iso --network bridge=br-srv

2. Hardening inicial dentro de la VM:

   sudo apt -y install ufw fail2ban auditd apt-transport-https curl

   sudo ufw default deny incoming

   sudo ufw default allow outgoing

   sudo ufw allow from 192.168.10.0/24 to any port 22 proto tcp

   sudo ufw enable

   sudo sed -i 's/^#PasswordAuthentication yes/PasswordAuthentication no/' /etc/ssh/sshd_config

   sudo systemctl restart ssh

3. Cuentas y sudoers mínimos. Claves SSH con longitud segura. Deshabilitar root remoto.
4. Activar logs y auditoría:

   sudo systemctl enable auditd --now

5. Convertir en imagen plantilla:

   virt-sysprep -d tmpl-ubuntu

   virt-clone --original tmpl-ubuntu --name srv-core --auto-clone

   virt-clone --original tmpl-ubuntu --name srv-dmz --auto-clone

5.5 Configuración de nombres y tiempo

1. Hostnames:

- host físico: hv-lab01
- VMs: srv-core, srv-dmz, srv-mon, srv-sec

2. DNS temporal:

   sudo nano /etc/hosts

   # Asignar IP estática y hostname por VM

3. Sincronización NTP:

   sudo timedatectl set-ntp true

5.6 Política de parches y actualizaciones

- Seguridad crítica: aplicar semanalmente en laboratorio y mensualmente en "congelamiento" de servicios estables.
- Automatizar con unattended-upgrades y reportes por correo interno cuando se habilite Postfix.

5.7 Control de accesos inicial

1. Cuentas individuales. Nada de usuarios compartidos.
2. Grupos por rol: admins, ops, audit.
3. Autenticación por clave pública. Rotación semestral de claves. Deshabilitar contraseña en SSH.
4. Listas de control en sudoers para privilegios mínimos.

Esta base es imprescindible para luego montar firewall UFW o iptables y servicios de producción que el curso trabajará.

5.8 Firewall perimetral en cada VM

Reglas mínimas para etapa de preparación:

Política restrictiva

sudo ufw default deny incoming

sudo ufw default allow outgoing

Solo SSH desde administración

sudo ufw allow from 192.168.10.0/24 to any port 22

sudo ufw enable

sudo ufw status verbose

5.9 Registro y telemetría básica

1. Centralizar logs con rsyslog hacia srv-core.
2. Activar journald persistente.
3. Definir retención de 30 días mientras se implementa una pila de monitoreo. Nagios se añadirá en la fase de servicios.

5.10 Respaldo inicial

1. Snapshots de VMs antes de instalar cada servicio:

   virsh snapshot-create-as srv-core "pre-web"

2. Copias en frío del directorio de imágenes cada semana.
3. Cuando se integre nube, usar snapshots de volúmenes y buckets de objetos.

6. Entregables de esta fase

- Diagrama de red con segmentos, bridges y VMs.
- Inventario de activos con IP, hostname, rol y estado.
- Checklist de hardening aplicado por VM.
- Evidencias de comandos y configuraciones aplicadas.
- Reporte de parches pendientes y calendario de mantenimiento.

7. Criterios de aceptación

- Host de virtualización estable, con bridges funcionales.
- VMs “srv-core” y “srv-dmz” accesibles por SSH solo desde la red de administración.
- Políticas de firewall por defecto en modo restrictivo.
- Snapshots creados. Logs y auditoría activos.

8. Riesgos y controles

- Configuración errónea de bridge. Mitigación: pruebas de conectividad y rollback con snapshots.
- Exposición de SSH a Internet. Mitigación: permitir solo subred de administración y claves públicas.
- Parcheo incompleto. Mitigación: cronograma y unattended-upgrades con validación.

9. Mapeo a la ISO 27110

- Identificar: inventario, topología, riesgos iniciales.
- Proteger: hardening, firewall, control de accesos, cifrado, parches.
- Detectar: auditoría y logs.
- Responder y Recuperar: snapshots y política de respaldo.
  Este andamiaje es coherente con las unidades del curso sobre administración Linux, scripting Bash, KVM, seguridad de servidores y preparación para servicios de red y nube.

II. Implementación de servicios básicos de red

1. Objetivo

Configurar y asegurar servicios críticos de red en entornos Linux (Web, FTP, Correo y Mensajería), garantizando confidencialidad, integridad y disponibilidad. Estos servicios representan la base de las operaciones organizacionales y son indispensables para el cumplimiento de la norma ISO/IEC 27110.

2. Alcance

- **Servidores involucrados:** srv-core (interno) y srv-dmz (expuesto en la zona perimetral).
- **Servicios implementados:**
  - Servidor Web (Apache/Nginx).
  - Servidor FTP seguro (vsftpd).
  - Servidor de Correo (Postfix).
  - Servidor de Mensajería Instantánea (Ejabberd – XMPP).
- **Usuarios:** empleados de TI con autenticación individual y políticas de privilegios mínimos.

3. Procedimiento paso a paso

3.1 Servidor Web (Apache)

1. Instalación:

   sudo apt -y install apache2 libapache2-mod-security2

2. Configuración de hosting virtual:

   sudo nano /etc/apache2/sites-available/empresa.conf

   # VirtualHost con ServerName intranet.empresa.local

3. Habilitación:

   sudo a2ensite empresa.conf

   sudo systemctl reload apache2

4. Seguridad:

- Forzar **HTTPS** con Let’s Encrypt:

  sudo apt -y install certbot python3-certbot-apache

  sudo certbot --apache -d intranet.empresa.local
- Activar ModSecurity (WAF).
- Deshabilitar listado de directorios (Options -Indexes).

3.2 Servidor FTP seguro (vsftpd)

1. Instalación:

   sudo apt -y install vsftpd
2. Configuración:

   sudo nano /etc/vsftpd.conf

   # Habilitar local users, chroot_local_user=YES

   # Activar SSL/TLS: ssl_enable=YES
3. Generación de certificado propio:

   openssl req -x509 -nodes -days 365 \

   -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.key \

   -out /etc/ssl/certs/vsftpd.crt
4. Firewall:

   sudo ufw allow 21/tcp

   sudo ufw allow 40000:40100/tcp

3.3 Servidor de Correo (Postfix)

1. Instalación:

   sudo apt -y install postfix dovecot-imapd dovecot-pop3d
2. Configuración:

- Dominio interno: empresa.local.
- Autenticación con SASL y cifrado TLS.

- Buzones virtuales con Maildir.

  Archivo /etc/postfix/main.cf (extracto):

  smtpd_tls_cert_file=/etc/ssl/certs/mail.crt

  smtpd_tls_key_file=/etc/ssl/private/mail.key

  smtpd_use_tls=yes

3. Verificación:

   echo "Prueba correo" | mail -s "Test" usuario@empresa.local

3.4 Servidor de Mensajería Instantánea (Ejabberd – XMPP)

1. Instalación:

   sudo apt -y install ejabberd

2. Configuración básica:

- Dominio: chat.empresa.local.
- Usuarios creados con:

  ejabberdctl register user1 chat.empresa.local password1

  ejabberdctl register user2 chat.empresa.local password2

3. Seguridad:

- Cifrado TLS para todas las conexiones.
- Restricción de registros a administradores.
- Auditoría de conversaciones habilitada en logs.

4. Medidas de seguridad aplicadas

- Autenticación individual y claves fuertes para todos los servicios.
- Cifrado TLS en Web, FTP, Correo y XMPP.
- Reglas de firewall específicas (puertos 80/443, 21, 25, 5222, 5269).
- Logs centralizados en srv-core y respaldos semanales.

5. Entregables de esta fase

- Manual técnico de configuración de cada servicio.
- Evidencias de conexión segura (capturas de https, sftp, telnet 25, xmpp).
- Reporte de cumplimiento de la política de seguridad inicial.

6. Criterios de aceptación

- Página web institucional accesible por HTTPS.
- Transferencias de archivos por FTP solo bajo TLS.
- Correos enviados y recibidos correctamente en dominio empresa.local.
- Chat instantáneo funcional con usuarios internos.

7. Riesgos y controles

- **Riesgo:** ataques por fuerza bruta → **Control:** Fail2Ban.
- **Riesgo:** certificados caducados → **Control:** renovación automática con Certbot.
- **Riesgo:** apertura de puertos inseguros → **Control:** firewall restrictivo y auditoría mensual.

8. Mapeo ISO/IEC 27110

- **Identificar:** Servicios críticos de red y sus roles.
- **Proteger:** Cifrado TLS, firewall, autenticación.
- **Detectar:** Logs centralizados, Fail2Ban.
- **Responder/Recuperar:** Copias de configuración, snapshots de VM.

III. Seguridad en red y control de accesos

1. Objetivo

Fortalecer la infraestructura mediante la implementación de controles de red y gestión de accesos, garantizando que los servicios se utilicen de manera segura, confiable y controlada. La finalidad es reducir la superficie de ataque, mejorar la trazabilidad y habilitar conectividad remota cifrada bajo políticas corporativas.

2. Alcance

- **Servidores:** srv-core y srv-dmz.
- **Servicios a implementar:**
    - Firewall (iptables/UFW).
    - Servidor DNS interno (BIND).
    - Servidor DHCP (ISC DHCP).
    - VPN segura (OpenVPN).
- **Usuarios:** empleados de TI y personal autorizado con claves públicas y certificados digitales.

3. Procedimiento paso a paso

3.1 Firewall (iptables/UFW)

1. Configuración restrictiva:

   sudo ufw default deny incoming

   sudo ufw default allow outgoing

2. Reglas mínimas:

   sudo ufw allow 22/tcp comment 'SSH desde admin'

   sudo ufw allow 80,443/tcp comment 'Web seguro'

   sudo ufw allow 25/tcp comment 'Correo saliente'

   sudo ufw allow 5222,5269/tcp comment 'XMPP'

3. Habilitación:

   sudo ufw enable

4. Protección avanzada:

- Fail2Ban para mitigar fuerza bruta.
- Logging detallado de accesos y denegaciones.

3.2 Servidor DNS interno (BIND)

1. Instalación:

   sudo apt -y install bind9 bind9utils

2. Zona directa (empresa.local):

   $TTL 86400

   @ IN SOA ns1.empresa.local. admin.empresa.local. (

   2025091901 ; Serial

   3600 ; Refresh

   1800 ; Retry

   1209600 ; Expire

   86400) ; Minimum TTL

   @ IN NS ns1.empresa.local.

   ns1 IN A 192.168.20.10

   www IN A 192.168.30.20

   mail IN A 192.168.20.30

   chat IN A 192.168.20.40

3. Zona inversa (ejemplo 192.168.20.0/24).

4. Prueba de resolución:

   dig @192.168.20.10 www.empresa.local

3.3 Servidor DHCP (ISC DHCP)

1. Instalación:

   sudo apt -y install isc-dhcp-server

2. Configuración (/etc/dhcp/dhcpd.conf):

```
subnet 192.168.20.0 netmask 255.255.255.0 {
  range 192.168.20.100 192.168.20.200;
  option routers 192.168.20.1;
  option domain-name "empresa.local";
  option domain-name-servers 192.168.20.10;
}
```

3. Reservas para servidores críticos:

```
host srv-core {
  hardware ethernet 00:11:22:33:44:55;
  fixed-address 192.168.20.10;
}
```

4. Validación:

```
sudo systemctl restart isc-dhcp-server
tail -f /var/log/syslog | grep DHCP
```

3.4 Servidor VPN (OpenVPN)

1. Instalación:

```
sudo apt -y install openvpn easy-rsa
```

2. Generación de PKI:

```
make-cadir ~/openvpn-ca
cd ~/openvpn-ca
./easyrsa init-pki
./easyrsa build-ca
./easyrsa gen-req servidor nopass
./easyrsa sign-req server servidor
```

3. Configuración de servidor (/etc/openvpn/server.conf):

   port 1194

   proto udp

   dev tun

   server 10.8.0.0 255.255.255.0

   push "redirect-gateway def1"

   push "dhcp-option DNS 192.168.20.10"

   cipher AES-256-GCM

   auth SHA256

4. Arranque:

   sudo systemctl enable openvpn@server

   sudo systemctl start openvpn@server

5. Entrega de certificados a clientes.
6. Verificación de conectividad segura desde fuera de la red local.

4. Medidas de seguridad aplicadas

- Autenticación por certificados en VPN.
- Reglas de firewall actualizadas tras habilitar DNS, DHCP y VPN.
- Registro de solicitudes DNS y asignaciones DHCP para auditoría.
- Logs de OpenVPN revisados periódicamente.

5. Entregables

- Archivo de reglas de firewall (documentado).
- Zonas DNS y registros verificados.
- Configuración DHCP con asignaciones y reservas.
- Informe de pruebas de conexión VPN (clientes internos y externos).

6. Criterios de aceptación

- Ningún servicio expuesto sin reglas de firewall.
- Resolución interna de dominios funcional (ejemplo: www.empresa.local).
- Asignación automática de IPs válida en clientes.
- Conexión VPN estable y cifrada con acceso a recursos internos.

7. Riesgos y controles

- **Riesgo:** fuga de DNS hacia internet.
    - **Control:** reenviadores solo a servidores autorizados.
- **Riesgo:** uso indebido de la VPN.
    - **Control:** revocación inmediata de certificados comprometidos.
- **Riesgo:** saturación de DHCP.
    - **Control:** monitoreo de logs y límites de asignación.

8. Mapeo ISO/IEC 27110

- **Identificar:** Servicios críticos de red (DNS, DHCP, VPN).
- **Proteger:** Firewall, cifrado, control de acceso VPN.
- **Detectar:** Logs de DNS, DHCP y OpenVPN.
- **Responder/Recuperar:** Revocación de certificados y restauración de configuraciones.

IV. Monitoreo y auditoría

Objetivo

Garantizar la detección temprana de incidentes, el control sobre el estado de los servicios y la generación de evidencias para auditoría. Esto se logra con herramientas de monitoreo (Nagios), centralización de logs y pruebas de seguridad internas.

2. Alcance

- **Servidores:** srv-mon (dedicado a monitoreo) y los nodos srv-core y srv-dmz como hosts supervisados.
- **Servicios monitoreados:** Web, FTP, Correo, XMPP, DNS, DHCP, VPN y firewall.
- **Usuarios:** administradores de TI con accesos restringidos a paneles de monitoreo.

3. Procedimiento paso a paso

3.1 Implementación de Nagios

1. Instalación:

   sudo apt -y install nagios4 nagios-plugins nagios-nrpe-plugin

2. Configuración de NRPE en cada servidor:

   sudo apt -y install nagios-nrpe-server

   sudo nano /etc/nagios/nrpe.cfg

   # Definir comandos para CPU, memoria, disco, servicios

3. Definición de hosts y servicios en srv-mon:

```
define host {
  use linux-server
  host_name srv-core
  address 192.168.20.10
}


define service {
```

use generic-service

host_name srv-core

service_description HTTP

check_command check_http

}

4. Visualización: acceso vía navegador a https://srv-mon/nagios.

3.2 Centralización de logs

1. Instalación de rsyslog:

   sudo apt -y install rsyslog

2. Configuración en cada servidor (/etc/rsyslog.conf):

   . @@192.168.20.50:514

3. En el servidor central (srv-mon):

   sudo nano /etc/rsyslog.d/central.conf

   # Recepción UDP/TCP de logs

4. Revisión:

   tail -f /var/log/syslog | grep srv-core

3.3 Auditoría con Fail2Ban y reportes

1. Instalación:

   sudo apt -y install fail2ban

2. Definir reglas para Apache, SSH y Postfix:

   sudo nano /etc/fail2ban/jail.local

   [sshd]

   enabled = true

   port = ssh

   filter = sshd

logpath = /var/log/auth.log

maxretry = 3

3. Validación:

sudo fail2ban-client status sshd

3.4 Pruebas de seguridad internas

1. Escaneo de servicios expuestos con Nmap:

nmap -sV -p- 192.168.20.0/24

2. Evaluación de vulnerabilidades con OpenVAS o Nessus.
3. Generación de informe de hallazgos y plan de mitigación.

4. Medidas de seguridad aplicadas

- Monitoreo activo 24/7 de servicios críticos.
- Alertas configuradas por correo ante fallos o intentos de acceso no autorizados.
- Logs centralizados con retención mínima de 90 días.
- Pruebas periódicas de vulnerabilidad para validar controles.

5. Entregables

- Panel de Nagios con estado de todos los servicios.
- Reporte consolidado de logs.
- Informe de auditoría de seguridad con evidencias de bloqueos (Fail2Ban).
- Acta de pruebas de penetración internas.

6. Criterios de aceptación

- Todos los servicios monitoreados visibles en Nagios y con estado UP.
- Logs centralizados accesibles y consultables.
- Evidencias de bloqueos automáticos en intentos de intrusión.
- Informe de pruebas con recomendaciones de mejora.

7. Riesgos y controles

- **Riesgo:** sobrecarga de alertas → **Control:** afinación de umbrales en Nagios.
- **Riesgo:** pérdida de logs → **Control:** respaldo diario en almacenamiento externo.
- **Riesgo:** falsa sensación de seguridad → **Control:** auditorías externas semestrales.

8. Mapeo ISO/IEC 27110

- **Identificar:** registros centralizados.
- **Proteger:** Fail2Ban y alertas proactivas.
- **Detectar:** Nagios y escaneo de servicios.
- **Responder y Recuperar:** informes de vulnerabilidades y planes de acción.

V. Integración con la nube (Cloud Computing)

1. Objetivo

Extender la infraestructura local hacia la nube mediante el uso de servicios IaaS y PaaS, asegurando alta disponibilidad, escalabilidad y seguridad. Se busca aprovechar instancias virtuales, almacenamiento gestionado y servicios de plataforma para optimizar costos y reforzar la ciberseguridad.

2. Alcance

- **Proveedor elegido:** AWS (Free Tier para pruebas).
- **Servicios a integrar:**
    - IaaS: instancias EC2 (Linux).
    - Almacenamiento en nube (S3, EBS).
    - PaaS: despliegue de aplicación web con Elastic Beanstalk.
    - Seguridad: grupos de seguridad (firewall cloud) e IAM (gestión de identidades).

3. Procedimiento paso a paso

3.1 Preparación de cuenta y red en la nube

1. Crear cuenta AWS Free Tier.
2. Configurar VPC (Virtual Private Cloud) con subredes públicas y privadas.
3. Definir grupos de seguridad:
    - Permitir solo tráfico HTTP/HTTPS (80/443).
    - SSH restringido a IP de administración.
    - Denegar todo tráfico no autorizado.

3.2 Despliegue de instancias EC2 (IaaS)

1. Crear instancia EC2 con Ubuntu Server.
2. Conexión remota:

   ssh -i llave.pem ubuntu@<IP-publica>
3. Configuración básica:

- Instalar Apache y habilitar HTTPS con Let’s Encrypt.
- Montar volumen adicional (EBS) para datos críticos.

4. Seguridad:
    - Actualizaciones automáticas.
    - Acceso restringido con claves SSH.

3.3 Gestión de almacenamiento en la nube

1. Crear bucket S3 para respaldo de configuraciones.
2. Configurar políticas de acceso: solo administradores y servidores autorizados.
3. Automatizar backups con aws s3 sync.
4. Snapshots automáticos de volúmenes EBS para recuperación.

3.4 Implementación de PaaS (Elastic Beanstalk)

1. Subir aplicación web (ejemplo: intranet en Node.js o WordPress).
2. Configurar entorno con balanceador de carga y autoescalado.
3. Integrar con base de datos RDS (MySQL) para persistencia.
4. Conexión con almacenamiento en S3 para ficheros.

3.5 Gestión de accesos con IAM

1. Crear usuarios y roles con privilegios mínimos.
2. Políticas específicas:
    - Administrador (full access).
    - Operaciones (deploy y monitoreo).
    - Auditoría (solo lectura de logs).
3. Activar MFA (Multi-Factor Authentication).
4. Revisiones trimestrales de accesos.

3.6 Balanceo de carga y alta disponibilidad

1. Configurar Elastic Load Balancer (ELB).

2. Asociar al autoescalado:
    - Instancia mínima: 2
    - Instancia máxima: 5
    - Escalar si CPU > 70% durante 5 minutos.
3. Verificar failover apagando manualmente una instancia.

4. Medidas de seguridad aplicadas

- Firewall cloud con reglas estrictas.
- Accesos IAM basados en roles.
- Datos cifrados en reposo (S3 y EBS) y en tránsito (TLS).
- Respaldo automático en múltiples zonas de disponibilidad.

5. Entregables

- Diagrama de arquitectura en nube (IaaS + PaaS + almacenamiento).
- Reporte de configuración de IAM y políticas aplicadas.
- Evidencias de despliegue de aplicación web en Elastic Beanstalk.
- Capturas de balanceador y autoescalado en funcionamiento.

6. Criterios de aceptación

- Aplicación web disponible en internet con HTTPS.
- Respaldos automáticos confirmados en S3 y snapshots.
- Accesos IAM revisados y documentados.
- Balanceador funcionando con pruebas de failover exitosas.

7. Riesgos y controles

- **Riesgo:** exposición pública indebida de instancias.
    - **Control:** seguridad estricta en grupos de seguridad.
- **Riesgo:** escalamiento excesivo → sobrecostos.
    - **Control:** políticas de autoescalado optimizadas.

- **Riesgo:** pérdida de credenciales IAM.
    - **Control:** MFA y rotación periódica de claves.

8. Mapeo ISO/IEC 27110

- **Identificar:** servicios críticos desplegados en nube.
- **Proteger:** IAM, firewall cloud, cifrado.
- **Detectar:** monitoreo integrado y alertas.
- **Responder y Recuperar:** snapshots y backups en S3.