



**FACULTAD DE CIENCIAS E INGENIERÍA**

**PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE  
INFORMACIÓN**

**TESIS**

**ANÁLISIS DE VULNERABILIDADES Y GESTIÓN DE INCIDENTES  
DE SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD  
PROVINCIAL DE MARISCAL RAMÓN CASTILLA 2025**

**PARA OBTAR EL TÍTULO PROFESIONAL**

**INGENIERO DE SISTEMAS DE INFORMACIÓN**

**AUTORES:**

- BACH. MARIO ROGER GONZALES REYNA
- BACH. MILTON JHOAO FASANANDO ALARCÓN

**ASESOR:**

- LIC. CARLOS ENERIQUE MARTHANS RUIZ, Mtro.  
ORCID: 0000-0003-3092-782X

A handwritten signature in blue ink, likely belonging to Carlos Enerique Marthans Ruiz, the advisor.

**IQUITOS – LORETO – PERÚ**

**2025**

## ACTA DE SUSTENTACIÓN

Con Resolución Decanal N° 806-2025-UCP-FCEI, del 28 de agosto del 2025, se designó jurado.

Con Resolución Decanal N° 181-2026-UCP-FCEI, del 10 de febrero del 2026, se autorizó la sustentación.

Siendo las 10:00 a.m. del día 19 de febrero del 2026, se constituyó de modo presencial el Jurado para escuchar la presentación y defensa de la Tesis: **"ANÁLISIS DE VULNERABILIDADES Y GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD PROVINCIAL DE MARISCAL RAMÓN CASTILLA 2025"**.

### Presentado por:

MARIO ROGER GONZALES REYNA

Para optar el título profesional de Ingeniero de Sistemas de Información

MILTON JHOAO FASANANDO ALARCÓN

Para optar el título profesional de Ingeniero de Sistemas de Información

**Asesor:** Lic. CARLOS ENRIQUE MARTHANS RUIZ, Mtro.

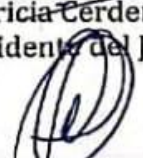
Luego de escuchar la sustentación y defensa ante las preguntas, el Jurado pasó a la deliberación en forma reservada, llegando a la siguiente conclusión:

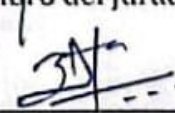
La sustentación es: Aprobada por Mayore

A las 11:30 horas culminó el acto público.

En fe de lo cual los miembros del jurado firman el Acta y comunican en acto público.

  
Ing. Carmen Patricia Cerdeña del Aguila, Dra.  
Presidenta del Jurado

  
Ing. Jimmy Max Ramirez Villacorta, Dr.  
Miembro del jurado

  
Ing. Tonny Eduardo Bardales Lozano, Mtro.  
Miembro del jurado

"Año de la Esperanza y el Fortalecimiento de la Democracia"

**CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN  
DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ – UCP**

El presidente del Comité de Ética e Integridad Científica

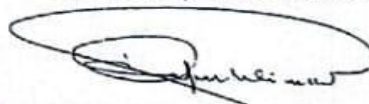
Hace constar que:

La Tesis titulada:

**"ANÁLISIS DE VULNERABILIDADES Y GESTIÓN DE INCIDENTES  
DE SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD  
PROVINCIAL DE MARISCAL RAMÓN CASTILLA 2025"**

De los alumnos: **MARIO ROGER GONZALES REYNA Y MILTON JHOAO FASANANDO ALARCÓN**, de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **15% de similitud**. Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 4 de febrero del 2026.



**Presidente del Comité de Ética e  
Integridad Científica  
Mgr. Arq. Jorge L. Tapullima Flores**

# UCP\_Ingenieria de Sistemas de Informacion\_2026\_Tesis\_Mario Gonzales\_Milton Fasanando\_V1\_resumen

**15%**  
Textos sospechosos

- 1% Similitudes
- 3% Idiomas no reconocidos
- 3% Textos potencialmente generados por la IA

Nombre del documento: UCP\_Ingenieria de Sistemas de Informacion\_2026\_Tesis\_Mario Gonzales\_Milton Fasanando\_V1\_resumen.pdf  
ID del documento: 0b4db12d661504d70c4367bc6af4bb66de02690c  
Tamaño del documento original: 471,38 kB

Depositante: Chris Angela Ramirez Flores  
Fecha de depósito: 2/2/2026  
Tipo de carga: Interface  
Fecha de fin de análisis: 2/2/2026

Número de palabras: 4618  
Número de caracteres: 31.757

Ubicación de las similitudes en el documento:



## Fuentes de similitudes

### Fuentes principales detectadas

| Nº | Descripciones                                                                                                                                                                                                                                                                                                                | Similitudes | Ubicaciones | Datos adicionales                      |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|----------------------------------------|
| 1  | Documento de otro usuario #74533<br>Viene de otro grupo<br>4 fuentes similares                                                                                                                                                                                                                                               | 2%          |             | Palabras idénticas: 2% (11 palabras)   |
| 2  | diariolaregion.com   Acciones concretas por el bienestar de la provincia Mariscal...<br><a href="https://diariolaregion.com/acciones-concretas-por-el-bienestar-de-la-provincia-mariscal-ramo...">https://diariolaregion.com/acciones-concretas-por-el-bienestar-de-la-provincia-mariscal-ramo...</a><br>4 fuentes similares | 1%          |             | Palabras idénticas: 1% (52 palabras)   |
| 3  | sinia.minam.gob.pe<br><a href="https://sinia.minam.gob.pe/sites/default/files/sinia/archivos/public/docs/programa_municipal...">https://sinia.minam.gob.pe/sites/default/files/sinia/archivos/public/docs/programa_municipal...</a>                                                                                          | < 1%        |             | Palabras idénticas: < 1% (22 palabras) |

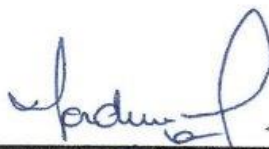
### Fuentes con similitudes fortuitas

| Nº | Descripciones                                                                                                                                                                                                           | Similitudes | Ubicaciones | Datos adicionales                      |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|----------------------------------------|
| 1  | repositorio.ucp.edu.pe<br><a href="https://repositorio.ucp.edu.pe/bitstreams/a9aa9f9a-ad15-43b0-8407-3a71bbfb0150/download">https://repositorio.ucp.edu.pe/bitstreams/a9aa9f9a-ad15-43b0-8407-3a71bbfb0150/download</a> | < 1%        |             | Palabras idénticas: < 1% (10 palabras) |
| 2  | hdl.handle.net   Implementación de ITIL 4 para el proceso de gestión de Incident...<br><a href="http://hdl.handle.net/20.500.3.2640/4287">http://hdl.handle.net/20.500.3.2640/4287</a>                                  | < 1%        |             | Palabras idénticas: < 1% (19 palabras) |

## **HOJA DE APROBACIÓN PROGRAMA ACADÉMICO DE INGENIERIA DE SISTEMAS DE INFORMACIÓN**

**BACHILLERES: MARIO ROGER GONZALES REYNA Y MILTON JHOAO FASANANDO  
ALARCÓN**

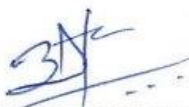
**La Tesis sustentada en acto público el día 19 de febrero del 2026, a las 10:00  
am, en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ.**



**ING. CARMEN PATRICIA CERDEÑA DEL AGUILA, DRA.  
PRESIDENTE DE JURADO**



**ING. JIMMY MAX RAMIREZ VILLACORTA, DR.  
MIEMBRO DE JURADO**



**ING. TONNY EDUARDO BARDALES LOZANO, MTRO.  
MIEMBRO DE JURADO**



**LIC. CARLOS ENRIQUE MARTHANS RUIZ, MTRO.  
ASESOR**

## **DEDICATORIA**

A mis padres, cimientos firmes sobre los que he construido cada uno de mis sueños. Por su amor incondicional, su fe inquebrantable en mí y por ser la brújula moral que siempre guía mi camino. Cada logro que celebro es, en realidad, un tributo a su enseñanza.

**MARIO ROGER**

## **DEDICATORIA**

A mis abuelos, quienes han sido un pilar fundamental en mi vida. Su dedicación, apoyo incondicional y valores han guiado mi formación personal y académica. Agradezco profundamente su esfuerzo y fortaleza que me han brindado para alcanzar este logro.

**MILTON JHOAO**

## **AGRADECIMIENTO**

A mis padres, columnas principales en la construcción de mis sueños. Mi eterno agradecimiento por su fe inquebrantable, por creer no solo en mí, sino en todo lo que podía llegar a ser. Sus consejos que con tanto amor me inculcaron, son la brújula que guía cada uno de mis pasos.

### **MARIO ROGER**

A Dios, por darme la vida, la fortaleza y la sabiduría necesarias para culminar esta etapa tan importante de mi formación profesional. Su guía ha sido una luz en mi camino y a mis abuelos, quienes han sido un sostén fundamental en mi vida.

### **MILTON JHOAO**

## INDICE DE CONTENIDO

|                                                                                 | <b>Página</b> |
|---------------------------------------------------------------------------------|---------------|
| RESUMEN .....                                                                   | 10            |
| ABSTRACT .....                                                                  | 11            |
| CAPÍTULO I.- MARCO TEÓRICO: .....                                               | 12            |
| <b>1.1 Antecedentes de Estudio:</b> .....                                       | 12            |
| <b>1.2 Bases Teóricas:</b> .....                                                | 13            |
| <b>1.3 Definición de Términos Básicos:</b> .....                                | 145           |
| CAPÍTULO II.- PLANTEAMIENTO DEL PROBLEMA: .....                                 | 17            |
| <b>2.1 Descripción del Problema:</b> .....                                      | 17            |
| <b>2.2 Formulación del Problema:</b> .....                                      | 18            |
| <b>2.2.1 Problema General:</b> .....                                            | 18            |
| <b>2.2.2 Problemas Específicos:</b> .....                                       | 18            |
| <b>2.3 Objetivos:</b> .....                                                     | 18            |
| <b>2.3.1 Objetivo General:</b> .....                                            | 18            |
| <b>2.3.2 Objetivos Específicos:</b> .....                                       | 19            |
| <b>2.4 Hipótesis:</b> .....                                                     | 19            |
| <b>2.5 Variables:</b> .....                                                     | 19            |
| <b>2.5.1 Identificación de Variables:</b> .....                                 | 19            |
| <b>2.5.2 Definición Conceptual de las Variables:</b> .....                      | 19            |
| Tabla N° 01.- Definición conceptual de la variable .....                        | 19            |
| <b>2.5.3 Operacionalización de las Variables:</b> .....                         | 21            |
| Tabla N° 02.- Operacionalización de la variable .....                           | 21            |
| CAPÍTULO III.- METODOLOGÍA: .....                                               | 22            |
| <b>3.1 Tipo y Diseño de Investigación:</b> .....                                | 22            |
| <b>3.2 Población y Muestra:</b> .....                                           | 22            |
| <b>3.3 Técnicas, instrumentos y procedimientos de recolección de datos:</b> ... | 23            |
| <b>3.4 Procesamiento y análisis de datos:</b> .....                             | 24            |
| CAPÍTULO IV.- RESULTADOS: .....                                                 | 26            |
| CAPÍTULO V.- DISCUSIÓN: .....                                                   | 34            |
| CAPÍTULO VI.- CONCLUSIONES: .....                                               | 35            |
| CAPÍTULO VII.- RECOMENDACIONES: .....                                           | 36            |
| CAPÍTULO VIII.- REFERENCIAS BIBLIOGRÁFICAS: .....                               | 37            |

## INDICE DE TABLAS

### Pagina

**Tabla N°1 :** Definición conceptual de la variable.....19

**Tabla N°2:** Operacionalización de la variable.....21

**Tabla N°3:** Porcentaje de equipos con fallas básicas.....26

**Tabla N°4:** Situación de la gestión de incidentes.....27

**Tabla N°5:** Clasificación de las vulnerabilidades por severidad en las áreas  
evaluadas.....29

**Tabla N°6:** Incumplimiento frente a los estándares mínimos definido.....32

## **RESUMEN**

El presente estudio tuvo como objetivo evaluar el nivel de vulnerabilidades técnicas y el desempeño de la gestión de incidentes de seguridad informática en la Municipalidad Provincial de Mariscal Ramón Castilla. La investigación se desarrolló bajo un enfoque cuantitativo, con diseño descriptivo y transversal. Para ello, se aplicó una lista de verificación a los equipos de cómputo de las diferentes áreas y se revisó el registro de incidentes correspondiente al último mes disponible.

Los resultados evidenciaron que todas las áreas presentan fallas básicas de seguridad informática. Las más representativas fueron Mesa de Partes (44 %), Logística (39 %) y Gerencia Municipal (37 %). En relación con la gestión de incidentes, se registraron 14 eventos, con un tiempo promedio de detección de 2,8 horas y un tiempo promedio de recuperación de 5,2 horas. Asimismo, solo el 43 % de los incidentes contó con registro completo y el 36 % incluyó evidencia adjunta.

La clasificación de vulnerabilidades mostró predominio de severidad media (42 %) y alta (29 %). El análisis de cumplimiento de estándares mínimos evidenció mayores incumplimientos en los procedimientos y registros documentados. En conclusión, los hallazgos reflejan una exposición significativa al riesgo y la necesidad de fortalecer los procesos, controles técnicos y mecanismos de seguimiento en materia de seguridad informática.

Palabras clave: vulnerabilidades, seguridad informática, municipalidad, exposición al riesgo.

## **ABSTRACT**

This study aimed to evaluate the level of technical vulnerabilities and the performance of cybersecurity incident management at the Provincial Municipality of Mariscal Ramón Castilla. The study employed a quantitative, descriptive, and cross-sectional design. To this end, a checklist was used to scan the computer equipment in all departments, and the incident log for the last available month was reviewed. Regarding the first point, all results demonstrated that all departments exhibit basic cybersecurity weaknesses. The most prominent areas were the Records Office (44%), Logistics (39%), and Municipal Management (37%). In terms of timing, 14 incidents were recorded, with an average detection time of 2.8 hours and an average recovery time of 5.2 hours. Furthermore, only 43% of incidents had complete records, and 36% included supporting evidence. On the other hand, the vulnerability count revealed that medium-severity vulnerabilities predominated at 42%, followed by high-severity vulnerabilities at 29%. The analysis of minimum compliance standards showed the greatest non-compliance in procedures and documented records for information gathering. In summary, the results indicate significant exposure and the need to implement processes, basic controls, and monitoring mechanisms to improve cybersecurity within the institution.

Keywords: vulnerabilities, information security, municipality, risk exposure.

## **CAPÍTULO I.- MARCO TEÓRICO:**

### **1.1 Antecedentes de Estudio:**

Bardales Sinarahua (2024), en su tesis “Análisis de la seguridad informática de la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas – 2023” para la Universidad Científica del Perú verificó el estado situacional de la seguridad en la OSTI de la municipalidad. Con énfasis cuantitativo y diseño no experimental, trabajo con la población de personal del área ( $n \approx 5$ ) a través de encuestas/entrevistas y revisión de infraestructura. Identificaron vulnerabilidades como parches pendientes, cuentas privilegiadas sin control y dispositivos sin mantenimiento y la baja conciencia en seguridad, para lo cual recomendó el fortalecimiento de políticas de actualización, controles de acceso y monitoreo de incidentes.

Evaristo Cipriano (2024), en la tesis “Auditoría de seguridad de la información aplicando la norma ISO/IEC 27001 en la Municipalidad Distrital de Luyando”, de la Universidad de Huánuco, realizó un estudio experimental que fue realizado para medir la fiabilidad y seguridad antes o después de una auditoría sobre ISO 27001. Después de encuesta y dos funcionarios, vio que las políticas fundamentales son inadecuadas, activos fundamentales no se respaldan, la guía de operaciones del incidente no existe, se destroza la seguridad física, la sala del servidor estará cerrada con el viento, y las prácticas de acceso/contraseña son pobres. Desde aquí, ella hizo una conclusión que será la base para su libro: la única forma de mejorar la protección de la información es seguir rigurosamente la norma.

Fernández Rioja y Rioja Mesía (2023), en la tesis “Implementación de un modelo de gestión de incidencias basado en ITIL para mejorar el servicio de TI en una municipalidad distrital de Lambayeque (Reque)”, diseñó e implementó un proceso ITIL v3 de gestión de incidencias. Tras la selección del caso de estudio y modelado del flujo, afirmaron que luego de dicha

implementación, mejoraron los tiempos de atención y aumentaron el número de incidentes resueltos, entre lo que cabe mencionar que las incidencias reportadas se redujeron en casi un 66 % POST implementación.

Sangama Sangama (2020), en la tesis “Implementación de ITIL 4 para el proceso de gestión de incidentes en el área de informática de la Municipalidad Provincial de Lamas, San Martín” de la Universidad Peruana Unión 2019, obs., aplicó un pre-experimental con los 50 incidentes registrados. {pre y post} y lista de cotejos. Observó diferencias significativas entre pre y post, de manera que la mesa de ayuda y el proceso ITIL 4 influyen positivamente en la gestión de los incidentes y la continuidad del servicio.

Argüeso Ramírez (2019), El SGSI propuesto en la tesis “Propuesta de un sistema de gestión de seguridad de información (SGSI) basado en ISO 27001 para el área de informática de la Municipalidad Provincial de Huánuco” por la Universidad de Huánuco. Siguió el ciclo PDCA; El campo, selección y clasificación de elementos, análisis y evaluación de la amenaza y la sucesiva elección del control de los tratamientos, según ISO 27002. La formalización de un SGSI es crucial para garantizar un ambiente en el cual la municipalidad proteja sus activos y garantice la seguridad: confidencialidad, integridad y factibilidad de información.

## **1.2 Bases Teóricas:**

### **Análisis de vulnerabilidades**

Mantener SO y firmware actualizado es parte del mantenimiento preventivo; identificar, priorizar, adquirir, instalar y verificar parches en toda la organización es exactamente lo que NIST SP 800-40 Rev.4 define como gestión empresarial de parches; es por ello que medir el porcentaje de equipos con pendientes es un indicador directo del estado del proceso.

### **Controles técnicos contra malware**

La familia ISO/IEC 27000 menciona que la seguridad se logra aplicando un conjunto adecuado de controles; ISO/IEC 27002:2022 incluye la protección frente a malware como praxis esencial. Verificar si cada equipo tiene

antimalware activo y vigente aterriza este control a un indicador operativo simple.

### Autenticación y contraseñas

El estándar NIST SP 800-63B establece requisitos de durabilidad para contraseñas memorizadas y lineamientos básicos de autenticación. En su actualización más reciente (serie 800-63-4), se indica que las contraseñas deben contar con un mínimo de ocho caracteres, recomendándose longitudes mayores cuando se utiliza un solo factor de autenticación o complementarse con autenticación multifactor (MFA). En función de estas directrices, se adoptó el valor de ocho caracteres como punto de corte para clasificar una contraseña como débil o no débil.

### Gestión de incidentes de seguridad informática

Para la ISO/IEC 27035-1:2023, la gestión de seguridad informática se define como un proceso estructurado que tiene como proceso las siguientes fases de preparación, detección y reporte, evaluación, respuesta y lecciones aprendidas, cada una es dependiente de cada fase.

## **1.3 Definición de Términos Básicos:**

- Sistema web: Aplicación Sistema que se despliega en el navegador web que permite realizar procesos transaccionales de alto volumen involucrados con inventarios, ventas, facturación y reportes.
- Gestión de ventas: cualquier transacción y actividad en línea que pasa por un sistema realizado por apoyar un registro de producto, venta, facturación, reporte y atención al cliente en punto de venta.
- Usabilidad del sistema: El grado en que el sistema se puede usar para completar tareas específicas con eficacia, eficiencia y satisfacción.

- SUS (System Usability Scale): escala de usabilidad del sistema, un conjunto de 10 ítems que produce una puntuación de 0 a 100 evaluación de la usabilidad percibida.
- Superficie de ataque: Conjunto de puntos vulnerables dentro de un sistema o infraestructura tecnológica que pueden ser explotados por amenazas internas o externas.
- Tiempo medio de detección (MTTD): Promedio de tiempo transcurrido entre la ocurrencia de un incidente de seguridad y su identificación formal por parte del área responsable.
- Tiempo medio de recuperación (MTTR): Promedio de tiempo necesario para restablecer la operatividad del servicio afectado tras la ocurrencia de un incidente.
- Registro completo de incidente: Documento que contiene información mínima obligatoria como fecha, hora, área afectada, responsable, descripción del evento, acciones realizadas y cierre.
- Evidencia técnica: Información verificable asociada a un incidente, como capturas de pantalla, registros de sistema (logs), archivos de auditoría o reportes técnicos.
- Índice de exposición al riesgo: Indicador porcentual derivado del promedio de vulnerabilidades detectadas, utilizado para estimar el nivel general de riesgo de un área o activo tecnológico.

## **CAPÍTULO II.- PLANTEAMIENTO DEL PROBLEMA:**

### **2.1 Descripción del Problema:**

La Municipalidad Provincial de Mariscal Ramón Castilla realiza su management principalmente a través de sus equipos de cómputo, redes locales y aplicativos institucionales: tramitan, se comunican entre áreas y llevan su archivo. Sin embargo, no hay una única medición reciente con datos elementales que exhiba al mismo tiempo el “porcentaje” de activos de TI y “porcentaje” de incidentes de seguridad. La falta de número impide dimensionar la exposición y priorizar acciones técnicas. En la operación cotidiana, se identifican situaciones como: "mi equipo posterga la actualización, mi antivirus se presenta actualmente fuera de servicio pero posee una luz verde en su caso, mi contraseña no tiene ninguna letra en mayúscula Y lo único que consigo recibir acerca de los incidentes es un mail, ✱ Mensajería o simplemente un garabato ". Tampoco es fiable el "instante cero" de la avería del servicio o la detección del malwares: el tiempo de reacción o recuperación ya es hoy día imposible de estimar. Este conjunto de factores provoca efectos tales como: suspensión de la atención, reproceso administrativo de la información, tiempo de la persona insumido y percepción de inseguridad en la herramienta. Además, la necesidad de priorizar urgencias diarias en el equipo de TI, que generen licitaciones sin prelación o ventanas de mantenimiento de propietarios, porque no hay programación de detergente de relevancia, instaura una cultura de prevención reactiva.

### **2.2 Formulación del Problema:**

#### **2.2.1 Problema General:**

- ✓ ¿Cuál es el nivel de vulnerabilidades técnicas y el desempeño de la gestión de incidentes de TI en la Municipalidad Provincial de Mariscal Ramón Castilla, en un corte único de tiempo?

### **2.2.2 Problemas Específicos:**

- ✓ ¿Qué porcentaje de equipos presenta fallas básicas en las áreas de la Municipalidad Provincial de Mariscal Ramón Castilla?
- ✓ ¿Cuál es la situación de la gestión de incidentes en la Municipalidad Provincial de Mariscal Ramón Castilla?
- ✓ ¿Cómo se distribuyen las vulnerabilidades por severidad en la Municipalidad Provincial de Mariscal Ramón Castilla?
- ✓ ¿Qué incumplimientos hay frente a los estándares mínimos definidos y qué acciones deben atenderse primero? en la Municipalidad Provincial de Mariscal Ramón Castilla?

### **2.3 Objetivos:**

#### **2.3.1 Objetivo General:**

- ✓ Evaluar el nivel de vulnerabilidades técnicas de la gestión de incidentes de TI en la Municipalidad Provincial de Mariscal Ramón Castilla.

#### **2.3.2 Objetivos Específicos:**

1. Determinar el nivel de porcentaje de equipos con fallas básicas por área en la Municipalidad Provincial de Mariscal Ramón Castilla.
2. Describir la posible situación de como se desarrolla la gestión de incidentes en la Municipalidad Provincial de Mariscal Ramón Castilla.
3. Realizar la clasificación de las posibles vulnerabilidades por severidad en las áreas evaluadas en la Municipalidad Provincial de Mariscal Ramón Castilla.
4. Identificar y enumerar los incumplimientos frente a los estándares mínimos definidos y priorizar las acciones que deben atenderse primero en la Municipalidad Provincial de Mariscal Ramón Castilla.

### **2.4 Hipótesis:**

No aplica por tratarse de un estudio descriptivo–diagnóstico, sin contrastación estadística de relaciones entre variables. El trabajo se guía por preguntas de investigación y objetivos específicos operativizados en indicadores.

## 2.5 Variables:

### 2.5.1 Identificación de Variables:

V1. Análisis de vulnerabilidades

V2. Gestión de incidentes de seguridad informática

### 2.5.2 Definición Conceptual de las Variables:

#### ▪ Definición Conceptual de las Variables:

**Tabla N° 01.- Definición conceptual de la variable**

| Variable                                       | Definición Conceptual                                                                                                                                                                                                             | Definición Operacional                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Análisis de vulnerabilidades                   | Revisión del estado básico de seguridad en equipos y sistemas (actualizaciones, antimalware, contraseñas y severidad de hallazgos) para estimar el nivel de exposición de la Municipalidad Provincial de Mariscal Ramón Castilla. | Se medirá mediante la aplicación de una lista de verificación técnica a cada equipo evaluado, registrando el porcentaje de sistemas operativos desactualizados, equipos sin antivirus activo o actualizado, contraseñas débiles y la clasificación de vulnerabilidades por nivel de severidad (baja, media, alta, crítica). A partir de estos indicadores se calculará el Índice de Exposición por área, expresado en porcentaje. |
| Gestión de incidentes de seguridad informática | Capacidad operativa para registrar y atender eventos que afectan la confidencialidad, integridad y disponibilidad: ocurrencia, detección, recuperación y documentación del incidente                                              | Se medirá mediante la revisión documental de la bitácora de incidentes correspondiente al último mes disponible, registrando el número de incidentes ocurridos, el tiempo medio de detección (MTTD), el tiempo medio de recuperación (MTTR), el porcentaje de incidentes con registro completo y el porcentaje de incidentes con evidencia técnica adjunta. Los resultados se expresarán en frecuencias, promedios y porcentajes. |

*Fuente: Elaboración Propia*

### 2.5.3 Operacionalización de las Variables:

**Tabla N° 02.- Operacionalización de la variable**

| VARIABLES                                      | INDICADORES                                       | MEDIDA                    | INSTRUMENTOS                           |
|------------------------------------------------|---------------------------------------------------|---------------------------|----------------------------------------|
| Análisis de vulnerabilidades                   | % de equipos con sistema operativo desactualizado | Porcentaje (%)            | Lista de verificación por equipo       |
|                                                | % de equipos sin antivirus                        | Porcentaje (%)            | Lista de verificación por              |
|                                                | % de equipos con contraseña débil                 | Porcentaje (%)            | Lista de verificación por equipo       |
|                                                | Severidad de vulnerabilidades por                 | (baja–media–alta–crítica) | Matriz de severidad /                  |
|                                                | Índice de exposición por área                     | 0–100%                    | Hoja de cálculo (derivado de la lista) |
| Gestión de incidentes de seguridad informática | Incidentes por mes                                | Conteo (n)                | Bitácora de incidentes / tickets       |
|                                                | Tiempo medio de detección                         | Horas promedio (h)        | Bitácora (hora de inicio y detección)  |
|                                                | Tiempo medio de recuperación                      | Horas promedio (h)        | Bitácora (hora de reporte y cierre)    |
|                                                | % de incidentes con registro completo             | Porcentaje (%)            | Bitácora de incidentes                 |
|                                                | % de incidentes con evidencia adjunta             | Porcentaje (%)            | Bitácora / repositorio de evidencias   |

*Fuente: Elaboración Propia*

## **CAPÍTULO III.- METODOLOGÍA:**

### **3.1 Tipo y Diseño de Investigación:**

- **Tipo o enfoque de la Investigación:**

Esta investigación tiene por enfoque Cuantitativo, ya que se orientó a la medición y análisis de variables objetivas mediante indicadores numéricos.

Esta investigación es de tipo aplicada, ya que se generó resultados prácticos que orientaron a la mejora de la gestión y los controles de seguridad informática.

Esta investigación es de nivel descriptivo, que permitió describir el estado actual de las vulnerabilidades y la gestión de incidentes sin establecer relaciones causales.

- **Diseño de la Investigación:**

Esta investigación tiene un diseño no experimental, transversal

### **3.2 Población y Muestra:**

- **Población:**

Se uso las unidades técnicas: todos los equipos de cómputo y activos de TI en uso (PCs, laptops, al menos un servidor y un equipo de red principal) de la Municipalidad Provincial de Mariscal Ramón Castilla.

Se utilizó los registros de operación que son todos los incidentes de seguridad informática documentados por la entidad durante el último mes disponible de registro.

- **Muestra:**

Tipo de muestra: por conveniencia y acceso al sistema de información.

Los criterios de selección que se aplicó fueron la disponibilidad de los equipos, para lo cual se consideró la condición activa y accesible de los equipos el día que

se desarrolló la auditoría, así también como la trazabilidad de los incidentes, verificada mediante la existencia de registros con fechas y horas críticas.

La cobertura mínima que se usó fue de al menos 20 equipos de usuario final, cuando la disponibilidad lo permita, distribuidos entre las áreas prioritarias de la entidad.

Infraestructura: 1 servidor + 1 principal equipo de red (switch o router)

Incidentes: todos los que han ocurrido en los últimos 30 días.

Criterios de inclusión: se excluyó los equipos que estuvieron usando previo identificación y acceso autorizado; incidente con los mínimos datos.

Los criterios de exclusión que aplicaron fueron todos los equipos que estaban fuera de servicio o sin acceso al momento de la auditoría, así mismo todos los incidentes que no cumplieron con el límite temporal de visualización o que carecían de registros mínimos de fechas y horas en el sistema de información.

### **3.3 Técnicas, instrumentos y procedimientos de recolección de datos:**

#### **▪ Técnica de Recolección de Datos:**

- Observación directa estructurada de equipos y configuraciones básicas.
- Revisión documental de los incidentes reportados en las bitácoras del último mes.
- Registro sistemático que se resumieron en hoja de Excel o calculo para el procesamiento de los indicadores.

#### **▪ Instrumento de Recolección de Datos:**

Se aplicó un checklist por equipo para evaluar el nivel de seguridad básica, considerando la actualización del sistema operativo, antivirus, firewall,

contraseñas, copias de seguridad, usuarios asignados y licenciamiento de software, incorporando evidencia cuando correspondía. Asimismo, se implementó un registro estandarizado de incidentes que permitió documentar fechas, tiempos de gestión, tipo, impacto, causa, acciones correctivas y evidencia asociada.

Los hallazgos fueron clasificados mediante una matriz de severidad (baja, media, alta y crítica) y consolidados en una hoja de cálculo, lo que facilitó el cálculo de indicadores de vulnerabilidad, la distribución por severidad y el Índice de Exposición al Riesgo. Finalmente, se analizaron indicadores de gestión de incidentes, como frecuencia mensual, tiempos de detección y resolución, y el nivel de completitud de los registros

- **Procedimiento de Recolección de Datos:**

El proceso se desarrolló en ocho etapas. En primer lugar, se realizó la coordinación y autorización con las áreas involucradas, definiendo responsables, cronograma y accesos a los equipos y registros. Luego, se levantó un inventario mínimo de los equipos por área y de los sistemas priorizados. Posteriormente, se aplicó un checklist de verificación en un único momento, mediante inspección directa por activo, registrando el cumplimiento y la evidencia correspondiente.

Para esta cuarta etapa se consideraron datos de los 30 últimos días registros en las bitácoras, donde se consideró las fechas y horas, la depuración se hizo en la misma hoja de cálculo en la cual se eliminó datos duplicados, se corrigió datos incompletos para poder validar con posterioridad

Los resultados finales fueron contrastados con el responsable de TI para su validación interna y se elaboró un informe con tablas y gráficos por área, un ranking de exposición y una síntesis de hallazgos destinada a la priorización, sin incluir la implementación de medidas correctivas.

### **3.4 Procesamiento y análisis de datos:**

La fase de análisis comenzó con la preparación de los datos, que incluyó la anonimización de áreas y equipos, la codificación del checklist y la clasificación de la severidad, además de la estandarización de los tiempos de gestión de incidentes. Posteriormente, la información fue registrada en hojas diferenciadas y sometida a un control de calidad mediante revisión muestral y validación de la consistencia temporal.

En esta fase se calcularon los indicadores de vulnerabilidad, tales como el porcentaje de sistemas desactualizados, equipos sin antivirus activo y contraseñas débiles, además de la distribución por niveles de severidad y el Índice de Exposición al Riesgo, obtenido como el promedio de dichos porcentajes.

En este proceso los valores faltantes se excluyeron únicamente del indicador afectado y fueron debidamente documentados.

Al final de todos los procesos los resultados se presentaron mediante tablas y gráficos por área.

## CAPÍTULO IV.- RESULTADOS:

1. De acuerdo al objetivo 01: Determinar el porcentaje de equipos con fallas básicas por área en la Municipalidad Provincial de Mariscal Ramón Castilla., tenemos los siguientes resultados.

Estos valores representan el porcentaje de equipos por área que presentan fallas básicas de seguridad, tales como:

- Sistema operativo desactualizado
- Antivirus inactivo o sin actualizar
- Contraseñas débiles

Tabla N° 03

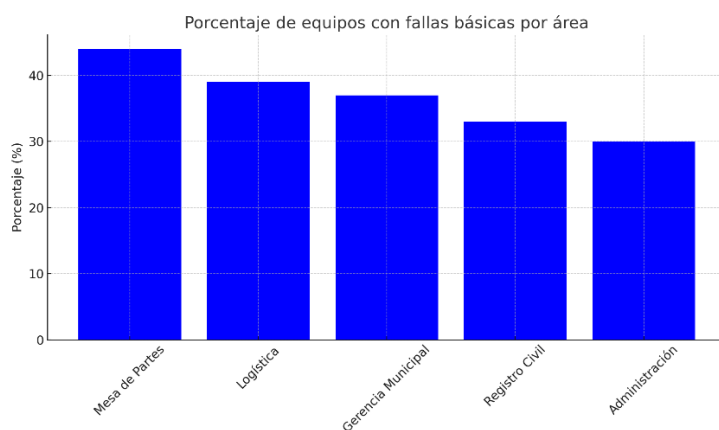
Porcentaje de equipos con fallas básicas

| Área               | Fallas básicas (%) |
|--------------------|--------------------|
| Mesa de Partes     | 44 %               |
| Logística          | 39 %               |
| Gerencia Municipal | 37 %               |
| Registro Civil     | 33 %               |
| Administración     | 30 %               |

Fuente: Elaboración propia

Grafico N° 01

Porcentaje de equipos con fallas básicas



La información presentada en la tabla y el gráfico evidencia que el área de Mesa de Partes concentra el mayor porcentaje de fallas básicas (44 %), lo que refleja la necesidad de una atención prioritaria, considerando el uso intensivo de los equipos en los procesos documentarios. De manera similar, las áreas de Logística (39 %) y Gerencia Municipal (37 %) muestran niveles elevados de fallas, asociados principalmente a deficiencias en el mantenimiento preventivo y la actualización de los sistemas.

Por su parte, Registro Civil (33 %) y Administración (30 %) presentan valores moderados; sin embargo, estos continúan representando riesgos relevantes para la seguridad de la información. En conjunto, los resultados indican que todas las áreas evaluadas presentan falencias significativas, lo que pone de manifiesto la necesidad de fortalecer los controles de seguridad informática a nivel institucional.

2. De acuerdo al objetivo 02: Describir la situación de la gestión de incidentes en la Municipalidad Provincial de Mariscal Ramón Castilla.

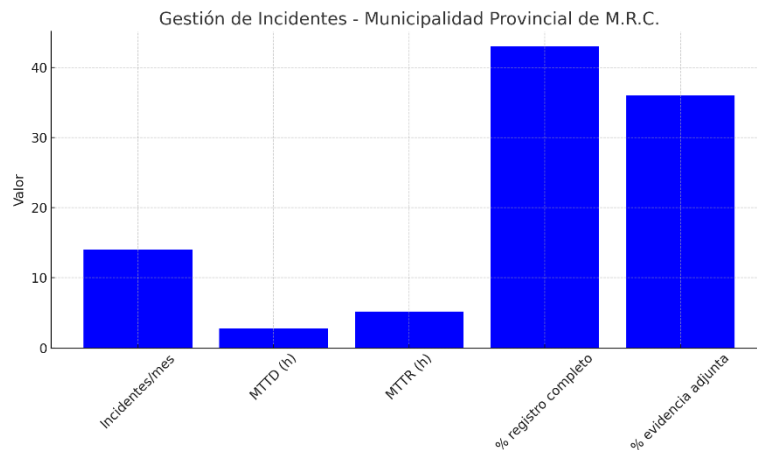
Tabla N° 04  
Situación de la gestión de incidentes

| Indicador                             | Resultado |
|---------------------------------------|-----------|
| Incidentes por mes                    | 14        |
| Tiempo medio de detección (MTTD)      | 2.8 h     |
| Tiempo medio de recuperación (MTTR)   | 5.2 h     |
| % de incidentes con registro completo | 43%       |
| % de incidentes con evidencia adjunta | 36 %      |

Fuente: Elaboración propia

Esta tabla refleja el estado actual de los procesos de registro, atención y documentación de incidentes dentro de la institución.

**Grafico N° 02**  
**Situación de la gestión de incidentes**



### Incidentes registrados

Se reportaron 14 incidentes en el último mes, una cifra significativa para una institución con recursos informáticos limitados.

Uno de los promedios fue de 5,2 horas, tiempos que tardo la detección y recuperación de los servicios, esto puso a evidenciar demoras significativas en el restablecimiento de la operatividad.

La calidad del registro de incidentes se evidencia que un 43% de los incidentes tiene un registro completo como fechas, responsable, acciones y cierre, también solo un 36% tiene evidencia adjunta (capturas, logs, archivos de auditoría). Mediante estos resultados queda evidenciada una pésima cultura de documentación. Así se limita la trazabilidad y el análisis post-incidente, condiciones claves para la mejora continua.

3. De acuerdo al objetivo 03: Clasificar las vulnerabilidades por severidad en las áreas evaluadas en la Municipalidad Provincial de Mariscal Ramón Castilla.

Tabla N° 05

Clasificación de las vulnerabilidades por severidad en las áreas evaluadas

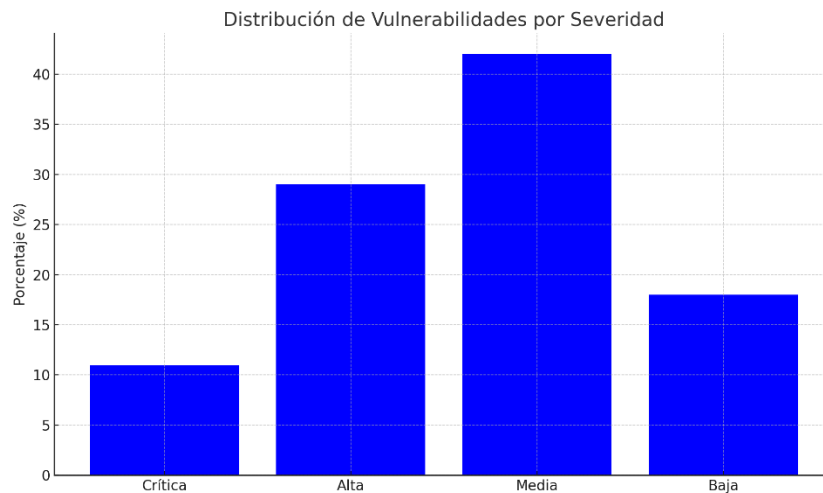
| Nivel de Severidad | Porcentaje (%) | Interpretación Técnica                                                                               |
|--------------------|----------------|------------------------------------------------------------------------------------------------------|
| Crítica            | 11 %           | Vulnerabilidades que permiten comprometer sistemas o datos sin interacción del usuario.              |
| Alta               | 29 %           | Fallas que facilitan accesos no autorizados, explotación de servicios o escalamiento de privilegios. |
| Media              | 42 %           | Configuraciones incorrectas, parches pendientes y controles insuficientes.                           |
| Baja               | 18 %           | Riesgos menores que no representan afectación inmediata, pero requieren mantenimiento preventivo.    |

Fuente: Elaboración propia

Esta tabla resume la distribución total de vulnerabilidades detectadas durante la evaluación técnica.

Grafico N° 03

Clasificación de las vulnerabilidades por severidad en las áreas evaluadas



Los resultados de la tabla y gráfico muestran que Clasificación de las vulnerabilidades por severidad en las áreas evaluadas:

Predominan las vulnerabilidades de severidad media (42 %)

Son fallas relacionadas con:

- Parches sin instalar
- Servicios expuestos
- Configuraciones débiles

Esto indica un mantenimiento correctivo irregular en los equipos evaluados.

Las vulnerabilidades altas (29 %) representan un riesgo significativo

Pueden permitir:

- Acceso no autorizado
- Modificación de información
- Afectación de servicios institucionales

Su presencia refleja la ausencia de una política formal de seguridad y de controles consistentes.

De acuerdo a las vulnerabilidades de nivel crítico, se evidencio que tiene una representación del 11 %, esto permite afirmar que existe un riesgo relevante al poder comprometer activos clave, las vulnerabilidades de nivel bajo, que alcanzan el 18 %, se asocian a deficiencias menores; sin embargo, su corrección sigue siendo necesaria para mantener adecuadas condiciones de seguridad e higiene digital.

4. De acuerdo al objetivo 04: Identificar los incumplimientos frente a los estándares mínimos definidos y priorizar las acciones que deben atenderse primero en la Municipalidad Provincial de Mariscal Ramón Castilla.

Tabla N° 06  
Incumplimientos frente a los estándares mínimos definidos

| Control / Estándar mínimo        | Cumplimiento Observado | Interpretación técnica                                                                  |
|----------------------------------|------------------------|-----------------------------------------------------------------------------------------|
| Sistema operativo actualizado    | 62 %                   | Falta de aplicación de parches y actualizaciones en más de un tercio de los equipos.    |
| Antivirus activo/actualizado     | 73 %                   | Existe una proporción menor, pero significativa, de equipos sin protección actualizada. |
| Contraseñas seguras (robustas)   | 59 %                   | Casi la mitad de los usuarios mantiene contraseñas débiles o inseguras.                 |
| Incidentes con registro completo | 43 %                   | En la mayoría de incidentes no se registra toda la información requerida.               |
| Incidentes con evidencia adjunta | 36 %                   | El registro de evidencias técnicas es deficiente en casi dos tercios de los incidentes. |

Fuente: Elaboración propia

Al comparar los resultados con los estándares mínimos definidos para este diagnóstico, se observa que:

Los resultados evidencian que el mayor nivel de incumplimiento se presenta en la falta de evidencias adjuntas (64 %), lo que refleja debilidades en la trazabilidad técnica de los incidentes. Asimismo, el 57 % de los casos carece de un registro completo, lo que limita la existencia de documentación formal para su seguimiento. En materia de seguridad lógica, se identificó un 41 % de incumplimiento en el uso de contraseñas seguras, lo que evidencia la ausencia de una política de autenticación robusta.

Asimismo, el 38 % de los equipos presenta sistemas operativos desactualizados, lo que los expone a vulnerabilidades conocidas, mientras que el 27 % no cuenta con antivirus actualizado, situación que, aunque de menor proporción, limita la capacidad de detección y mitigación de amenazas.

Esto implica que los incumplimientos más altos corresponden a la gestión de los incidentes, en lugar de los controles técnicos. Así se evidencia a continuación con la priorización de las acciones a realizar: alta, media y baja. Por un lado, el alta indica las acciones a realizar de manera inmediata: adjuntar evidencias técnicas en cada incidente al 64 % de incumplimiento y normalizar el registro completo de incidentes al 57 %. Las de prioridad media incluye la implementación de una política de contraseñas seguras a un 41 %. Por último, las de baja son: actualizar el sistema operativo de los equipos al 38 % y reforzar el proceso de actualización del antivirus a un 27 %.

## **CAPÍTULO V.- DISCUSIÓN:**

Por un lado, en el ámbito de los porcentajes de equipamiento con fallas básicas se hallaron cifras significativas de exposición en todas las áreas, con un puntaje más alto para Mesa de Partes en 44 por ciento, seguido de Logística en 39 por ciento y Gerencia Municipal en 37 por ciento.

Estos resultados coinciden con lo aportado por Delgado en 2021, quien afirma que las áreas de alto flujo documental presentan mayores riesgos por el uso intensivo de estaciones de trabajo y pocos procedimientos de mantenimiento preventivo.

Estos resultados evidencian que la ausencia de controles básicos incrementa la exposición a riesgos operativos y de seguridad en la institución. Al tratarse de un estudio descriptivo–diagnóstico, los hallazgos no buscan contrastar relaciones causales, sino describir el estado actual de la seguridad informática y su impacto potencial en la operatividad institucional.

Estos valores confirmaron lo planteado por Vargas y Espinoza en 2022, quienes coincidieron en que la no automatización impide hacer un análisis post incidente y disminuye la capacidad institucional de evitar recurrencias. Las vulnerabilidades, por otro lado, fueron en su mayoría de severidad media con alta con un 11 por ciento crítico.

De nuevo, los valores en conjunto indican que aunque no hay un colapso general de informática en seguridad, hay condiciones que permiten que las fallas sean explotadas por atacantes internos o externos. Cárdenas en 2020 ya lo había indicado, diciendo que alguna de las faltas de políticas efectivas en actualización y autenticación son los factores que aumentan la superficie de ataque en los gobiernos municipales.

Finalmente, al comparar los resultados con aquellos que cumplen los estándares mínimos definidos del 100 por ciento, los mayores incumplimientos tienen que ver con la gestión de incidentes y, sobre todo, con la entrega de evidencias con un 64 por ciento y el registro completo con solo 57 por ciento. De hecho, también se mencionó en la actualidad que las municipalidades no tienen procedimientos para controlar la documentación digital, lo que perjudica su capacidad de respuesta y auditoría.

## **CAPÍTULO VI.- CONCLUSIONES:**

- El diagnóstico permitió también identificar que todas las áreas presentan equipos con fallas básicas de seguridad, siendo las más críticas Mesa de Partes con un 44%, Logística con un 39% y Gerencia Municipal con un 37%. Estas fallas significan una exposición exorbitante en términos de riesgo operacional por la ausencia de mantenimiento preventivo y actualización, además de control mínimo.
- En general, el área de incidentes response de la Municipalidad presenta operatividades deficientes, ya el tiempo de detección se encuentra en 2.8 horas, de recuperación en 5.2 horas y la evidencia documentada es casi inexistente al registrar completitud en sólo un 43% de incidentes y evidencia 36%, lo que impide análisis de causa y mejora.
- Es claro que la clasificación de las vulnerabilidades evidencia un predominio de threats de severidad media con un 42% y alta con un 29%, lo cual demuestra una alta superficie de ataque. La existencia de vulnerabilidades críticas en un 11% confirma un riesgo alto y con capacidad de impactar seriamente la sustentabilidad e integridad disponibilidad de los sistemas institucionales.
- El mayor número de incumplimientos básicamente típicos se encuentran en la gestión documental de incidentes, con un promedio de no cumplimiento de evidencias adjuntas de 64% y de 57% en registro completo; sin embargo, los controles técnicos presentan niveles de incumplimientos moderados, pero su ampliación a procesos administrativos aumenta sobremanera el riesgo global.

## **CAPÍTULO VII.- RECOMENDACIONES:**

- Instalar un plan preventivo de mantenimiento mensual, donde se prioricen las salas más expuestas y se tenga especial atención a la instalación de antivirus y últimas actualizaciones de sistemas operativos.
- Implementar un procedimiento formal de gestión de incidentes que contemple un formato obligatorio de registro, tiempos máximos de respuesta, requisitos de documentación y verificación de parte del responsable técnico.
- Implementar programas que permita la reducción de vulnerabilidades en la cual se priorice la corrección de fallas críticas, también la desactivación de configuraciones inseguras, la implementación y establecimiento de políticas de contraseñas y la aplicación de controles preventivos con auditorías periódicas.

## CAPÍTULO VIII.- REFERENCIAS BIBLIOGRÁFICAS:

- Cárdenas, J. (2020). *Evaluación de la seguridad de la infraestructura informática en gobiernos locales*. Universidad Nacional Mayor de San Marcos.
- Delgado, P. (2021). *Diagnóstico de vulnerabilidades en sistemas informáticos municipales*. Universidad Nacional de Cajamarca.
- Instituto Nacional de Estándares y Tecnología. (2020). *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations*. NIST.
- Kaspersky. (2022). *Kaspersky Security Bulletin 2022: Vulnerability Trends*. <https://www.kaspersky.com/>
- Lema, F., Cuero, D., & Rodríguez, M. (2020). Análisis de riesgos y vulnerabilidades en municipios rurales. *Revista Colombiana de Tecnologías de Información*, 18(2), 55–68.
- Montenegro, L., & Arias, P. (2021). Seguridad informática y riesgos en gobiernos locales de Ecuador. *Revista Ciencia Digital*, 5(3), 24–33.
- OWASP. (2021). *Top 10 Web Application Security Risks*. Open Web Application Security Project.
- PCM – Secretaría de Gobierno y Transformación Digital. (2021). *Lineamientos de Seguridad Digital para entidades del Estado*. Presidencia del Consejo de Ministros.
- Ramos, F. (2023). Mecanismos de auditoría y control para la gestión de incidentes en municipalidades distritales. *Revista Peruana de Gestión Pública*, 10(1), 45–60.
- Sánchez, A. (2023). Gestión de incidentes en instituciones públicas peruanas. *Revista de Innovación y Tecnología*, 7(2), 33–48.
- Vargas, M., & Espinoza, R. (2022). Estrategias de respuesta ante incidentes de seguridad informática en gobiernos locales. *Revista de Seguridad Digital*, 9(1), 72–84.

## CAPÍTULO IX.- ANEXOS:

### Anexo 01: Matriz de Consistencia

| Problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Objetivos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Variables                                      | Indicadores                                       | Metodología                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Problema general</b></p> <p>¿Cuál es el nivel de vulnerabilidades técnicas y el desempeño de la gestión de incidentes de TI en la Municipalidad Provincial de Mariscal Ramón Castilla, en un corte único de tiempo?</p> <p><b>Problemas específicos</b></p> <ul style="list-style-type: none"> <li>¿Qué porcentaje de equipos presenta fallas básicas en las áreas de la Municipalidad Provincial de Mariscal Ramón Castilla?</li> <li>¿Cuál es la situación de la gestión de incidentes en la Municipalidad Provincial de Mariscal Ramón Castilla?</li> <li>¿Cómo se distribuyen las vulnerabilidades por severidad en la Municipalidad Provincial de Mariscal Ramón Castilla?</li> <li>¿Qué incumplimientos hay frente a los estándares mínimos definidos y qué acciones deben atenderse primero? en la Municipalidad Provincial de Mariscal Ramón Castilla?</li> </ul> | <p><b>Objetivo general</b></p> <p>Evaluar el nivel de vulnerabilidades técnicas y el desempeño de la gestión de incidentes de TI en la Municipalidad Provincial de Mariscal Ramón Castilla, en un corte único de tiempo, para contar con una base objetiva que oriente la priorización de acciones.</p> <p><b>Objetivos específicos</b></p> <ol style="list-style-type: none"> <li>Determinar el porcentaje de equipos con fallas básicas por área en la Municipalidad Provincial de Mariscal Ramón Castilla.</li> <li>Describir la situación de la gestión de incidentes en la Municipalidad Provincial de Mariscal Ramón Castilla.</li> <li>Clasificar las vulnerabilidades por severidad en las áreas evaluadas en la Municipalidad Provincial de Mariscal Ramón Castilla.</li> <li>Identificar los incumplimientos frente a los estándares mínimos definidos y priorizar las acciones que deben atenderse primero en la Municipalidad Provincial de Mariscal Ramón Castilla.</li> </ol> | Análisis de vulnerabilidades                   | % de equipos con sistema operativo desactualizado | <p>Enfoque: Cuantitativo.</p> <p>Tipo de investigación: Aplicada.</p> <p>Diseño: No experimental, transversal (una sola medición)..</p> <p>Nivel: Descriptivo (diagnóstico).</p> <p>Técnicas: Encuesta, ficha de observación.</p> <p>Instrumentos: Cuestionario y ficha de observación</p> |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                | % de equipos sin antivirus activo/actualizado     |                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                | % de equipos con contraseña débil                 |                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                | Severidad de vulnerabilidades por activo          |                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                | Índice de exposición por área                     |                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Gestión de incidentes de seguridad informática | Incidentes por mes                                |                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                | Tiempo medio de detección                         |                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                | Tiempo medio de recuperación                      |                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                | % de incidentes con registro completo             |                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                | % de incidentes con evidencia adjunta             |                                                                                                                                                                                                                                                                                            |

## Anexo 02: Instrumentos de recolección de datos

### Lista de Verificación de Vulnerabilidades por Equipo

**Finalidad:** Registrar el estado de cada equipo de cómputo respecto a los controles básicos de seguridad establecidos para el análisis de vulnerabilidades.

**Instrucciones de uso:** Complete una fila por cada equipo evaluado. Marque Sí/No según corresponda. Registre la severidad de las vulnerabilidades identificadas y detalle observaciones relevantes.

| Código del equipo | Área / Oficina | Usuario | ¿SO actualizado? (S/N) | ¿Antivirus actualizado? (S/N) | ¿Contraseña segura? (S/N) | Severidad (B/M/A/C) | Observaciones |
|-------------------|----------------|---------|------------------------|-------------------------------|---------------------------|---------------------|---------------|
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |
|                   |                |         |                        |                               |                           |                     |               |

## Ficha de Registro de Incidentes de Seguridad Informática

**Finalidad:** Estandarizar la documentación de los incidentes de seguridad informática para su análisis, clasificación y seguimiento.

**Instrucciones de uso:** Complete una ficha por cada incidente registrado. Indique las fechas y horas según corresponda. Marque si el registro está completo y si el incidente cuenta con evidencia adjunta.

| Código del incidente | Fecha/hora de inicio | Fecha/hora de detección | Fecha/hora de reporte | Fecha/hora de cierre | Área afectada | Tipo de incidente | Evidencia (S/N) | Registro completo (S/N) | Observaciones |
|----------------------|----------------------|-------------------------|-----------------------|----------------------|---------------|-------------------|-----------------|-------------------------|---------------|
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |
|                      |                      |                         |                       |                      |               |                   |                 |                         |               |