FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

DESARROLLO DE UNA METODOLOGÍA PARA LA GESTIÓN DE INCIDENTES EN SEGURIDAD INFORMÁTICA CON APLICACIÓN DE LA ISO 27001 Y PROTOCOLOS NIST PARA EL HOSPITA MARÍA

SUSTENTADO POR:
CRISTOPHER LEONEL RIVAS TURCIOS
WILMER FERNANDO ESQUIVEL MEJIA

ASESOR METODOLÓGICO
JORGE RAÚL MARADIAGA CHIRINOS

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.
MES, 2025

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA
UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA
ROSALPINA RODRÍGUEZ

VICERRECTOR ACADÉMICO NACIONAL
JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL
ROGER MARTÍNEZ MIRALDA

DECANA FACULTAD DE POSTGRADO
ANA DEL CARMEN RETTALLY VARGAS

DESARROLLO DE UNA METODOLOGÍA PARA LA GESTIÓN DE INCIDENTES EN SEGURIDAD INFORMÁTICA CON APLICACIÓN DE LA ISO 27001 Y PROTOCOLOS NIST PARA EL HOSPITAL MARÍA

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN

ASESOR METODOLÓGICO

JORGE RAÚL MARADIAGA CHIRINOS

MIEMBROS DE LA TERNA:

MASTER KEVIN FUNEZ
MASTER ALBA GARAY
MASTER MANUEL GARCÍA LACAYO

FACULTAD DE POSTGRADO

DESARROLLO DE UNA METODOLOGÍA PARA LA GESTIÓN DE INCIDENTES EN SEGURIDAD INFORMÁTICA CON APLICACIÓN DE LA ISO 27001 Y PROTOCOLOS NIST PARA EL HOSPITAL MARÍA

CRISTOPHER LEONEL RIVAS TURCIOS
WILMER FERNANDO ESQUIVEL MEJÍA

Resumen

Este trabajo tuvo como finalidad desarrollar una metodología para la gestión de incidentes de seguridad informática en el Hospital María, tomando como base las normas ISO 27001, ISO 27035 y el marco de ciberseguridad NIST. El estudio se enfocó en mejorar la protección de los datos clínicos y garantizar la continuidad de los servicios médicos ante posibles ciberataques. Se utilizó un enfoque mixto, con alcance descriptivo y explicativo. La población incluyó a 7 colaboradores del área técnica y administrativa en tecnologías de la información. Se aplicaron instrumentos como encuestas con escala Likert, entrevistas, análisis FODA y matriz de riesgos para identificar vulnerabilidades, evaluar el nivel de preparación institucional y conocer el grado de conocimiento del personal sobre normativa y protocolos. Los resultados mostraron que, aunque existe cierta familiaridad con estándares internacionales, no hay políticas claras ni procedimientos establecidos para responder ante incidentes. Además, se detectaron limitaciones en recursos tecnológicos y formación del personal. A partir de estos hallazgos, se propuso una metodología estructurada y adaptada al contexto del hospital, dividida en fases de prevención, detección,

respuesta, recuperación y mejora continua, con énfasis en la capacitación del personal y la formalización de procesos de seguridad.

Palabras claves: Datos sensibles, implementación, Incidente de seguridad informática, metodología

GRADUATE SCHOOL

DEVELOPMENT OF A METHODOLOGY FOR MANAGING COMPUTER SECURITY INCIDENTS WITH APPLICATION OF ISO 27001 AND NIST PROTOCOLS FOR THE MARÍA HOSPITAL

CRISTOPHER LEONEL RIVAS TURCIOS
WILMER FERNANDO ESQUIVEL MEJÍA

Abstract

The purpose of this study was to develop a methodology for managing cybersecurity incidents at María Hospital, based on ISO 27001 and ISO 27035 standards and the NIST cybersecurity framework. The study focused on improving the protection of clinical data and ensuring the continuity of medical services in the face of potential cyberattacks. A mixed-method approach was used, with a descriptive and explanatory scope. The sample included seven collaborators from the technical and administrative areas of information technology. Instruments such as Likert-scale surveys, interviews, SWOT analyses, and risk matrices were used to identify vulnerabilities, assess the level of institutional preparedness, and determine staff knowledge of regulations and protocols. The results showed that, although there is some familiarity with international standards, there are no clear policies or established procedures for responding to incidents. Furthermore, limitations in technological resources and staff training were detected. Based on these findings, a structured methodology adapted to the hospital context was proposed, divided into phases of prevention, detection, response, recovery, and continuous improvement,

with an emphasis on staff training and the formalization of safety processes.

Keywords: Sensitive data, implementation, cybersecurity incident, methodology

DEDICATORIA

A Dios y a la Virgen María, por darme la claridad, la fortaleza y la sabiduría necesarias para culminar este importante paso en mi vida. Sin su guía y bendición, este logro no habría sido posible.

A mi amada esposa y a mi querida hija, por ser mi soporte incondicional, mi motivación constante y el refugio de amor y comprensión que necesitaba para salir avante en este proceso, gracias por caminar conmigo, por creer en mí y por ser parte esencial de este logro, que también les pertenece. Con todo mi amor y gratitud.

Cristopher Leonel Rivas Turcios

Primeramente, quiero dedicarle este trabajo a Dios por todo su apoyo y darme la sabiduría para seguir adelante a pesar de todas las adversidades.

También a mi familia, padre, madre y hermano por su apoyo y darme ánimo para nunca rendirme y seguir siempre en buen camino, siempre creyendo en mi en todo momento y preocupándose por algunos momentos duros y por último y no menos importante a mi compañero Cristopher por el apoyo que me dio al momento de trabajar juntos y siempre esforzarnos en gran manera.

Wilmer Fernando Esquivel Mejia

AGRADECIMIENTO

Expreso mi más sincero agradecimiento a los docentes que me acompañaron a lo largo de este proceso académico, brindándome su apoyo, orientación y consejo en cada etapa del camino. Su compromiso con la formación de profesionales íntegros y su dedicación en la enseñanza fueron fundamentales para la culminación de este proyecto.

De manera especial, agradezco al **asesor metodológico Master Jorge Raúl Maradiaga Chirinos**, por su invaluable guía, paciencia y disposición para orientar cada parte del desarrollo de esta investigación. Su experiencia y compromiso fueron clave para darle estructura y sentido al presente trabajo.

Asimismo, extiendo mi gratitud al **Lic. Adonys Santos** y a la **Lic. Lorena Arana**, quienes, con profesionalismo y generosidad, facilitaron la información y el apoyo necesarios para llevar a cabo este estudio en el Hospital María. Su colaboración fue determinante para la recopilación de datos y el cumplimiento de los objetivos planteados.

A todos ustedes, gracias por ser parte esencial de este logro.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

El presente trabajo de investigación tiene como propósito desarrollar una metodología para la gestión de incidentes de seguridad informática en el Hospital María, con base en estándares internacionales como la ISO 27001, ISO 27035 y el marco de ciberseguridad del NIST. La creciente digitalización de los servicios de salud ha expuesto a las instituciones médicas a múltiples riesgos cibernéticos, lo cual hace urgente la implementación de estrategias formales que aseguren la confidencialidad, integridad y disponibilidad de los datos clínicos.

En el **Capítulo I** se expone el planteamiento del problema, evidenciando la ausencia de políticas y procedimientos estandarizados en el Hospital María para responder ante incidentes de seguridad. Asimismo, se establecen los objetivos de la investigación, las preguntas que orientan el estudio y la justificación de su relevancia para el fortalecimiento institucional.

El **Capítulo II** desarrolla el marco teórico, abordando conceptos clave sobre gestión de incidentes, ciberseguridad, normativas internacionales y nacionales, así como las amenazas y vulnerabilidades específicas del sector salud. Se analiza el contexto global y nacional, y se revisan marcos de referencia como el NIST, la ISO 27001, la ISO 27032, la ISO 27799 y modelos de informática forense, resaltando su aplicabilidad en entornos hospitalarios.

En el **Capítulo III** se describe la metodología de investigación empleada, la cual tuvo un enfoque mixto, con alcances descriptivo y explicativo. La población objeto del estudio estuvo conformada por el personal técnico y administrativo del área de tecnologías de la información del Hospital María. Se aplicaron encuestas estructuradas, entrevistas semiestructuradas, análisis FODA y matrices de riesgo para evaluar el estado actual de la seguridad informática en la

institución.

El **Capítulo IV** presenta los resultados del análisis de datos. Se identificaron deficiencias significativas en cuanto a políticas institucionales, protocolos de respuesta, infraestructura tecnológica y formación del personal. Si bien se constató que los colaboradores poseen conocimientos básicos sobre normas como ISO/NIST, no se cuenta con una estrategia clara ni herramientas suficientes para gestionar adecuadamente los incidentes.

En el **Capítulo V** se exponen las conclusiones y recomendaciones. Se determinó la necesidad de adoptar una metodología estructurada que permita fortalecer la capacidad de detección, respuesta y recuperación ante incidentes de seguridad informática. Como propuesta final, se planteó un modelo metodológico adaptado al contexto del Hospital María, con base en buenas prácticas internacionales, estructurado en fases e integrado con medidas de capacitación, documentación y controles técnicos.

En el **Capítulo VI** se desarrolla la propuesta. Se originó la necesidad de proponer una metodología en gestión de incidentes basado en ISO 27001/NIST para facilitar el trabajo y proteger la seguridad del Hospital María, a su vez se explica con detalle como se organizaron las diferentes herramientas para el desarrollo de la propuesta y poder capacitar, fortalecer y mantener una política clara y concisa para mayor efectividad.

1.2 ANTECEDENTES DEL PROBLEMA

La seguridad de la información en el sector salud ha adquirido una importancia creciente debido al aumento de ciberataques dirigidos a instituciones médicas. Estos ataques no solo comprometen la confidencialidad de los datos de los pacientes, sino que también ponen en riesgo la continuidad operativa de los servicios de salud. Un caso emblemático es el ciberataque al

Hospital Clínic de Barcelona en marzo de 2023, donde se sustrajeron 4,5 terabytes de información confidencial, evidenciando la ausencia de medidas de seguridad adecuadas y un análisis de riesgos insuficiente (Coll, 2024) Este incidente destaca la urgencia de implementar metodologías estandarizadas para la gestión de incidentes de seguridad informática en entornos hospitalarios.

La creciente digitalización en el sector salud ha incrementado la superficie de ataque, exponiendo a las instituciones a diversas ciberamenazas. Según datos del Instituto Nacional de Ciberseguridad (González J. D., 2025), el 60% de los ciberataques en el sector salud son perpetrados por delincuencia organizada con motivaciones económicas, afectando principalmente a centros asistenciales y hospitales (González J. D., 2025). Esta tendencia resalta la necesidad de fortalecer las defensas cibernéticas en el ámbito sanitario.

A pesar de la existencia de marcos normativos como la Directiva NIS-2 y el Reglamento DORA, diseñados para mejorar la gestión de riesgos y la notificación de incidentes en sectores críticos, incluyendo la salud, muchas instituciones aún carecen de procesos estandarizados para la gestión de incidentes. La implementación efectiva de estas normativas es esencial para robustecer la ciberseguridad en hospitales y asegurar la continuidad de los servicios médicos. La Directiva NIS-2, por ejemplo, establece requisitos específicos para la seguridad de las redes y sistemas de información en el sector salud, promoviendo la cooperación entre los Estados miembros y estableciendo obligaciones claras en materia de seguridad y notificación de incidentes (Ciberseguridad, 2025).

La Comisión Europea ha reconocido esta problemática y ha propuesto la creación de un centro paneuropeo de ciberseguridad para proteger a hospitales y proveedores sanitarios de ciberataques. Este centro, que formará parte de la Agencia de la UE para Ciberseguridad (ENISA), ofrecerá orientación personalizada, herramientas, servicios y entrenamiento para mejorar la

resiliencia de las instituciones sanitarias ante ciberamenazas (Ayuso, 2025). Se espera que esta iniciativa, que contempla un plan de acción de dos años, esté operativa en el segundo semestre de 2025, proporcionando un entorno más seguro para pacientes y profesionales de la salud.

Mientras estas iniciativas se desarrollan, es crucial que los hospitales implementen sus propias metodologías de gestión de incidentes adaptadas a sus contextos específicos. La ausencia de una metodología estandarizada puede conducir a respuestas descoordinadas y poco efectivas ante ciberataques, poniendo en riesgo la información sensible de los pacientes y la operatividad de los servicios médicos. Por lo tanto, es imperativo que las instituciones de salud desarrollen e implementen procesos claros y estructurados para la gestión de incidentes, basados en las mejores prácticas y marcos normativos vigentes.

La implementación de un plan de respuesta a incidentes de seguridad cibernética es fundamental para mitigar los riesgos asociados. Este plan debe incluir la identificación y evaluación de riesgos, la implementación de medidas preventivas, la promoción de una cultura de seguridad y la gestión de emergencias. Además, es esencial realizar auditorías regulares de sistemas y accesos, aplicar políticas de seguridad en dispositivos móviles utilizados por el personal y utilizar conexiones seguras para proteger los datos en tránsito (Legapin, 2025).

La formación y concienciación del personal sanitario en materia de ciberseguridad también juegan un papel crucial. La capacitación en concienciación de seguridad, el uso de tecnologías avanzadas de protección de datos y una gestión de acceso rigurosa pueden fortalecer la seguridad en hospitales y clínicas, asegurando la privacidad del paciente y la continuidad de los servicios críticos (Ciber-seguridad, 2025).

Los incidentes recientes y las iniciativas regulatorias resaltan la importancia de contar con metodologías estandarizadas para la gestión de incidentes de seguridad informática en hospitales.

El desarrollo e implementación de estas metodologías permitirán a las instituciones de salud responder de manera efectiva a las ciberamenazas, protegiendo la información de los pacientes y asegurando la continuidad de los servicios médicos. La colaboración entre organismos internacionales, gobiernos y las propias instituciones sanitarias es esencial para crear un entorno seguro y resiliente frente a las ciberamenazas en el sector salud.

El sistema de salud pública en Honduras enfrenta importantes desafíos en términos de infraestructura, gestión y seguridad de la información. Según estudios recientes, los hospitales públicos del país operan con recursos limitados, sistemas de información desactualizados y una deficiente inversión en tecnología (Andino R, 2022). La digitalización en el sector salud ha avanzado lentamente, lo que ha provocado que muchas instituciones médicas dependan de sistemas manuales o bases de datos locales sin medidas de seguridad adecuadas. Además, informes del Observatorio de la Salud de Honduras señalan que el 80% de los hospitales públicos carecen de protocolos estandarizados para la protección de datos de los pacientes, aumentando el riesgo de ciberataques y filtraciones de información (Hernández, 2021). Esta vulnerabilidad es particularmente preocupante, dado el incremento de ataques de ransomware y accesos no autorizados a registros médicos en instituciones de salud de América Latina.

En el contexto hondureño, la falta de políticas de ciberseguridad en el sector hospitalario representa un obstáculo para la modernización de los sistemas de información de salud. Un estudio de la Universidad Nacional Autónoma de Honduras (UNAH) indica que menos del 15% de los hospitales públicos cuentan con una estrategia formal de gestión de incidentes en seguridad informática (Martínez, 2022)Esta situación se agrava debido a la escasez de personal capacitado en ciberseguridad y la limitada asignación presupuestaria para la actualización de equipos tecnológicos. A nivel gubernamental, el Reglamento de Tecnologías de Información y

Comunicación del Sector Público (2022) establece lineamientos generales para la seguridad digital, pero su implementación en hospitales es mínima. En este sentido, se hace evidente la necesidad de desarrollar metodologías de gestión de incidentes adaptadas a la realidad nacional, con el fin de garantizar la protección de datos médicos y la continuidad operativa de los hospitales públicos en Honduras.

1.3 DEFINICIÓN DEL PROBLEMA

El Hospital María no cuenta con una metodología normalizada para administrar incidentes de seguridad informática y está en serio riesgo de sufrir ciberataques. La falta de procesos definidos puede conducir a respuestas inadecuadas y desorganizadas, lo que a su vez podría afectar la confidencialidad, integridad y disponibilidad de la información del paciente y la provisión de servicios médicos. Por lo tanto, básica e imperativamente, esta deficiencia debe ser abordada por una metodología de respuesta a incidentes desarrollada e introducida para adaptarla a los requerimientos en el área de TIC.

1.4 PREGUNTAS DE INVESTIGACIÓN

1.4.1 PREGUNTA GENERAL

¿Cómo puede el Hospital María desarrollar una metodología estandarizada para la gestión de incidentes de seguridad informática que garantice la protección de la información y la continuidad de los servicios médicos?

1.4.2 PREGUNTAS ESPECÍFICAS

1. ¿Cuáles son las principales vulnerabilidades y amenazas de seguridad informática a las que está expuesto el Hospital María?
2. ¿Qué marcos normativos y mejores prácticas existen para la gestión de incidentes

de seguridad informática en el sector salud?

3. ¿Qué recursos y capacidades actuales posee el Hospital María para la gestión de incidentes de seguridad informática?
4. ¿Cómo se puede diseñar e implementar una metodología de gestión de incidentes que se adapte a las necesidades y contexto del Hospital María?

1.5 OBJETIVOS DEL PROYECTO

1.5.1 OBJETIVO GENERAL

Proponer el desarrollo de una metodología estandarizada para la gestión de incidentes de seguridad informática en el Hospital María, con el fin de garantizar la protección de la información y la continuidad de los servicios médicos.

1.5.2 OBJETIVOS ESPECÍFICOS

1. Identificar y analizar las principales vulnerabilidades y amenazas de seguridad informática que afectan al Hospital María.
2. Examinar y mejorar los marcos normativos y mejores prácticas aplicables a la gestión de incidentes de seguridad informática en el sector salud.
3. Inspeccionar los recursos y capacidades actuales del Hospital María para la gestión de incidentes de seguridad informática.
4. Proponer una metodología factible de implementar para la gestión de incidentes de seguridad informática en el Hospital María, alineada con los estándares ISO 27001, ISO 27035 y NIST.

1.6 JUSTIFICACIÓN

La creciente dependencia de los sistemas informáticos en el sector salud y el aumento de ciberataques dirigidos a hospitales han puesto en evidencia la necesidad de contar con metodologías efectivas para la gestión de incidentes de seguridad informática. Instituciones médicas, como el Hospital María, manejan información altamente sensible de los pacientes, cuya confidencialidad, integridad y disponibilidad deben garantizarse en todo momento. La ausencia de un enfoque estructurado para responder a incidentes puede comprometer la operatividad del hospital, afectando la calidad del servicio y poniendo en riesgo la seguridad de los datos.

Este estudio es relevante porque busca desarrollar una metodología de gestión de incidentes que permita al Hospital María mejorar su capacidad de detección, respuesta y recuperación ante amenazas cibernéticas. La implementación de un marco metodológico adaptado no solo fortalecerá la seguridad de la información, sino que también garantizará el cumplimiento de normativas internacionales y nacionales en materia de ciberseguridad. Además, el proyecto contribuirá a la mejora continua de los procesos internos, minimizando el impacto de posibles ataques y optimizando los recursos tecnológicos y humanos del hospital.

Desde una perspectiva práctica, la metodología propuesta servirá como referencia para otras instituciones de salud que enfrentan desafíos similares en la protección de sus sistemas de información. La seguridad en el sector hospitalario es fundamental para la confianza de los pacientes y la continuidad de los servicios médicos. Por lo tanto, contar con una estrategia bien definida para la gestión de incidentes permitirá reducir riesgos, mejorar la resiliencia institucional y promover una cultura de seguridad digital dentro del hospital.

Este estudio no solo responde a una necesidad crítica del Hospital María, sino que también aporta valor al sector salud en general. Al establecer un modelo de gestión de incidentes de

seguridad informática, se sentarán las bases para una respuesta más efectiva ante amenazas digitales, protegiendo tanto a la institución como a los pacientes que dependen de sus servicios.

CAPÍTULO II. MARCO TEÓRICO

2.1 MACROENTORNO GLOBAL

2.1.1 INTRODUCCIÓN DE GESTIÓN DE INCIDENTES

La Gestión de Incidente nos permite poder corregir problema y mejorar significativamente los procesos u estrategia, según (Maus, 2024) es un requisito fundamental para el funcionamiento seguro y sin problemas de una empresa u organización, además de ser fundamental la gestión de incidentes es un componente central de la gestión de servicios de TI (ITSM). Su objetivo es identificar, documentar y resolver de manera rápida y eficaz las interrupciones o disrupciones en las operaciones. Este proceso permite minimizar el impacto negativo de eventos inesperados en las operaciones del servicio y restablecer la funcionalidad normal lo más rápido posible. Los incidentes pueden incluir una amplia gama de fallas, desde problemas técnicos hasta incidentes relacionados con la seguridad. Incluyen cualquier cosa que impida o perjudique el funcionamiento normal.

La gestión de incidentes tiene un enfoque estructurado que incluye:

- una estructura de escalada clara
- comunicación efectiva
- formas definidas de priorizar incidentes y de mejora continua.

También hay que tener en cuenta que no se debe de confundir 2 términos como ser la gestión de Incidentes y la gestión de problema, ambos trabajan de la manera, pero cada uno desempeña su propia función, como ser lo siguiente:

Tabla 1: Diferencia entre Incidentes y Problemas

La Gestión de Incidentes	Gestión de problemas

Es una interrupción a corto plazo o un evento inesperado que altera las operaciones normales de una empresa y que debe resolverse rápidamente	Es una causa subyacente de una interrupción que conduce a incidentes recurrentes
Se centra en soluciones sostenibles para evitar una interrupción en una empresa	Identifica y aplica un análisis de la causa raíz para implementar soluciones a largo plazo

2.1.2 MEDIDAS BÁSICAS GESTIÓN DE INCIDENTES

La gestión de incidentes es una responsabilidad permanente que implica la vigilancia para seguir los pasos adecuados con el fin de mantener el lugar de trabajo a salvo de los riesgos identificados, con lo que a continuación (SafetyCulture, 2024) exponen las medidas básicas de gestión de incidentes que se debe aplicar en el lugar de trabajo.

Figura 1: Medidas básicas para la gestión de incidentes

Paso 1: Notificación de Incidentes

El primer paso vital en la gestión de incidentes que da a conocer un incidente y provoca la acción correspondiente es la notificación de incidentes. Toda la información que pueda contribuir a la comprensión del incidente debe ser recogida y comunicada inmediatamente.

¿Qué información se debe de reunir para un informe de incidente?

Según lo mencionan. Al recopilar información para un informe de incidente, la persona responsable de informar debe pedir lo siguiente:

- Qué tipo de incidente ocurrió
- ¿Quiénes son las personas implicadas?
- ¿Dónde se produjo el incidente?
- ¿Cuándo ocurrió el incidente?
- La gravedad del incidente y, si es posible, el motivo de este.

Paso 2: Acción Correctiva

Dado que los incidentes en el lugar de trabajo se anticiparon sobre la base de los riesgos identificados, deben aplicarse las acciones correctivas correspondientes para mitigar el impacto negativo de los incidentes y evitar que se repitan. Lo ideal es que las acciones correctivas se supervisen para garantizar que se completan y que se consigue el resultado deseado.

Paso 3: Investigación y análisis

Para mantener el buen funcionamiento y la seguridad en el lugar de trabajo, los riesgos y peligros conocidos se mantienen a raya mediante la aplicación de controles que eliminan la posibilidad de que se produzcan incidentes o mitigan su impacto. Si se produce un incidente y éste tiene un impacto moderado en la empresa o es grave, se requiere una investigación para recopilar

más información que se analizará para llegar a la causa raíz del incidente y proponer mejores controles para su aplicación.

Llevar a cabo un análisis de la causa raíz o seguir el proceso CAPA puede ayudar a descubrir posibles lagunas de seguridad y llegar a la causa principal de un incidente y aplicar controles más proactivos.

Una investigación de incidentes puede implicar la recopilación de datos personales de las personas implicadas en el incidente, así como de información sensible procedente de documentos, fotos y otros medios que pueden ayudar a comprender mejor la secuencia de acontecimientos que condujeron al incidente. El uso de herramientas de confianza con acceso a un almacenamiento de datos seguro puede ayudar a mantener la privacidad de la información y el cumplimiento de las normas del sector.

Paso 4: Cierre del incidente

El último paso es el cierre del informe de incidentes tras comprobar si se han completado los pasos anteriores. El cierre del incidente ayuda a verificar si se ha determinado la causa raíz de este, si se han completado las acciones correctivas y si se ha aplicado lo aprendido para mejorar los procesos con el fin de afinar continuamente las medidas de seguridad en el lugar de trabajo.

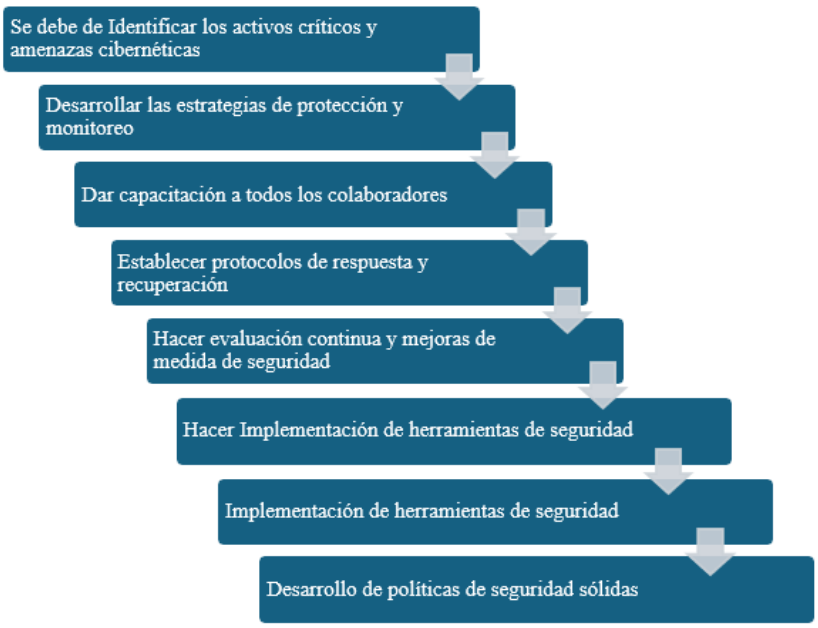
2.1.3 APLICACIÓN ISO 27032

(Global Trust Association, 2025) nos dice que para aplicar la ISO 27032:2023, las organizaciones se necesita seguir un enfoque estructurado antes de comenzar con las medidas básicas:

1. **Identificación de activos críticos y amenazas cibernéticas:** Esto permite poder crear un listado de diferentes activos que se pueden analizar para gestionarlo como ser: hardware, software, redes, datos entre otros

2. **Desarrollo de estrategias de protección y monitoreo en tiempo real:** Se encarga de poder anticipar todos los activos ya identificados en el primer punto para tomar medidas respecto a ello
3. **Capacitación y concienciación en ciberseguridad para todos los colaboradores:** Esto es demasiado importante porque permite poder entrenar a los colaboradores para prevenir incidentes que pueda afectar a la empresa
4. **Establecimiento de protocolos de respuesta y recuperación ante incidentes de seguridad:** Gracias a este paso nos permite poder reaccionar antes futuras amenazas y poder recuperarse ante cualquier incidente que se sufra
5. **Evaluación continua y mejora de medidas de seguridad para adaptarse a nuevas amenazas:** Este proceso implica poder evaluar continuamente los procesos y hacer análisis para poder identificar posibles debilidades y poder ajustar las estrategias
6. Implementación de herramientas de seguridad avanzadas como firewalls, antivirus, sistemas de detección de intrusos y soluciones de cifrado.
7. Colaboración con organismos internacionales y redes de seguridad para compartir información sobre amenazas emergentes.
8. Desarrollo de políticas de seguridad sólidas que contemplen la protección de datos personales y confidenciales.

Figura 2: Implementación ISO 27032



2.1.4 BENEFICIOS DE LA IMPLEMENTACIÓN ISO 27032

Adoptar las directrices de la ISO 27032:2023 trae consigo múltiples ventajas, tanto para las organizaciones como para los profesionales de la ciberseguridad como:

1. **Protección de la información y los sistemas digitales:** Al poder implementar la ISO 27032 esto permitirá hacerles frente a amenazas cibernéticas emergentes.
2. **Mejor gestión de riesgos** Ayuda a poder planear un buen sistema de detección de incidentes mediante estrategias preventivas y correctivas.
3. **Mayor confianza de clientes y socios comerciales** Al tener una mejor gestión, esto ayudará a demostrar a los clientes y socios un enfoque proactivo en seguridad.
4. **Resiliencia ante ataques cibernéticos** Mediante planes de respuesta y recuperación efectivos, se podrá tener una mejor protección de los datos y garantizar la seguridad.

5. **Cumplimiento de regulaciones internacionales:** Es fundamental para cualquier entidad que opere a nivel global, como materia de ciberseguridad y privacidad de datos, acceso a mercados internacionales, mejora de procesos internos y demás.
6. **Fortalecimiento de la colaboración:** Fomenta la comunicación entre distintos colaboradores para combatir el cibercrimen, como medidas de seguridad unas otras estrategias.
7. **Reducción de pérdidas financieras** al minimizar incidentes de seguridad y sus consecuencias económicas.
8. **Mejora continua en la protección de la infraestructura tecnológica**: Garantiza una buena mejora continua de la protección mediante auditorías y evaluaciones regulares.

Figura 3: Beneficios de implementar ISO 27032

2.1.5 IDENTIFICACIÓN Y ANÁLISIS DE VULNERABILIDAD Y AMENAZAS EN EL SECTOR SALUD A NIVEL INTERNACIONAL

La ciberseguridad en el sector salud enfrenta desafíos significativos a nivel global debido al incremento de amenazas cibernéticas dirigidas a hospitales y sistemas de información médica. Según un estudio de (Cybersecurity Ventures, 2024), los ataques de ransomware dirigidos a instituciones sanitarias han aumentado en más del 70% en la última década, poniendo en riesgo la integridad y disponibilidad de la información de los pacientes.

Las principales amenazas identificadas en el sector salud incluyen:

- **Ransomware**: Ataques que cifran la información de los hospitales, exigiendo un rescate para su liberación.
- **Phishing y ataques de ingeniería social:** Intentos de obtener credenciales de acceso mediante correos electrónicos fraudulentos.
- **Intrusiones en redes hospitalarias:** Accesos no autorizados a bases de datos y sistemas críticos de gestión médica.
- **Malware especializado:** Programas diseñados para manipular o extraer información de dispositivos médicos conectados a la red.

Casos como el ciberataque al Hospital Clínic de Barcelona en 2023, donde se sustrajeron 4,5 terabytes de información confidencial, subrayan la urgencia de implementar mejores estrategias de ciberseguridad en hospitales a nivel global.

2.1.6 MARCOS NORMATIVOS Y MEJORES PRÁCTICAS INTERNACIONALES

Dado el impacto de los ataques cibernéticos en el sector salud, organismos internacionales han desarrollado regulaciones y marcos normativos que buscan fortalecer la resiliencia de las instituciones médicas. Entre los más destacados se encuentran:

- **Directiva NIS-2 (Unión Europea):** Obliga a los proveedores de servicios críticos, incluyendo hospitales, a reforzar sus medidas de ciberseguridad y notificar incidentes en un plazo determinado (ENISA, 2023).
- **Reglamento DORA:** Diseñado para mejorar la resiliencia cibernética de sectores críticos, garantizando la protección de los datos de salud.
- **HIPAA (Estados Unidos):** Regula la protección de datos de los pacientes y establece sanciones en caso de incumplimiento.
- **ISO 27799:** Estándar internacional que establece directrices específicas para la gestión de la seguridad de la información en el sector salud.

La implementación de estos marcos normativos es clave para mitigar riesgos en hospitales y garantizar la continuidad de los servicios médicos en entornos digitales cada vez más vulnerables.

2.1.7 INFORMÁTICA FORENSE Y EVIDENCIA DIGITAL

La incorporación de blockchain como estrategia para mejorar la seguridad de la información en diversos sectores de la sociedad se ha identificado como una potencial solución para reducir los riesgos asociados con el tratamiento de datos en Internet. Garantizar la cadena de custodia en investigaciones forenses es esencial para preservar el registro y procedencia de la

evidencia digital.

En este estudio se aborda la metodología y las pautas. El cual se centra en explorar el estado actual de BC en el dominio de la CoC como mecanismo para garantizar la integridad y trazabilidad en evidencia digital. El SMS permitió recopilar y clasificar las características utilizadas en el diseño y construcción de BC específicas para el dominio de la CoC en evidencia digital. También se identificó los beneficios, limitaciones y desafíos presentados por los autores, que permitirán aclarar el panorama actual de BC con relación a la CoC, además de apoyar futuros trabajos en este ámbito. El SMS se divide en diferentes pasos secuenciales, aplicación de criterios y filtros como se muestra en la Figura 1 de la sección de metodología propuesta por (Pablo A. Vaca, 2024).

Figura 4: Metodología basado en Informática forense

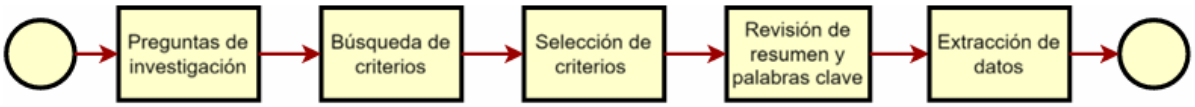


Figura 1. Proceso de mapeo sistemático basado en [31]. Fuente: elaboración propia.

2.1.8 CICLO DE VIDA DE RESPUESTA A INCIDENTES DE SANS

El SANS Institute propone un modelo estructurado para la respuesta a incidentes, que comprende seis fases:

1. **Preparación**: Desarrollo de políticas, procedimientos y formación del personal en ciberseguridad.
2. **Identificación**: Detección de incidentes mediante sistemas de monitoreo y análisis forense digital.
3. **Contención**: Implementación de estrategias para evitar la propagación de

amenazas dentro de la red hospitalaria.

4. **Erradicación**: Eliminación de amenazas y restauración de sistemas afectados.
5. **Recuperación**: Reintegración de sistemas con medidas de seguridad reforzadas.
6. **Lecciones aprendidas**: Evaluación del incidente y ajustes en la estrategia de seguridad para mejorar futuras respuestas.

Este enfoque es fundamental para los hospitales, ya que permite estructurar un protocolo eficiente de respuesta ante ataques cibernéticos como ransomware o brechas de seguridad en datos sensibles (Bromiley, 2019).

2.2 MICROENTORNO EN HONDURAS.

2.2.1 ANÁLISIS DE VULNERABILIDADES Y AMENAZAS EN EL HOSPITAL MARÍA

En el contexto hondureño, el Hospital María enfrenta una serie de vulnerabilidades que lo hacen un objetivo atractivo para ciberataques. Según el Instituto Nacional de Ciberseguridad de Honduras (INCIBE-HN, 2025), más del 60% de las instituciones de salud en el país no cuentan con planes de respuesta a incidentes cibernéticos.

Entre los principales riesgos identificados en el hospital se encuentran:

- Uso de sistemas informáticos obsoletos, lo que aumenta la vulnerabilidad ante ataques de malware.
- Ausencia de protocolos de seguridad en el manejo de datos sensibles de los pacientes.
- Deficiencia en la capacitación del personal administrativo y médico en temas de

ciberseguridad.

- Conectividad deficiente y ausencia de segmentación de red en los sistemas informáticos hospitalarios.

Estos factores elevan la probabilidad de que el hospital sea víctima de ataques cibernéticos, afectando la calidad de la atención médica y la seguridad de los datos de los pacientes.

2.2.2 EVALUACIÓN DE MARCOS NORMATIVOS Y MEJORES PRÁCTICAS EN HONDURAS

Honduras cuenta con ciertas regulaciones en materia de ciberseguridad y protección de datos, aunque su implementación en el sector salud sigue siendo limitada. Algunas normativas relevantes incluyen:

- **Ley de Protección de Datos Personales (Decreto No. 58-2020):** Regula el tratamiento de la información de los pacientes y establece principios básicos de seguridad.
- **Estrategia Nacional de Ciberseguridad 2023-2028:** Busca fortalecer la infraestructura de ciberseguridad en el país, aunque su aplicación en el sector salud es mínima.
- **Reglamento de Tecnologías de Información y Comunicación del Sector Público (2022):** Establece lineamientos generales para la seguridad informática en instituciones gubernamentales.

A pesar de estos esfuerzos, el país carece de normativas específicas dirigidas a la ciberseguridad hospitalaria, lo que deja a los hospitales públicos sin guías claras para la gestión de incidentes.

2.2.3 EVALUACIÓN DE RECURSOS Y CAPACIDADES DEL HOSPITAL MARÍA

El hospital presenta deficiencias significativas en recursos tecnológicos y humanos para la gestión de incidentes de ciberseguridad. Entre los desafíos identificados están:

- Limitado presupuesto para inversión en sistemas de seguridad informática.
- Escasez de profesionales especializados en ciberseguridad hospitalaria.
- Falta de herramientas avanzadas para la detección y mitigación de amenazas cibernéticas.

No obstante, existen oportunidades de mejora mediante la implementación de protocolos de seguridad, la capacitación del personal y la adquisición de tecnologías de prevención de ataques.

2.3 TEORÍAS DE SUSTENTO

La gestión de incidentes en seguridad informática en hospitales se fundamenta en diversas teorías y modelos que han sido desarrollados para mejorar la protección de la información y garantizar la continuidad de los servicios médicos. Estas bases teóricas permiten estructurar un enfoque metodológico sólido que facilite la identificación, mitigación y recuperación de incidentes de ciberseguridad.

2.3.1 MODELO DE GESTIÓN DE INCIDENTES DEL NIST

El National Institute of Standards and Technology (NIST) ha desarrollado un marco de referencia ampliamente utilizado para la gestión de ciberseguridad en organizaciones. Su enfoque está basado en cinco funciones clave:

1. **Identificación**: Determinar y comprender los activos tecnológicos y los riesgos

asociados.

2. **Protección**: Implementar salvaguardas para minimizar el impacto de los incidentes.
3. **Detección**: Monitorizar actividades inusuales y posibles amenazas.
4. **Respuesta**: Implementar acciones para contener y mitigar los incidentes de seguridad.
5. **Recuperación**: Restaurar los sistemas afectados y mejorar la resiliencia organizacional.

El NIST desarrolla estándares, directrices, mejores prácticas y otros recursos de ciberseguridad para satisfacer las necesidades de la industria, las agencias federales y el público en general de los EE. UU. Nuestras actividades van desde la producción de información específica que las organizaciones pueden poner en práctica de inmediato, hasta la investigación a más largo plazo que anticipa los avances en las tecnologías y los desafíos futuros.

El NIST también avanza en la comprensión y mejora la gestión de los riesgos de privacidad, algunos de los cuales se relacionan directamente con la ciberseguridad. Las áreas prioritarias a las que contribuye el NIST, y en las que planea centrarse más, incluyen la criptografía, la educación y la fuerza laboral, las tecnologías emergentes, la gestión de riesgos, la gestión de identidades y accesos, las mediciones, la privacidad, las redes y las plataformas confiables.

En el contexto hospitalario, este modelo es esencial, ya que proporciona una estructura adaptable que permite a los hospitales responder de manera eficiente ante amenazas digitales y garantizar la protección de los datos de los pacientes (NIST, 2024)

2.3.2 INFORMÁTICA FORENSE Y EVIDENCIA DIGITAL

La informática forense es un campo clave en la gestión de incidentes, ya que permite la identificación, recolección, análisis y presentación de evidencia digital en el contexto de investigaciones de ciberseguridad. En hospitales, su aplicación es crucial para:

1. Determinar el origen y alcance de un ataque.
2. Identificar vulnerabilidades explotadas por ciberdelincuentes.
3. Recopilar pruebas que puedan ser utilizadas en procedimientos legales o auditorías internas.

El uso de herramientas de informática forense permite mejorar la capacidad del hospital para responder de manera eficiente a incidentes de seguridad, minimizando la pérdida de información y fortaleciendo la infraestructura tecnológica.

Como, por ejemplo, la aplicación de "Espejo Chubut" es una herramienta diseñada por el Departamento de Informática Forense del Ministerio Público Fiscal del territorio patagónico que evita la necesidad de la incautación de un elemento para la recopilación de sus pruebas. Es un programa informático que genera una copia solo de los chats, audios, imágenes y videos de cualquier plataforma o red social que sean relevantes para la causa que se investiga. Lo hace sin invadir el resto de los contenidos que no sean referentes al caso. (Villar, 2024)

2.3.3 MARCO DE SEGURIDAD DE LA INFORMACIÓN ISO 27001 E ISO 27799

Las normas internacionales ISO 27001 e ISO 27799 establecen directrices para la gestión de la seguridad de la información en el sector salud. Estas normas incluyen:

1. Definición de políticas de seguridad informática.

2. Gestión de riesgos en la infraestructura hospitalaria.
3. Requisitos para la protección de datos médicos y confidenciales.
4. Estrategias para garantizar la continuidad operativa ante incidentes.

Además, esta Norma Internacional proporciona orientación a las organizaciones sanitarias y a otros custodios de información personal de salud sobre la mejor manera de proteger la confidencialidad, integridad y disponibilidad de dicha información. Se basa en la guía general de la norma ISO/IEC 27002:2013 y la amplía, y aborda las necesidades específicas de gestión de la seguridad de la información del sector sanitario y sus entornos operativos únicos. Si bien la protección y la seguridad de la información personal son importantes para todas las personas, empresas, instituciones y gobiernos, existen requisitos especiales en el sector sanitario que deben cumplirse para garantizar la confidencialidad, integridad, auditabilidad y disponibilidad de la información personal de salud. Este tipo de información se considera, por muchos, uno de los tipos más confidenciales de información personal. Proteger esta confidencialidad es esencial para mantener la privacidad de los sujetos de atención. La integridad de la información sanitaria debe protegerse para garantizar la seguridad del paciente, y un componente importante de dicha protección es garantizar que todo el ciclo de vida de la información sea totalmente auditable. La disponibilidad de la información sanitaria también es fundamental para una prestación eficaz de la atención sanitaria. Los sistemas informáticos de salud deben satisfacer las demandas específicas para mantenerse operativos ante desastres naturales, fallos del sistema y ataques de denegación de servicio.

Su implementación en hospitales permite asegurar el cumplimiento de regulaciones internacionales y mejorar las prácticas de seguridad digital (Informatics, 2016).

Las bases teóricas presentadas sustentan la importancia de contar con una metodología estandarizada para la gestión de incidentes de seguridad informática en hospitales. Aplicar estos modelos permitirá al Hospital María fortalecer su capacidad de respuesta ante ciberamenazas, garantizar la protección de los datos de los pacientes y mejorar la resiliencia organizacional frente a ataques digitales.

2.3.4 TEORÍA DE LA RESILIENCIA ORGANIZACIONAL EN CIBERSEGURIDAD

La resiliencia organizacional en ciberseguridad se basa en la capacidad de una institución para anticiparse, resistir, recuperarse y adaptarse ante incidentes de seguridad informática. Según estudios recientes, las organizaciones de salud deben adoptar un enfoque integral que incluya tecnología, procesos y cultura organizacional para fortalecer su resiliencia digital (Medina Astudillo, 2022).

En el Hospital María, la falta de una metodología estructurada de gestión de incidentes pone en riesgo su capacidad de respuesta. Aplicar la teoría de resiliencia organizacional permite no solo reaccionar ante incidentes, sino también desarrollar estrategias preventivas que reduzcan su impacto y frecuencia.

Según (Editora El Sol, 2024) Esta concientización se extiende a los empleados, quienes desempeñan un papel crucial. Es fundamental que comprendan los riesgos y cuenten con capacitación en las mejores prácticas en materia de seguridad de la información. Solo a través de una estrategia integral y proactiva, las empresas podrán proteger sus activos digitales y mantenerse un paso adelante en el cambiante panorama de ciberseguridad. También destacó que la adopción de buenas prácticas internacionales, como las establecidas en la norma ISO 27001/ISO 27002,

puede ofrecer un sólido marco para una gestión de riesgos más eficiente. Además, recomendó a las empresas a trabajar en la creación de una cultura organizacional que promueva la conciencia y responsabilidad en materia de seguridad. Esto implica el compromiso activo de la alta dirección en la promoción de la seguridad cibernética como un pilar fundamental de la estrategia empresarial.

2.4 METODOLOGÍAS DESARROLLADAS

2.4.1 CIBERSEGURIDAD DEL NIST

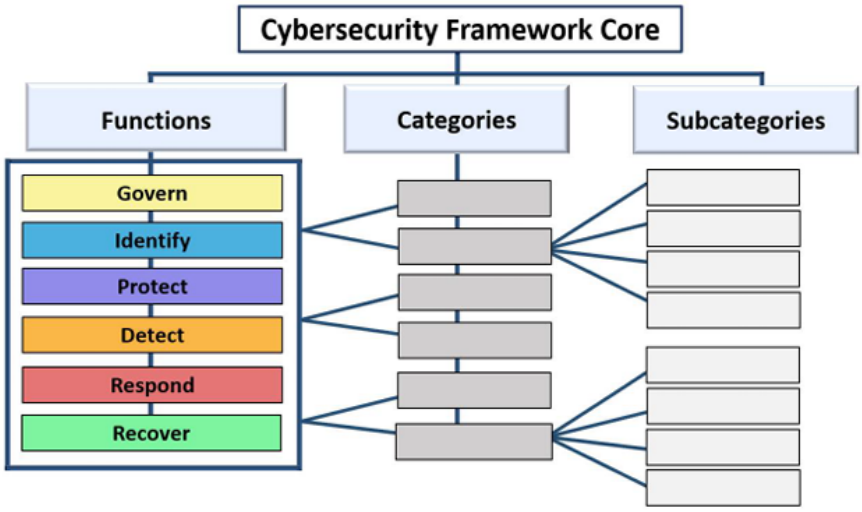
ANÁLISIS DE LA METODOLOGÍA NIST

El Marco de Ciberseguridad (CSF) 2.0 del NIST proporciona orientación a la industria, a las agencias gubernamentales y a otras organizaciones para gestionar los riesgos de ciberseguridad. Ofrece una taxonomía de resultados de ciberseguridad de alto nivel que puede utilizar cualquier organización, independientemente de su tamaño, sector o madurez, para comprender, evaluar, priorizar y comunicar mejor sus esfuerzos de ciberseguridad. El CSF no prescribe cómo se deben lograr los resultados. En cambio, ofrece enlaces a recursos en línea que brindan orientación adicional sobre las prácticas y los controles que podrían utilizarse para lograr esos resultados. Este documento describe el CSF 2.0, sus componentes y algunas de las muchas formas en que se puede utilizar. (NIST, 2024)

Núcleo de CSF

El núcleo del framework de ciberseguridad o su sigla en inglés CSF (**cibersecurity framework**) es un conjunto de resultados de ciberseguridad organizados por función, luego por categoría y, por último, por subcategoría, como se muestra en la Figura 4.

Figura 5: CSF



Estas funciones (**gobernar, identificar, proteger, detectar, responder y recuperar**) organizan los resultados de ciberseguridad en su nivel más alto

- **Gobernar:** Establecen, comunican y monitorean la estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización. Su función es proporcionar resultados para informar lo que una organización puede hacer para lograr y priorizar los resultados de las otras cinco funciones en el contexto de su misión y las expectativas de las partes interesadas.
- **Identificar:** Se comprenden los riesgos de ciberseguridad actuales de la organización, utilizando activos de la organización (**datos, hardware, software, sistemas, instalaciones, servicios, personas etc.**), esto permite a una organización priorizar sus esfuerzos de acuerdo con su estrategia de gestión de riesgos y las necesidades de la misión identificadas en la función de gobernar.
- **Proteger:** Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de la organización. Una vez que se identifican y priorizan los activos y los riesgos, respalda la

capacidad de asegurar esos activos para prevenir o reducir la probabilidad de un daño, así como para aumentar el impacto de aprovechar las oportunidades.

- **Detectar:** Se analizan posibles ataques y vulnerabilidades de seguridad cibernética. Esta función respalda las actividades de respuesta y recuperación ante incidentes exitosas.
- **Responder:** Se toman medidas en relación con un incidente de ciberseguridad detectada y apoya la capacidad de contener los efectos de los incidentes de ciberseguridad. Los resultados dentro de esta función abarcan la gestión, el análisis, la mitigación, la generación de informes y la comunicación de incidentes.
- **Recuperar:** Se restauran los activos y las operaciones afectadas por un incidente de ciberseguridad, que ayuda a respalda la restauración oportuna de las operaciones normales para reducir los efectos de los incidentes de ciberseguridad y permitir una comunicación adecuada durante las tareas de recuperación.

Figura 6: Funciones de CSF

Perfiles y niveles del CFS

Un perfil organizacional de CSF describe la postura actual o futura de una organización en materia de ciberseguridad en términos de los resultados del núcleo. Los perfiles organizacionales se utilizan para comprender, adaptar, evaluar, priorizar y comunicar los resultados del núcleo al considerar los objetivos de la misión de una organización, las expectativas de las partes interesadas, el panorama de amenazas y los requisitos.

Cada perfil organizacional incluye uno o ambos. Los perfiles son los siguientes:

- **Un perfil actual:** especifica los resultados principales que una organización está logrando actualmente (o intentando lograr) y caracteriza cómo o en qué medida se está logrando cada resultado.
- **Un perfil objetivo:** especifica los resultados deseados que una organización ha seleccionado y priorizado para lograr sus objetivos de gestión de riesgos de ciberseguridad.

Los pasos que se muestran en la Figura 6 ilustran una forma en que una organización podría utilizar un Perfil Organizacional para ayudar a informar la mejora continua de su ciberseguridad.

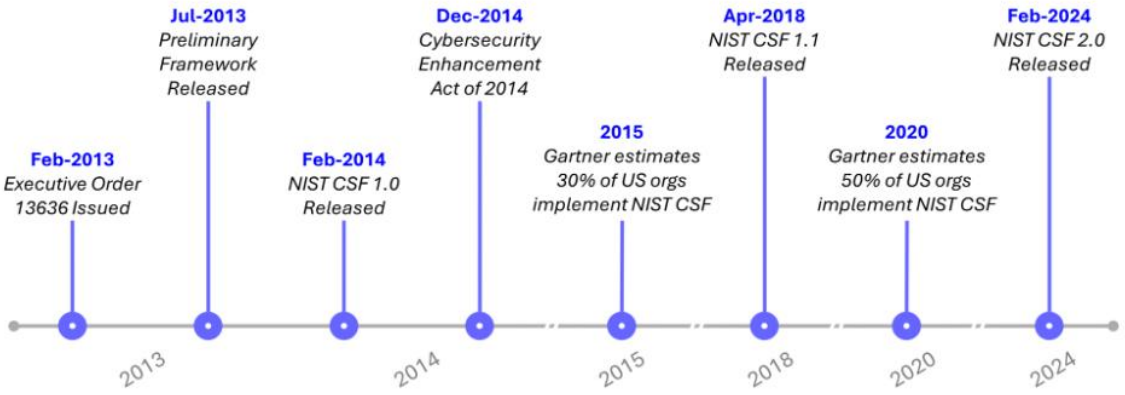
Figura 7: Creación de un perfil organización en CSF

ANTECEDENTES DE LA METODOLOGÍA NIST

Lo que nos confirma (Ellinger, 2024). En 2013, el presidente Obama publicó una orden ejecutiva titulada "Mejora de la ciberseguridad de la infraestructura crítica" en respuesta a las repetidas intrusiones en la infraestructura crítica de los Estados Unidos (plantas químicas, instalaciones de tratamiento de agua, etc.) La orden encargó al Instituto Nacional de Estándares y Tecnología (NIST) diseñar un marco para que las organizaciones del sector público y privado mitiguen los riesgos de ciberseguridad.

Más tarde, en 2014, el Congreso de los Estados Unidos aprobó la "Ley de Mejora de la Ciberseguridad de 2014". Esta ley alentó al NIST a continuar actualizando el Marco de manera continua. También alentó al sector privado a participar activamente en su elaboración, afirmando que ninguna información compartida por una entidad privada debía utilizarse para elaborar normas reglamentarias para esa entidad.

Figura 8: Evolución del NIST



ANÁLISIS CRÍTICO DE LA METODOLOGÍA NIST

El NIST será usada para ayudar a evitar o disminuir los problemas como incidentes o riesgos que pueda ocurrir dentro del Hospital María, utilizando lo que son las funciones del núcleo CSF, como lo siguiente:

Tabla 2: Aplicación del NIST

Función	**Categoría**	**Identificador de Categoría**
Gobernar (GV)	Contexto Organizacional	GV.OC
	Estrategia de Gestión de Riesgos	GV.RM
	Roles, Responsabilidades y Autoridades	GV.RR
	Política	GV.PO
	Supervisión	GV.OV
	Gestión de Riesgos de la Cadena de Suministro de Ciberseguridad	GV.SC
Identificar (ID)	Gestión de Activos	ID.AM
	Evaluación de Riesgos	ID.RA
	Mejora	ID.IM
Proteger (PR)	Gestión de Identidad, Autenticación y Control de Acceso	PR.AA
	Concienciación y Capacitación	PR.AT
	Seguridad de Datos	PR.DS
	Seguridad de la Plataforma	PR.PS
	Resiliencia de la Infraestructura Tecnológica	PR.IR
Detectar (DE)	Monitoreo Continuo	DE.CM
	Análisis de Eventos Adversos	DE.AE

Responder (RS)	Gestión de Incidentes	RS.MA
	Análisis de Incidentes	RS.AN
	Informes y Comunicación de Respuesta a Incidentes	RS.CO
	Mitigación de Incidentes	RS.MI
Recuperar (RC)	Ejecución del Plan de Recuperación de Incidentes	RC.RP
	Comunicación de Recuperación de Incidentes	RC.CO

2.4.2 METODOLOGÍA BASADA EN ISO 27001

ANÁLISIS DE LA METODOLOGÍA DE LA NORMA ISO 27001

La norma ISO/IEC 27001 es un estándar internacional para la gestión de la seguridad de la información, diseñado para ayudar a las organizaciones a establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) (ISO/IEC, 2022). La creciente interconectividad de los sistemas de información y el aumento de amenazas cibernéticas han convertido a la ISO 27001 en una herramienta clave para garantizar la seguridad y continuidad de los negocios. Este informe analiza la metodología de la norma ISO 27001, destacando su estructura, principios y aplicación en la gestión de incidentes de seguridad.

ANTECEDENTES DE LA ISO 27001

La seguridad de la información ha evolucionado significativamente desde la aparición de los primeros sistemas computacionales en la mitad del siglo XX. Con el crecimiento de la

computación y el uso de redes interconectadas, surgió la necesidad de normativas que aseguraran la confidencialidad, integridad y disponibilidad de la información.

El establecimiento de normas internacionales comenzó con el estándar británico BS 7799 en la década de 1990, el cual sirvió como base para la creación de la ISO/IEC 27001 en 2005. Desde entonces, la norma ha evolucionado para adaptarse a los nuevos desafíos de ciberseguridad, como el auge del cloud computing, la inteligencia artificial y el Internet de las Cosas (IoT).

REVOLUCIÓN INDUSTRIAL ISO 27001

La actual Cuarta Revolución Industrial, también conocida como Industria 4.0, ha sido impulsada por el avance de las tecnologías digitales, incluyendo el big data, la automatización inteligente y la interconectividad global (Schwab, 2016). La creciente dependencia de estos sistemas ha elevado la importancia de la ciberseguridad y la gestión de la información, haciendo que la ISO 27001 sea un marco fundamental para garantizar la seguridad en entornos industriales y empresariales.

Los cambios tecnológicos han dado lugar a nuevas amenazas, como los ataques cibernéticos a infraestructuras críticas, el robo de datos personales y la manipulación de información. En este contexto, la ISO 27001 proporciona directrices para la resiliencia digital de las organizaciones y la mitigación de riesgos en un entorno cada vez más interconectado.

Uno de los desafíos más significativos de la Cuarta Revolución Industrial es la protección de sistemas interconectados contra ciberataques sofisticados, donde la ISO 27001 actúa como una guía para desarrollar estrategias de seguridad proactivas. La gestión eficiente de la seguridad de la

información no solo previene incidentes, sino que también fortalece la confianza del cliente y el cumplimiento normativo global.

ANÁLISIS CRÍTICO DE LA METODOLOGÍA ISO 27001

La metodología de la ISO 27001 sigue un enfoque basado en riesgos y se desarrolla en varias fases clave:

1. Contexto Organizacional

Antes de implementar un SGSI, la organización debe comprender su contexto, necesidades y expectativas de las partes interesadas. La norma requiere la identificación de los factores internos y externos que pueden afectar la seguridad de la información (ISO/IEC 27001:2022, cláusula 4.1). Esto implica realizar un análisis de la estructura organizativa, los activos críticos de información y los riesgos asociados a su entorno digital.

2. Análisis y Evaluación de Riesgos

El enfoque basado en riesgos es fundamental en la ISO 27001. La organización debe identificar activos, amenazas y vulnerabilidades para evaluar el impacto y la probabilidad de los riesgos asociados. Este análisis permite priorizar las acciones de mitigación y asignar recursos de manera efectiva para la protección de la información.

3. Implementación de Controles de Seguridad

La norma proporciona un conjunto de controles en su Anexo A, alineados con el marco de referencia (ISO/IEC 27002, 2022). Estos controles incluyen medidas técnicas, organizativas y de recursos humanos para mitigar los riesgos identificados (ISO/IEC 27002:2022). Entre los principales controles se encuentran:

- **Gestión de accesos**: Implementación de políticas de autenticación y autorización.
- **Protección de la red y sistemas**: Medidas de firewall, cifrado y detección de intrusos.

- **Concienciación y formación**: Programas de capacitación en ciberseguridad para empleados.
- **Gestión de incidentes**: Desarrollo de procedimientos de respuesta ante incidentes de seguridad.

4. Monitoreo y Mejora Continua

La mejora continua es un pilar clave de la norma. La organización debe llevar a cabo auditorías internas, revisiones de la alta dirección y aplicar acciones correctivas para asegurar la efectividad del SGSI (Deming, 1986). Este ciclo de mejora continua sigue el modelo PHVA (Planificar, Hacer, Verificar, Actuar) para garantizar la adaptación a nuevas amenazas y cambios regulatorios.

APLICACIÓN DE LA METODOLOGÍA EN LA GESTIÓN DE INCIDENTES

La gestión de incidentes de seguridad es un proceso esencial en el SGSI. Según la ISO/IEC 27035 (2016), la respuesta a incidentes sigue una serie de fases:

- **Detección y notificación**: Identificación temprana de incidentes mediante monitoreo continuo.
- **Evaluación y clasificación**: Determinación del impacto y severidad del incidente.
- **Respuesta y mitigación**: Contención, erradicación y recuperación del incidente.
- **Aprendizaje y mejora**: Implementación de medidas correctivas para prevenir incidentes futuros.

La gestión de incidentes permite minimizar el impacto de amenazas como ataques de ransomware, filtraciones de datos y accesos no autorizados a la información crítica. Empresas líderes en tecnología han demostrado que la adopción de un plan de respuesta a incidentes basado en ISO 27001 mejora significativamente la resiliencia organizacional.

La metodología de la ISO 27001 proporciona un marco estructurado para la gestión de la seguridad de la información, basado en un enfoque sistemático de identificación, evaluación y tratamiento de riesgos. Su aplicación en la gestión de incidentes permite fortalecer la resiliencia organizacional y minimizar los impactos de amenazas cibernéticas. En el contexto de la Cuarta Revolución Industrial, su implementación es clave para garantizar la seguridad en entornos cada vez más digitalizados y conectados.

2.5 INSTRUMENTOS UTILIZADOS

2.5.1 HERRAMIENTAS DE LA METODOLOGÍA NIST

Las herramientas que se utiliza para desarrollar la metodología NIST para la propuesta de desarrollar una gestión de incidente para el Hospital María incluye los siguiente

- **Núcleo del framework de ciberseguridad (CSF):** Documento para desarrollar resultados en contra los incidentes y/o problemas dentro de la organización
- **Matriz de riesgos:** Técnica que nos ayudará a descubrir activos y vulnerabilidades para evitar o disminuir los riesgos.

2.5.2 HERRAMIENTAS DE LA NORMATIVA ISO 27001

Estas son las herramientas necesarias para las buenas prácticas de la protección de los datos salvaguardar la información importante

- **Análisis FODA:** Es una técnica utilizada para lograr ver las fortalezas, oportunidad, debilidades y amenazas para mejorar los procesos.
- **Detección de amenazas y/o Incidentes en tiempo real:** Software que nos permita detectar amenaza que perjudique a la empresa.

2.6 CONCEPTUALIZACIÓN

- **Gestión de Incidentes**: Proceso estructurado para identificar, documentar, analizar y mitigar incidentes que afectan la seguridad de la información dentro de una organización
- **Ciberseguridad**: Conjunto de prácticas, tecnologías y medidas diseñadas para proteger sistemas, redes y datos contra ataques cibernéticos
- **ISO 27001**: Norma internacional que establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), garantizando la confidencialidad, integridad y disponibilidad de los datos
- **ISO 27032**: Estándar que proporciona directrices para mejorar la ciberseguridad, abordando amenazas y vulnerabilidades en el ciberespacio
- **NIST Cybersecurity Framework (CSF):** Marco de referencia desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) para gestionar el riesgo cibernético en organizaciones públicas y privadas
- **Ciclo de Vida de la Respuesta a Incidentes (SANS)**: Modelo que describe las fases de respuesta ante incidentes de seguridad: preparación, identificación, contención, erradicación, recuperación y aprendizaje
- **Resiliencia Organizacional**: Capacidad de una entidad para anticipar, resistir y recuperarse de incidentes de ciberseguridad con el menor impacto posible
- **Informática Forense**: Disciplina que se encarga del análisis e investigación de incidentes de seguridad mediante la recolección y preservación de evidencias

digitales

- **Análisis de Riesgos en Ciberseguridad**: Proceso de identificación y evaluación de amenazas y vulnerabilidades que pueden comprometer la seguridad de la información en una organización
- **Amenazas Cibernéticas en el Sector Salud**: Riesgos específicos que afectan la infraestructura digital de hospitales y centros médicos, incluyendo ransomware, phishing y acceso no autorizado a sistemas clínicos
- **Vulnerabilidades en Infraestructuras de Salud**: Debilidades en sistemas de información hospitalarios que pueden ser explotadas por atacantes para comprometer datos sensibles
- **Ransomware**: Tipo de software malicioso que cifra archivos de una organización y exige un pago para su recuperación
- **Phishing**: Estrategia de ingeniería social en la que los atacantes engañan a los usuarios para obtener información confidencial, como credenciales de acceso
- **Protección de Datos Personales**: Normativas y prácticas orientadas a garantizar la privacidad y seguridad de la información personal en entornos digitales
- **Ley de Protección de Datos**: Marco legal que regula el tratamiento y protección de información personal en diversas jurisdicciones, asegurando los derechos de los usuarios
- **Plan de Recuperación ante Incidentes**: Estrategia estructurada para restaurar la operatividad de sistemas afectados por incidentes de seguridad

- **Autenticación Multifactorial**: Método de seguridad que requiere múltiples formas de verificación para conceder acceso a sistemas críticos
- **Análisis de Brechas en Seguridad**: Evaluación de la diferencia entre el estado actual y el estado deseado de la ciberseguridad en una organización
- **Monitoreo en Tiempo Real**: Uso de herramientas y tecnologías para la detección y respuesta inmediata a amenazas de seguridad
- **Capacitación en Ciberseguridad**: Entrenamiento y formación continua de personal para la prevención y mitigación de incidentes de seguridad

2.7 MARCO LEGAL

2.7.1 LEY DE LA PROTECCIÓN DE DATOS

- **Hábeas data:** Se reconoce la garantía de Habeas Data
- **Sistematización de archivos personales y su acceso:** Los datos personales serán protegidos siempre
- **Ley de Transparencia y Acceso a la Información Pública (Decreto Legislativo No. 170-2006):** incluye disposiciones relacionadas con la privacidad y protección de datos

La ley de la protección de datos fue obtenida gracias a EDT – Honduras por: (Tomé, 2019)

CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 ENFOQUE

El enfoque de la investigación es de tipo mixto, pero estará más basada en un enfoque cualitativo. Este enfoque permite obtener un análisis integral de la problemática relacionada con la gestión de incidentes de seguridad informática en el Hospital María. A través del método cuantitativo, se recopilarán datos medibles sobre la frecuencia y el impacto de los incidentes de ciberseguridad, permitiendo establecer patrones y tendencias en la ocurrencia de estos eventos. Paralelamente, el método cualitativo proporcionará una comprensión más profunda sobre las experiencias, percepciones y desafíos que enfrenta el personal hospitalario en la implementación de estrategias de seguridad informática, permitiendo analizar aspectos subjetivos que no pueden ser medidos numéricamente.

Según (John W. Creswell, 2022), el enfoque mixto permite una comprensión más profunda de los fenómenos de estudio al integrar tanto datos numéricos como narrativos. Este tipo de investigación es idóneo para abordar problemáticas complejas que requieren múltiples perspectivas y métodos de recolección de información. La combinación de enfoques proporciona una visión más holística del problema, evitando sesgos y permitiendo que los hallazgos sean más robustos y aplicables a contextos similares.

3.2 ALCANCE DE LA INVESTIGACIÓN

El alcance de la investigación es explicativo y descriptivo. En primer lugar, tiene un carácter descriptivo porque busca identificar y caracterizar las vulnerabilidades en la seguridad informática del Hospital María, analizando cómo afectan la continuidad de los servicios y la confidencialidad de los datos de los pacientes. De esta manera, se podrán establecer lineamientos

claros sobre la situación actual de la seguridad informática en el hospital.

Por otro lado, el alcance también es explicativo, ya que se pretende determinar las causas de estas vulnerabilidades y los factores que influyen en la efectividad de las estrategias actuales de ciberseguridad. A través de este análisis, se podrán identificar soluciones concretas y medidas preventivas que permitan mejorar la seguridad informática del hospital.

Hernández, Fernández y Baptista (2021) establecen que una investigación explicativa busca determinar las causas de un fenómeno, mientras que una investigación descriptiva se centra en caracterizar una situación o evento en particular. En este caso, ambos enfoques se complementan para ofrecer una visión integral sobre la problemática en estudio, permitiendo desarrollar una metodología de gestión de incidentes fundamentada en evidencia empírica y mejores prácticas internacionales.

3.3 DISEÑO DE LA INVESTIGACIÓN

3.3.1 POBLACIÓN

La población a la que va dirigido este estudio está compuesta por el personal que labora en el área de TI y ciberseguridad del Hospital María. Se decidió incluir a toda la población, dado que su número es reducido y es fundamental obtener su perspectiva directa sobre los procesos de gestión de incidentes de seguridad informática. Esta población proporciona información clave y representativa para el desarrollo e implementación de la metodología propuesta.

De acuerdo con Sampieri et al. (2014), la población de un estudio debe estar claramente delimitada y representar el universo de sujetos que tienen relación con el fenómeno en

investigación. La correcta delimitación de la población garantiza que los resultados obtenidos sean aplicables y útiles para la toma de decisiones dentro del hospital.

3.3.2 MUESTRA

La muestra estará conformada por una selección representativa del personal mencionado, utilizando criterios de selección específicos para garantizar que la información obtenida sea relevante para los objetivos de la investigación. Para ello, se seleccionaron individuos que tengan un conocimiento profundo sobre la seguridad informática del hospital y que hayan estado involucrados en la gestión de incidentes previos, para ellos se selecciona el 100% de la población para poder recolectar de una mejor manera la información deseada.

Según Patton (2015), el tamaño de la muestra en investigaciones cualitativas y mixtas debe basarse en el criterio de saturación de datos, lo que permite recolectar la información necesaria sin redundancias innecesarias. En este sentido, la muestra se ajustará a medida que se alcance un punto donde la información recolectada no aporte nuevas perspectivas significativas, asegurando así la eficiencia del estudio.

3.3.3 TÉCNICAS DE MUESTREO

Se empleará un muestreo no probabilístico por conveniencia, seleccionando a los participantes según su acceso y disponibilidad, dado que el estudio requiere información específica de expertos en seguridad informática dentro del hospital. Esta técnica permitirá obtener información de primera mano de aquellos profesionales que tienen un contacto directo con los sistemas de seguridad y la gestión de incidentes dentro de la institución.

De acuerdo con Etikan, Musa y Alkassim (2016), el muestreo por conveniencia permite obtener datos de una población difícil de acceder, facilitando la investigación en entornos

especializados como el sector salud. Aunque esta técnica no permite la generalización estadística de los resultados, sí permite obtener un conocimiento profundo y detallado del problema de estudio, lo que es esencial para el desarrollo de estrategias efectivas.

3.4 CRITERIOS PARA LA MUESTRA

Criterio	Permitido	No permitido
Identificación	• Especialista en ciberseguridad • Personal administrativo vinculado a TI • Médicos y enfermeros • Técnico de soporte informático • Personal, asistente y otra área vinculada a TI	• Paciente • Secretaria • Personal financiero no vinculado a TI • Encargado de inventario
Experiencia	Mínimo 2 años de experiencia en gestión de seguridad informática.	Menos de 2 año de experiencia en Área de TI
Disponibilidad	Disposición para participar en encuestas y entrevistas.	Personas no interesadas en las encuestas y entrevistas
Accesibilidad	Ubicación dentro del Hospital María.	Fuera del Hospital

3.5 OPERALIZACIÓN DE LAS VARIABLES

VARIABLES	DIMENSIONES	INDICADORES	INSTRUMENTOS
Gestión de incidentes de seguridad	Proceso de identificación de incidentes	Cantidad de incidentes detectados por mes	Reporte mensual de incidentes
	Respuesta ante incidentes	Tiempo promedio de respuesta a incidentes	Registro de tiempos de respuesta
	Comunicación del incidente	Tiempo promedio para informar a las partes involucradas	Encuestas a los responsables del proceso
	Recuperación del sistema	Porcentaje de recuperación dentro de plazos definidos	Documentación de tiempos de recuperación
Estándares de seguridad informática	Recuperación del sistema	Porcentaje de recuperación dentro de plazos definidos	Documentación de tiempos de recuperación
	Aplicación de la ISO 27001	Nivel de cumplimiento con controles establecidos	Auditorías internas
	Implementación de protocolos NIST	Cantidad de protocolos implementados exitosamente	Reportes de implementación
Continuidad de los servicios médicos	Resiliencia tecnológica	Cantidad de interrupciones en los servicios médicos	Registro de interrupciones
	Disponibilidad del sistema	Porcentaje de tiempo en que los sistemas están operativos	Informes de disponibilidad del sistema
Capacitación en seguridad informática	Nivel de formación del personal	Cantidad de empleados capacitados en protocolos NIST e ISO	Registro de asistencia a capacitaciones
	Evaluación de conocimientos adquiridos	Resultados promedio en evaluaciones post-capacitación	Cuestionarios de evaluación

3.6 TÉCNICAS, INSTRUMENTOS, PROCEDIMIENTO Y PLAN DE ANÁLISIS

3.7.1 TÉCNICAS

Para el desarrollo de esta investigación se utilizaron técnicas de recolección de datos tanto cuantitativas como cualitativas. Entre las principales técnicas empleadas se encuentran las encuestas estructuradas, entrevistas semiestructuradas y el análisis documental. La aplicación de

encuestas permitió recolectar datos sobre la frecuencia y el impacto de los incidentes de seguridad en el hospital, proporcionando información estadística clave para el análisis cuantitativo. Las entrevistas semiestructuradas fueron utilizadas para comprender la percepción y experiencias del personal de tecnología de la información y administradores en relación con la seguridad informática. Finalmente, el análisis documental permitió revisar normativas de seguridad aplicables, informes de incidentes previos y regulaciones internacionales como la ISO 27001 y NIST.

En cuanto a las técnicas específicas del **NIST Cybersecurity Framework (CSF),** se empleará el enfoque basado en las cinco funciones clave: **Identificar, Proteger, Detectar, Responder y Recuperar**. Dentro de estas, se hará énfasis en la función **Responder**, utilizando la metodología de gestión de incidentes recomendada por el NIST. Se empleará el modelo de **ciclo de vida de respuesta a incidentes**, que incluye las fases de **detección, análisis, contención, erradicación, recuperación y lecciones aprendidas.**

Según (John W. Creswell, 2022), la combinación de técnicas cuantitativas y cualitativas permite obtener una visión más integral del fenómeno estudiado, proporcionando evidencia más robusta para el análisis e interpretación de los resultados.

3.7.2 INSTRUMENTOS

Para la recolección de datos se utilizaron diversos instrumentos adaptados a cada una de las técnicas empleadas. Las encuestas fueron diseñadas con preguntas cerradas y escalas de Likert para evaluar la percepción sobre la efectividad de las medidas de seguridad informática. Las entrevistas semiestructuradas contaron con una guía de preguntas orientadas a explorar las experiencias y conocimientos del personal involucrado en la gestión de incidentes, lo cual, se emplearon listas de verificación para evaluar el cumplimiento de normativas internacionales y

locales en el ámbito de la ciberseguridad. Además, se aplicaron cuestionarios basados en el NIST para evaluar la madurez de la gestión de incidentes y medir la capacidad de respuesta ante amenazas cibernéticas. **Véase en Anexo1**

En cuanto a la aplicación del **NIST**, se utilizará la herramienta de **matrices de evaluación de riesgos**, basada en los controles del NIST para identificar las vulnerabilidades más críticas del hospital. **Ver en Anexo2**

(Patton, 2014) establece que la selección de instrumentos adecuados para cada técnica de investigación es esencial para garantizar la validez y fiabilidad de los datos obtenidos, permitiendo generar conclusiones fundamentadas y aplicables.

El análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) permite evaluar la situación actual del Hospital María en términos de su capacidad para gestionar incidentes de seguridad informática y mejorar su resiliencia cibernética. Este análisis FODA proporciona una visión estratégica sobre las áreas que deben fortalecerse y las oportunidades que pueden aprovecharse para mejorar la seguridad informática en el hospital. A través de una planificación adecuada, se pueden mitigar las debilidades y amenazas identificadas, asegurando un sistema de gestión de incidentes más robusto y eficaz. Como puede observar en el **Anexo3**

3.7.3 PROCEDIMIENTO

El proceso de recolección de datos se desarrolló en varias fases. En primer lugar, se realizó una revisión documental sobre los marcos normativos y mejores prácticas en seguridad informática aplicables al contexto hospitalario. Posteriormente, se diseñaron y validaron los instrumentos de recolección de datos mediante una prueba piloto con un grupo reducido de participantes.

Luego, se procedió a la aplicación de encuestas y entrevistas a la muestra seleccionada.

Finalmente, se realizó la transcripción y codificación de las entrevistas, así como el análisis de los datos cuantitativos obtenidos en las encuestas mediante herramientas estadísticas.

3.7.4 PLAN DE ANÁLISIS

Para el análisis de datos, se utilizaron métodos estadísticos descriptivos para sintetizar y visualizar la información obtenida en las encuestas. Se calcularon frecuencias, promedios y desviaciones estándar para identificar patrones en la ocurrencia de incidentes de seguridad informática. En el caso de los datos cualitativos, se utilizó un análisis temático para identificar las principales preocupaciones y desafíos mencionados por los entrevistados.

El análisis se complementará con el método de evaluación de riesgos del NIST, utilizando la clasificación de incidentes y las métricas de respuesta recomendadas por el framework. Se analizará la eficacia de las respuestas ante incidentes previos y se evaluará el impacto de la implementación de controles basados en el NIST.

Hernández, Fernández y Baptista (2021) explican que el análisis de datos debe realizarse de manera rigurosa para asegurar la objetividad e imparcialidad en la interpretación de los resultados, permitiendo obtener conclusiones válidas y fundamentadas.

3.8 FUENTES DE INFORMACIÓN

3.8.1 FUENTES PRIMARIAS

Las fuentes primarias corresponden a la información obtenida directamente de los sujetos de estudio a través de encuestas y entrevistas realizadas a los expertos en tecnología y seguridad informática del Hospital María. También se consideran fuentes primarias los registros y reportes internos del hospital sobre incidentes de seguridad ocurridos en los últimos años.

Según John W. Creswell (2022), las fuentes primarias aportan información original y de

primera mano, lo que permite obtener datos confiables y relevantes para la investigación.

3.8.1 FUENTES SECUNDARIA

Las fuentes secundarias incluyen literatura académica, normativas internacionales como la ISO 27001 y NIST, artículos científicos, informes gubernamentales y documentos institucionales sobre ciberseguridad en el sector salud. Además, se consultaron libros especializados y bases de datos académicas para fundamentar teóricamente la investigación.

3.9 MATRIZ DE CONGRUENCIA METODOLÓGICA

Lo que nos menciona (Parrales, 2023), una Matriz de Congruencia en una investigación es un resumen en forma de matriz o cuadro que te ayuda a ver patrones y similitudes en los datos, lo que conocemos como congruencia. Lo que puede ser muy útil para analizar patrones dentro de la investigación y definir el rumbo de esta.

Es en esencia un cuadro que incluye una serie de elementos que permiten al lector comprender de qué trata la investigación y la relación de sus elementos como objetivos y variables. De hecho, estudiar la congruencia de las variables es una de las razones principales de la Matriz de Congruencia

#	Pregunta de investigación	Objetivo	Hipótesis	Metodología	Variables	Dimensiones	Indicadores	Instrumento
1	¿Cuáles son las principales vulnerabilidades y amenazas de seguridad informática a las que está expuesto el Hospital María?	Identificar y analizar las principales vulnerabilidades y amenazas de seguridad informática que afectan al Hospital María.	La falta de capacitación en ciberseguridad del personal del hospital aumenta la vulnerabilidad ante ataques informáticos, ya que los errores humanos representan un factor clave en la ocurrencia de incidentes de seguridad	Mixta	**Independiente:** Protocolos de seguridad, nivel de capacitación.	Proceso de identificación de incidentes	Porcentaje de personal capacitado.	Encuestas al personal
					Dependiente: Número de incidentes, impacto en servicios médicos.		Frecuencia de incidentes reportados.	análisis de registros de incidentes.
							Tiempo de respuesta ante incidentes.	
2	¿Qué marcos normativos y mejores prácticas existen para la gestión de incidentes de seguridad informática en el sector salud?	Examinar y mejorar los marcos normativos y mejores prácticas aplicables a la gestión de incidentes de seguridad informática en el sector salud.	La implementación de una metodología basada en ISO 27001 y NIST mejorará la capacidad de respuesta ante incidentes de seguridad informática en el Hospital María, reduciendo el tiempo de mitigación y fortaleciendo la infraestructura	Cualitativo	**Independientes:** Existencia de normas y prácticas adoptadas.	Aplicación de la ISO 27001	Porcentaje de cumplimiento de estándares internacionales.	Revisión de estándares internacionales como ISO 27001/NIST
					Dependientes: Eficiencia en respuesta a incidentes y reducción de riesgos.	Recuperación del sistema	Impacto de incidentes en la continuidad de servicios.	entrevistas a personal del sector.

			digital del hospital.					
3	¿Qué recursos y capacidades actuales posee el Hospital María para la gestión de incidentes de seguridad informática?	Inspeccionar los recursos y capacidades actuales del Hospital María para la gestión de incidentes de seguridad informática.	El hospital no tiene recursos suficientes para una gestión adecuada	Cualitativo	**Independientes :** Recursos existentes, capacidades del personal.	Nivel de formación del personal	Frecuencia de incidentes gestionados.	Encuestas
					Dependientes: Eficiencia en la gestión de incidentes.	Comunicación del incidente	Tiempos promedio de respuesta.	
							Nivel de satisfacción del personal con los recursos disponibles.	entrevistas al personal de TI.
4	¿Cómo se puede diseñar e implementar una metodología de gestión de incidentes que	Diseño de una metodología de gestión de incidentes de seguridad informática adaptada al	La implementación de un plan estructurado de capacitación en ciberseguridad para el personal del hospital	Mixto	Capacitación del personal	Resiliencia tecnológica	Porcentaje de personal capacitado en ciberseguridad y frecuencia de sesiones de formación realizadas.	Lista de verificación

	se adapte a las necesidades y contexto del Hospital María?	contexto y necesidades del Hospital María.	reducirá significativamente la frecuencia e impacto de los incidentes de seguridad informática.		Política de seguridad	Aplicación de la ISO 27001	Porcentaje de cumplimiento de los protocolos de seguridad y número de auditorías realizadas anualmente.	Entrevistas semiestructuradas:

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

Este capítulo presenta los resultados obtenidos tras la aplicación de los instrumentos de recolección de datos, diseñados para diagnosticar el estado actual de la gestión de incidentes de seguridad informática en el Hospital María. A través de una encuesta dirigida al personal de tecnología y ciberseguridad, se recopilaron datos clave sobre la implementación de políticas de seguridad, el nivel de conocimiento del personal, la existencia de protocolos, la percepción de riesgos y el uso de marcos normativos como ISO/IEC 27001 y NIST.

La finalidad de esta fase es interpretar los datos de forma objetiva y profunda, identificando fortalezas, debilidades y oportunidades de mejora. Se utilizaron herramientas gráficas y de análisis para visualizar tendencias y percepciones significativas en la muestra.

4.1 ANÁLISIS DE VULNERABILIDADES Y AMENAZAS DE SEGURIDAD INFORMÁTICA

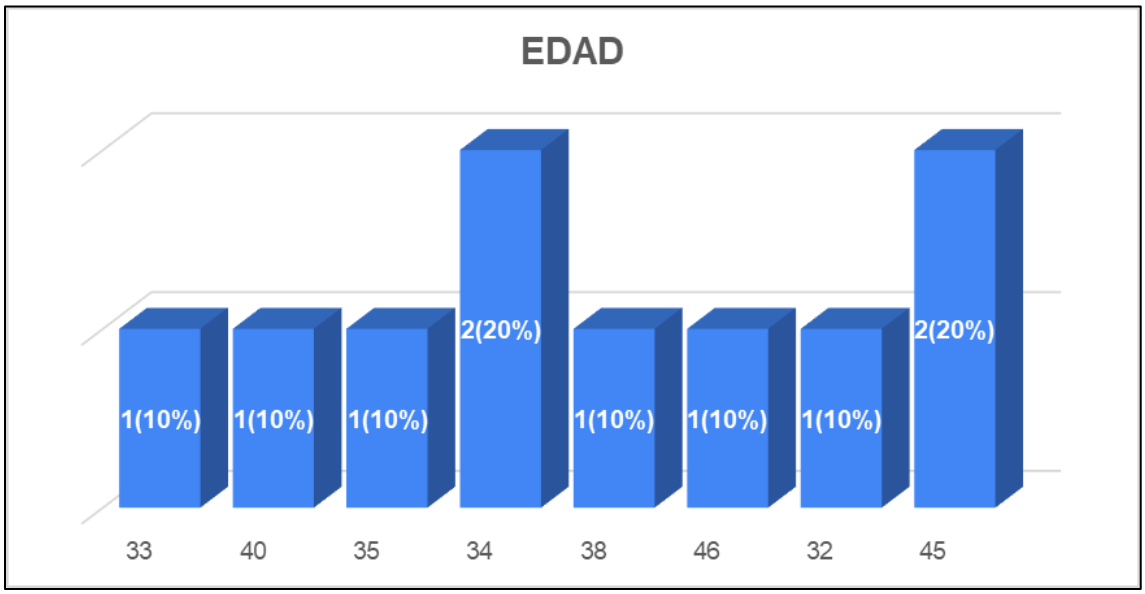
El análisis inicial evidenció debilidades estructurales en la gestión de incidentes de seguridad informática. A través del levantamiento de información y la revisión documental interna, se identificó que el Hospital María carece de políticas formales y procedimientos estandarizados para la respuesta a incidentes. Esta ausencia implica que, ante un evento adverso, las acciones a seguir dependen de la intuición o experiencia individual de los técnicos, lo que resulta en una respuesta descoordinada, lenta y, en muchos casos, no documentada.

Esta situación representa un riesgo elevado para la continuidad operativa del hospital. En el contexto de los servicios de salud, donde se manejan datos altamente sensibles (expedientes clínicos, historiales médicos, información personal), una falla en la respuesta a un incidente puede comprometer la privacidad de los pacientes y afectar la confianza institucional.

Un ataque tipo ransomware dirigido a los servidores que almacenan historiales médicos, sin un procedimiento formal de respuesta, podría paralizar los servicios clínicos por horas o días. La falta de lineamientos impediría una respuesta rápida, la contención del daño, y la correcta recolección de evidencia para análisis forense o reporte a autoridades.

Distribución de los participantes:

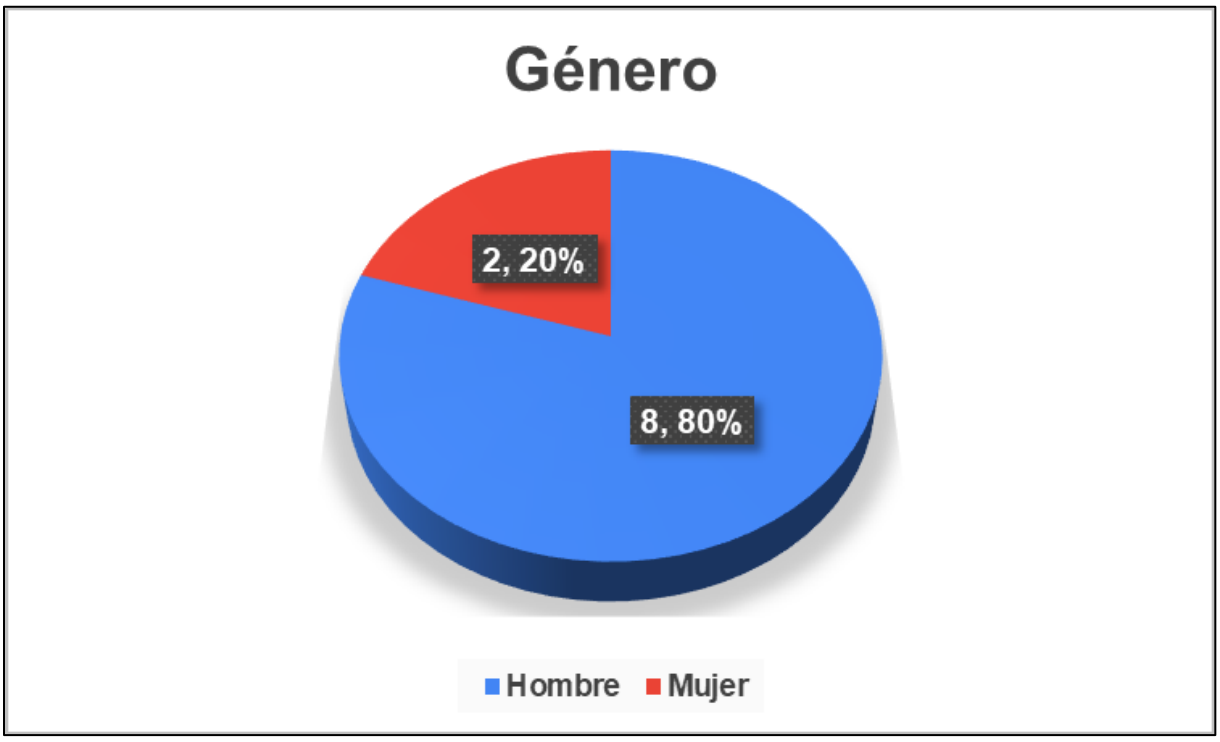
Gráfica 1: Edad



Análisis: En el gráfico se puede observar que tienen 32 años en adelante, esto nos permite analizar con qué tipo de personas estamos tratando ya puede ser jóvenes o adultos, según los resultados obtenidos, todos son adultos, eso significa tener una facilidad para dialogar de manera más madura con todo el personal. También se puede influir en varios factores clave, como: los jóvenes suelen adaptarse rápidamente a nuevas tecnologías, pero pueden subestimar los riesgos, mientras que los mayores son más cautelosos, pero pueden requerir más capacitación. La distribución generacional impacta la percepción de seguridad, la cultura organizacional y las

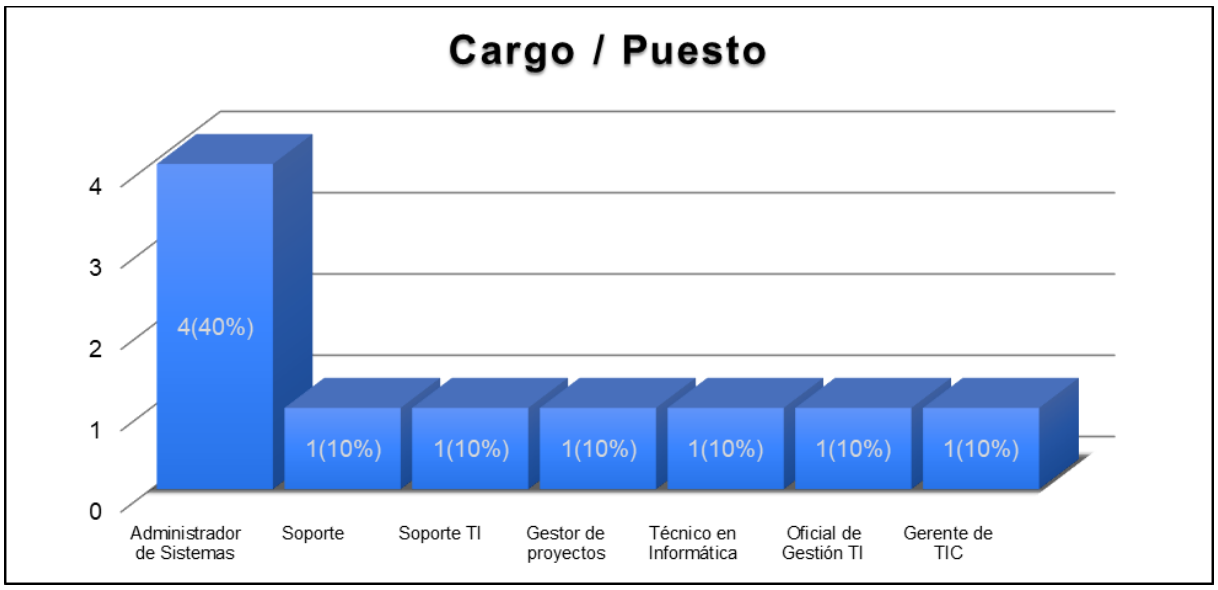
estrategias de formación. Dependiendo de la predominancia de edades en el estudio, pueden ajustarse las estrategias para mejorar la conciencia y protección en el área de seguridad informática.

Gráfica 2: Género



Análisis: El género juega un papel muy importante a la hora de percibir riesgos en el área de la seguridad, como la toma de decisiones, esto se debe a que impacta bastante en las políticas de seguridad y cultura organizacional que se tiene dentro de la empresa. Si hay una distribución donde un género predomina al otro, puede decir que se debe hacer una mejorar en las áreas de la seguridad para que se muestren más opiniones y decisiones con mayor efectividad.

Gráfica 3: Cargo / Puesto

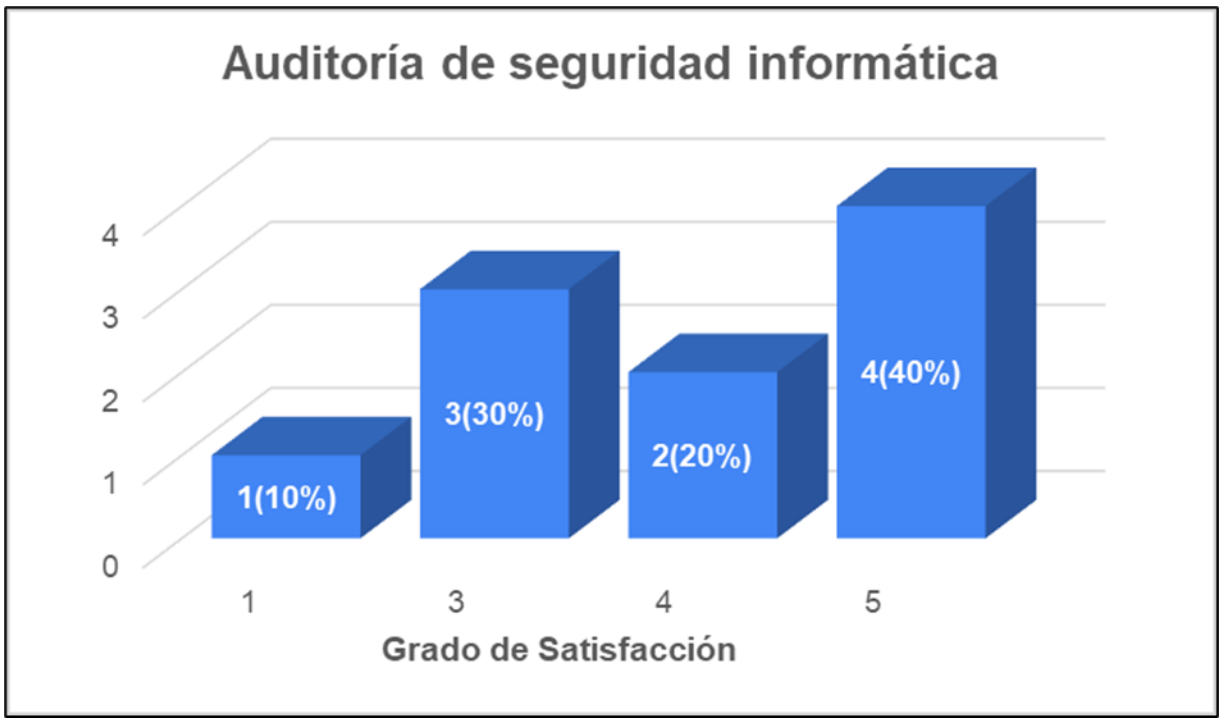


Análisis: El gráfico nos muestra que los administradores de sistemas tienen un impacto directo con la responsabilidad de configurar y dar mantenimiento al sistema, donde los roles como Soporte son los que permite a mantenerse conectado con el usuario y el equipo, el rol de gestor de proyecto influye estratégicamente a definir las políticas adecuadas y asignar los recursos necesario para la misma. Además, cada rol cumple con un importante trabajo dentro de su área donde permite mantener todo con confidencialidad, integridad y disponibilidad de los datos

4.1.1 ANÁLISIS DE SEGURIDAD INFORMÁTICA EN EL HOSPITAL MARÍA

Damos a conocer los resultados que se obtuvieron en cada pregunta, la cual fue de gran ayuda, porque nos permite analizar a detalle todos los puntos clave que se dio a entender. Esta información fue utilizada para el análisis de tendencias, prácticas y oportunidades de mejora en el ámbito de la seguridad informática, contribuyendo a una investigación aplicada en el área de las tecnologías de la información con el objetivo de identificar y analizar las principales vulnerabilidades y amenazas de seguridad informática que afectan al Hospital María.

Gráfica 4: Auditoría de seguridad informática

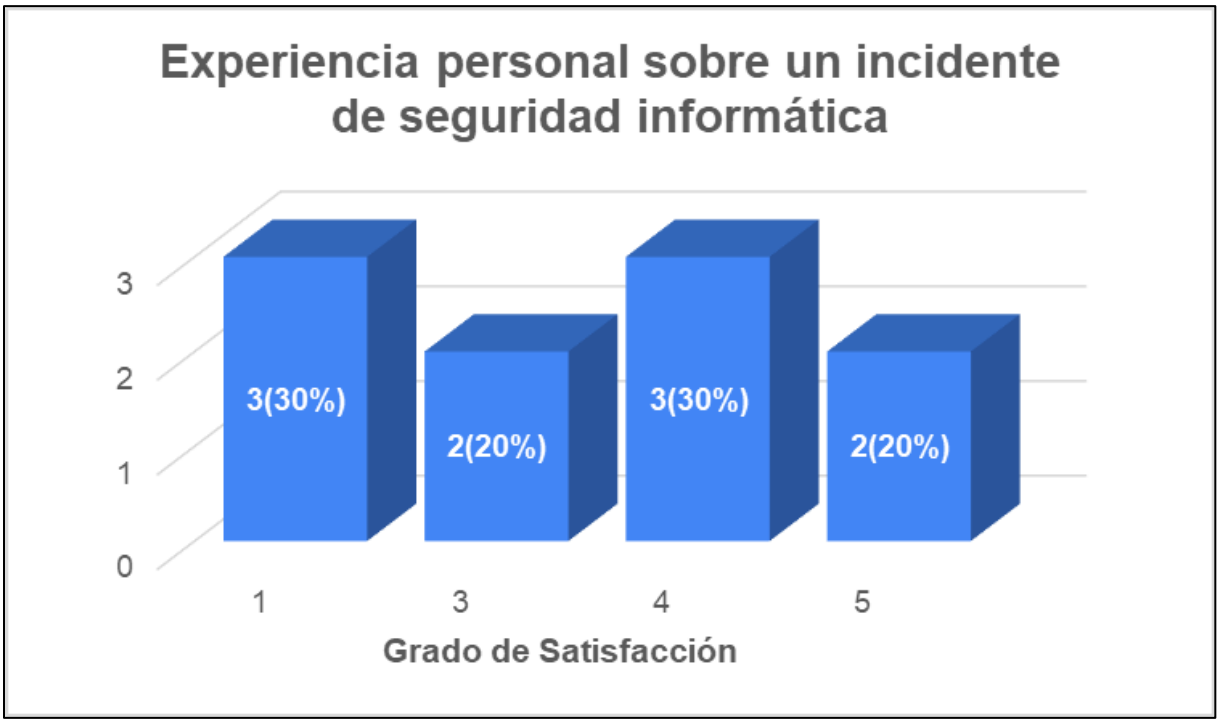


Nota: En el grado de satisfacción 2 (En desacuerdo) no se recibió ningún dato.

Análisis: La práctica de auditorías no es constante ni sistemática, lo que representa una debilidad operativa, el promedio ronda entre 3 (neutro) y 4 (de acuerdo) lo cual suma el 70% de la población. Esto indica que el hospital necesita mejorar la comunicación sobre cuándo y cómo se hacen estas auditorías, o quizás hacerlas de forma más consistente y visible, para que todos confíen

en que la seguridad que se revisa continuamente para corregir los problemas a tiempo.

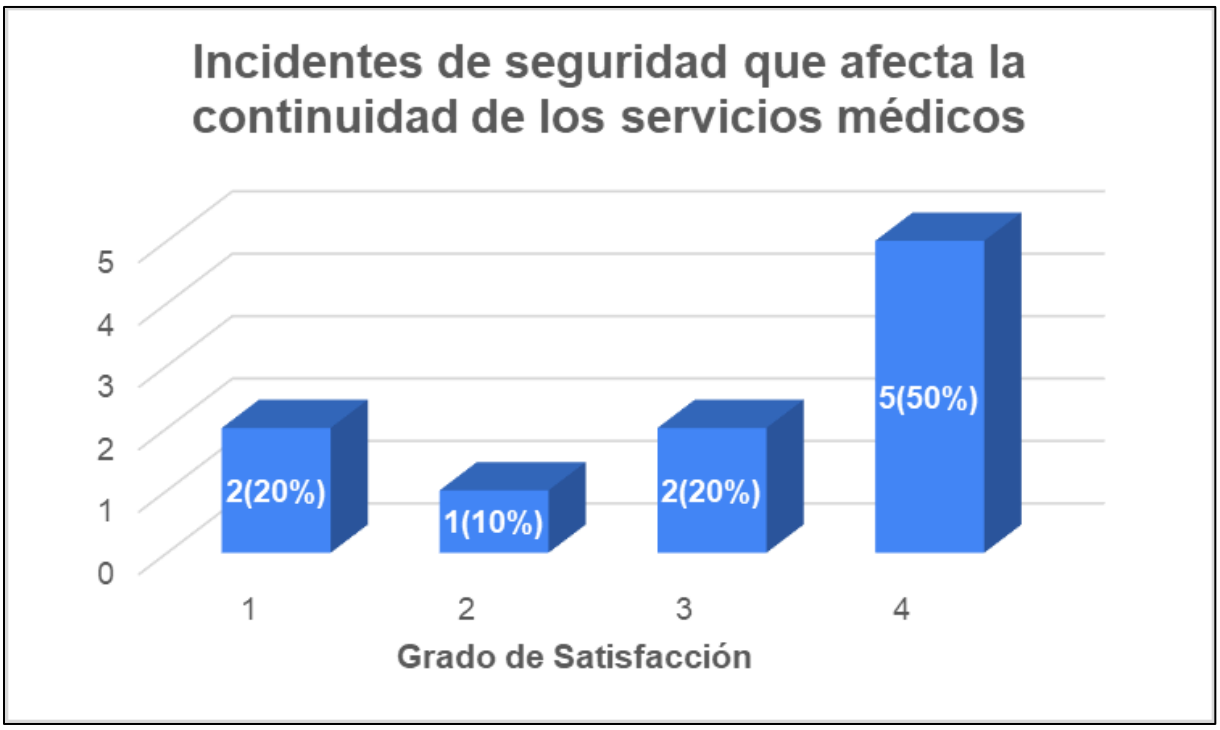
Gráfica 5: Experiencia personal sobre un incidente de SI



Nota: Nadie de los encuestado respondió el grado de satisfacción 2 (en desacuerdo).

Análisis: La mitad del personal del hospital haya experimentado personalmente un incidente de seguridad informática es una señal de alerta importante. Esto sugiere que los incidentes no son eventos aislados y podrían indicar fallos en los controles de seguridad, una alta exposición a amenazas, o una falta de concienciación efectiva. Es fundamental para el hospital investigar la naturaleza y frecuencia de estos incidentes percibidos, mejorar los mecanismos de prevención, detección, y utilizar estas experiencias para fortalecer la formación en ciberseguridad y la cultura de reporte de incidentes en toda la organización.

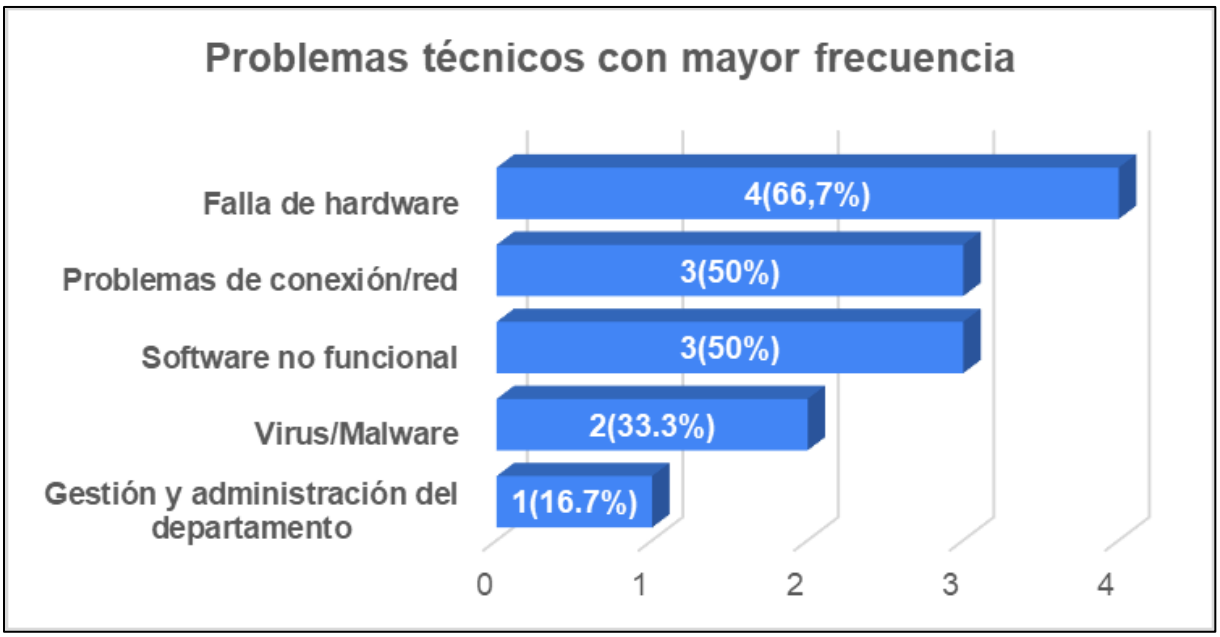
Gráfica 6: Incidentes de seguridad que afecta la continuidad de los servicios médicos



Nota: Ninguno de los encuestados están totalmente de acuerdo

Análisis: La grafica revela que los incidentes de seguridad informática han afectado la continuidad de los servicios médicos por parte de la mitad del personal es un hallazgo crítico y alarmante. Subraya la necesidad urgente de que el hospital priorice la ciberseguridad no solo como un problema de TI, sino como un elemento fundamental para la seguridad del paciente y la operación ininterrumpida de sus servicios vitales. Es imperativo fortalecer las defensas, los planes de respuesta y recuperación, y la concienciación para mitigar este impacto y garantizar la continuidad de la atención médica.

Gráfica 7: Problemas técnicos con mayor frecuencia



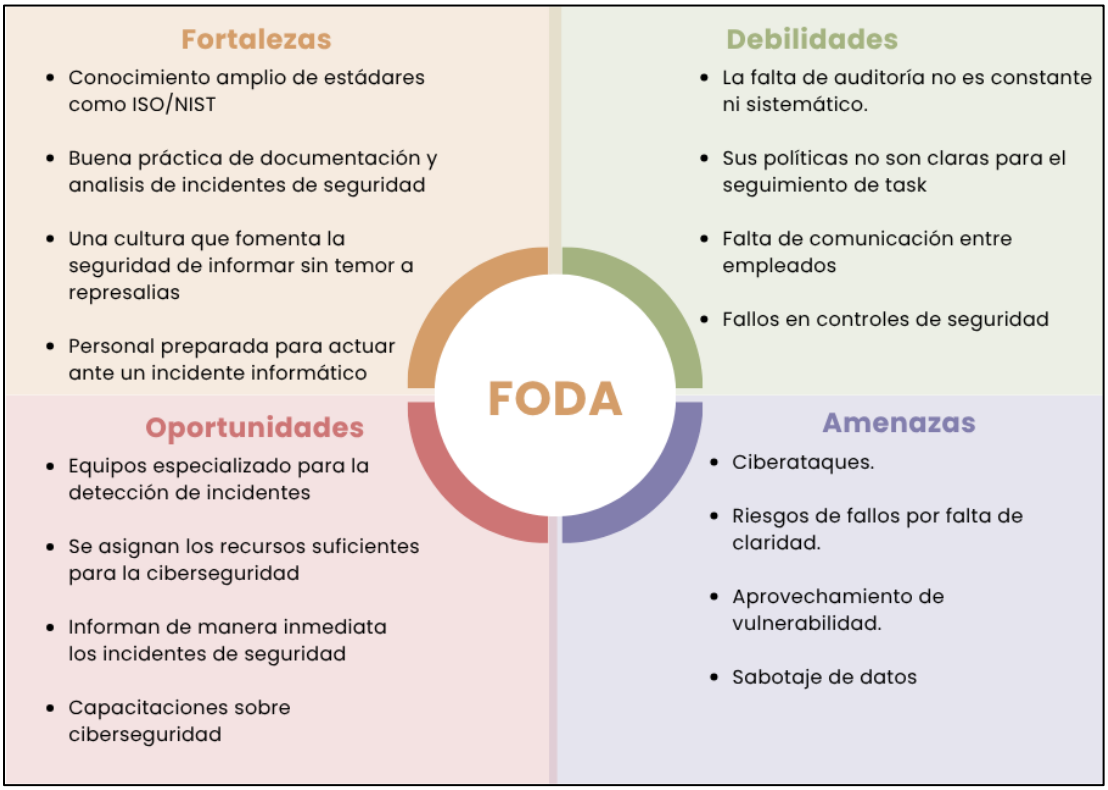
Análisis: Los encuestados reportaron mayoritariamente enfrentar fallas de hardware, problemas de red y soporte a software. Cuatro de seis participantes mencionaron múltiples categorías simultáneamente, lo que evidencia la versatilidad de las funciones asignadas al personal TIC del Hospital María. Este patrón indica que los técnicos están más enfocados en tareas operativas inmediatas y no necesariamente especializadas en seguridad informática.

Esto también demuestra que los incidentes de ciberseguridad podrían quedar ocultos o dar un mal servicio al ser tratados como problemas comunes de red o software. Este hallazgo sugiere la necesidad de un procedimiento diferenciado y una capacitación clara para reconocer e intervenir adecuadamente cuando hay indicios de amenazas de seguridad informática.

4.1.2 ANÁLISIS FODA

A continuación, se evaluó un análisis que señala las fortaleza, oportunidad, debilidades y amenazas que tiene el Hospital María, esto nos ayudó a poder analizar más a fondos sus características para hacer una mejor estrategia para asegurar los datos y mantenerlos más seguro con mejores políticas, gracias a la normativa de ISO/NIST que nos indicó como se debe llevar a cabo estas estrategias de seguridad informática.

Figura 9: Análisis FODA



4.1.3 ANÁLISIS DE MATRIZ DE RIESGO

Se desarrolló una matriz de riesgos que está basado gracias a las entrevista y encuesta, a su vez también se obtuvo datos a través del Análisis FODA que tomó un gran valor para el desarrollo de esta matriz basada con ISO/NIST donde el NIST toma algunas referencias como la ISO 31000 (Gestión de riesgos), sin dejar de lado todas las posibilidades que pueden ocurrir como amenazas que no se pueden controlar a simple vista, como son los errores de usuario o desastres naturales.

Tabla 3: Descripción de Activos y Amenazas

Alcance:	Protección de Datos

PROBABILIDAD DE AMENAZAS	
TIPO	AMENAZA
Criminalidad	Ciberataques
	Sabotaje
Sucesos físicos	Desastres Naturales
	Enegía
	Falla de hardware
Descuidos	Entrada acceso no autorizado
	Mala administración del servidor
	Uso compartido de contraseña

ACTIVOS	
TIPO	AMENAZA
Físicos	Almacenamientos
	Computadoras
	Redes
	Servidor
No Físicos	Base de Datos
	Software
Seguridad Física	Cámaras de seguridad

Nota: Elaborado gracias a la normativa de ISO 31000 (Gestión de Riesgo).

Descripción: Antes de iniciar con la elaboración de la matriz de riesgos se evaluó primeramente el alcance(**propósito**), luego se analizó profundamente las amenazas y los activos que puede provocar riesgos para la empresa.

Tabla 4: Medición de la matriz de riesgo

			Impacto			
			1	2	3	4
			Bajo	**Medio**	**Alto**	**Muy Alto**
Probabilidad	1	**Baja**	1	2	3	4
	2	**Media**	2	4	6	8
	3	**Alta**	3	6	9	12
	4	**Muy Alta**	4	8	12	16

Impacto	1 a 3	Bajo
	4 a 6	Media
	7 a 9	Alta
	12 a 16	Muy Alta

RT(Riesgo total) = P*I
I = Impacto de las amenazas
P= Probabilidad de Amenazas

Nota: Elaboración propia gracias a la guía NIST

Descripción: Esta tabla nos indica como va a estar conformado la medición del riesgo donde el número máximo de riego es "4" que significa muy alta y el bajo es "1" que significa baja, además se evalúa que la cantidad máxima del impacto está entre el rango de 12 a 16. Este tipo de medición ayudará a medir de una manera clara todos los activos y averiguar qué tan crítica está la situación para luego crear estrategias para disminuir el riesgo.

Tabla 5: Matriz de riesgo

		Departamento IT							
Matriz de Análisis de Riesgo		P							
Elemento de Información	I	**Criminalidad**		**Sucesos Físicos**			**Descuido**		
		Ciberataques	Sabotaje	Desastres naturales	Energía	Falla de software	Acceso no autorizado	Mala administración del servidor	Uso compartido de contraseña
		3	1	1	3	3	1	3	2
Activos Físicos									
Almacenamientos	3	9	3	3	9	9	3	9	6
Computadoras	4	12	4	4	12	12	4	12	8
Redes	3	9	3	3	9	9	3	9	6
Servidor	4	12	4	4	12	12	4	12	8
Activos No Físicos									
Base de datos	4	12	4	4	12	12	4	12	8
Software	2	6	2	2	6	6	2	6	4
Seguridad Física									
Cámaras de seguridad	1	3	1	1	3	3	1	3	2

Nota: Elaboración propia

Descripción: Esta matriz de riesgo nos permitió sacar conclusión acerca de cuáles son los riesgos que se debe de tratar con más cuidado y conseguir crear nueva estrategia para evitar o disminuir el riesgo dentro del Hospital María, dando uso a la información de la ISO 27001(Seguridad de la información) y la ISO 31000 (Gestión de riesgo) se pudo determinar planes y estrategia para combatir con la causa.

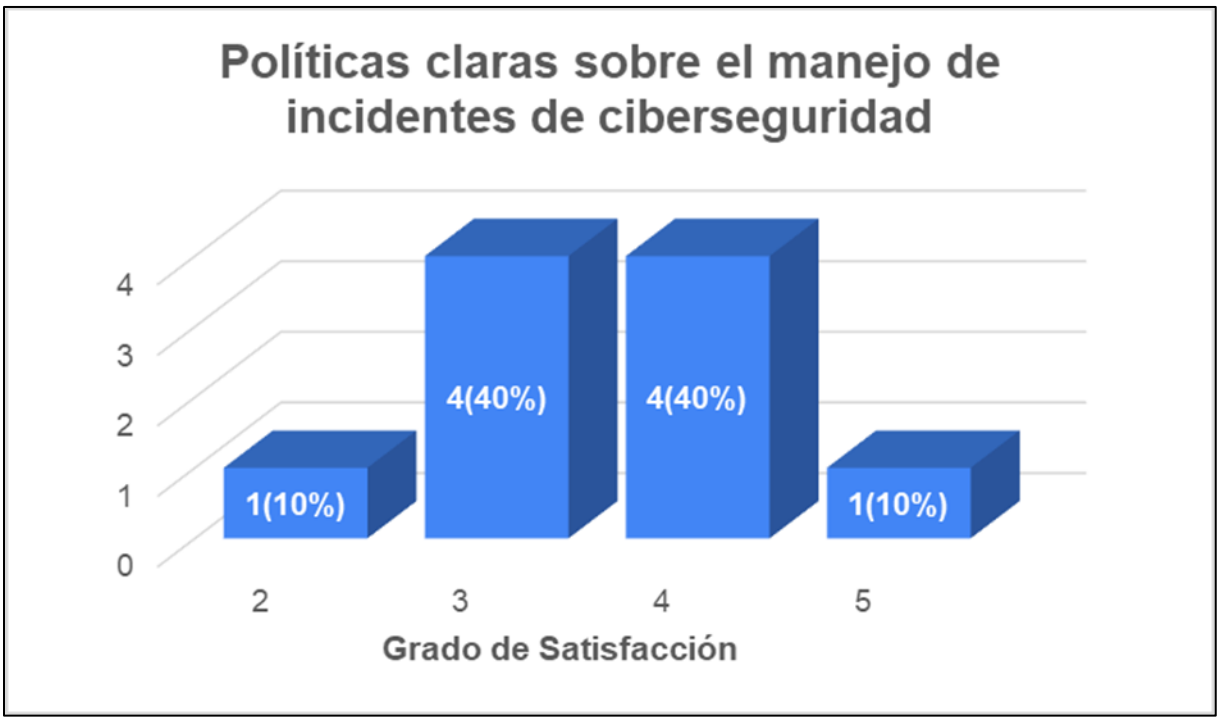
4.2 MEJORA DE NORMATIVAS EN LA GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

De las encuestas realizadas al personal de TI y ciberseguridad, el 83.3% afirmó que el hospital no cuenta con normativas internas claras que regulen la gestión de incidentes. Esto refuerza el hallazgo anterior y revela una desconexión entre la realidad operativa y la necesidad de cumplir con estándares de seguridad.

Esta carencia normativa sugiere que el hospital se encuentra en un nivel de madurez bajo en cuanto a gestión de incidentes, y que las iniciativas de respuesta dependen más de la voluntad que de un sistema institucionalizado. Además, muestra que no existe una cultura de ciberseguridad consolidada.

Relación con la propuesta: La metodología diseñada incluye una fase inicial de preparación, en la que se establecerán políticas internas alineadas con ISO 27001, ISO 27035 y NIST 800-61r2. Esto permitirá institucionalizar los procesos y elevar el nivel de madurez del hospital.

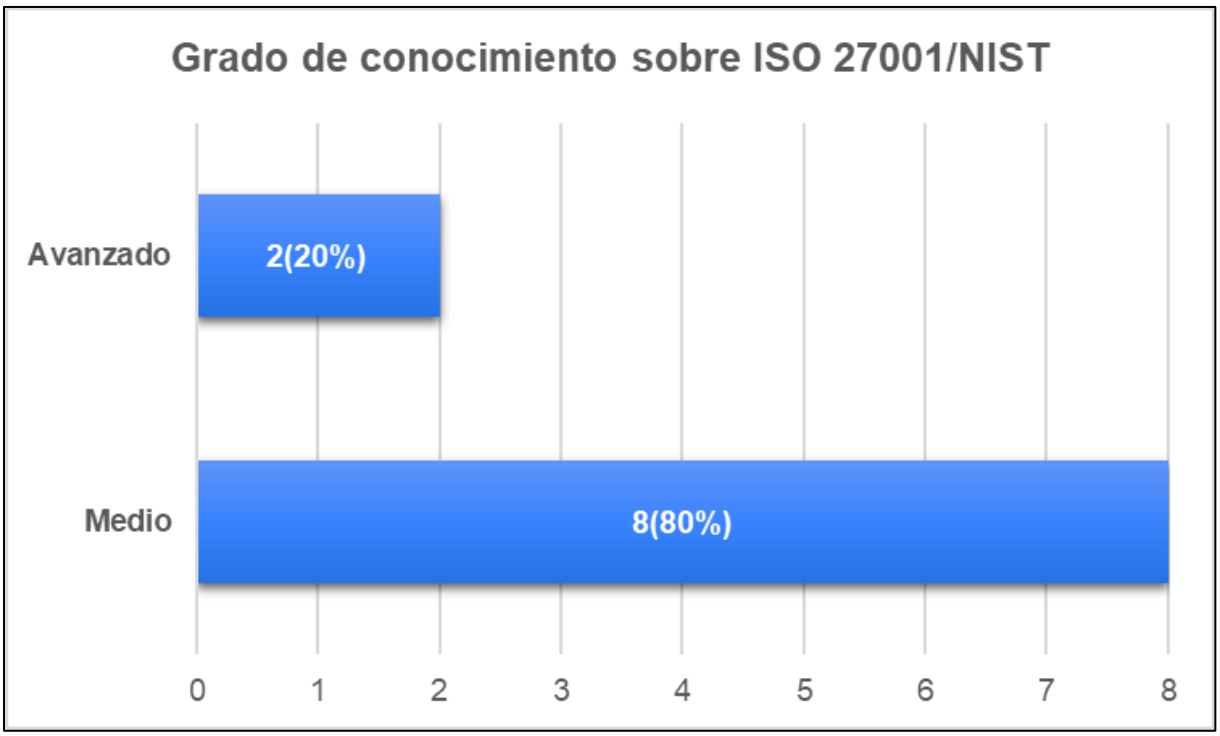
Gráfica 8: Políticas claras sobre el manejo de incidentes de ciberseguridad



Nota: Ninguna respuesta en el grado de satisfacción 1 (Totalmente desacuerdo).

Análisis: La claridad de las políticas de manejo de incidentes de ciberseguridad muestra resultados mixtos entre 3 (neutro) y 4 (de acuerdo) con un 40%, pero hay un 10% que dices que no son claras, eso indica que hay falta de comunicación para explicar con exactitud las políticas. Puede ser que el otro 10% esté totalmente de acuerdo con las políticas, pero se necesita dejar claro esa información para poder mejorar la compresión y la aplicación, haciendo uso de capacitación ante el personal.

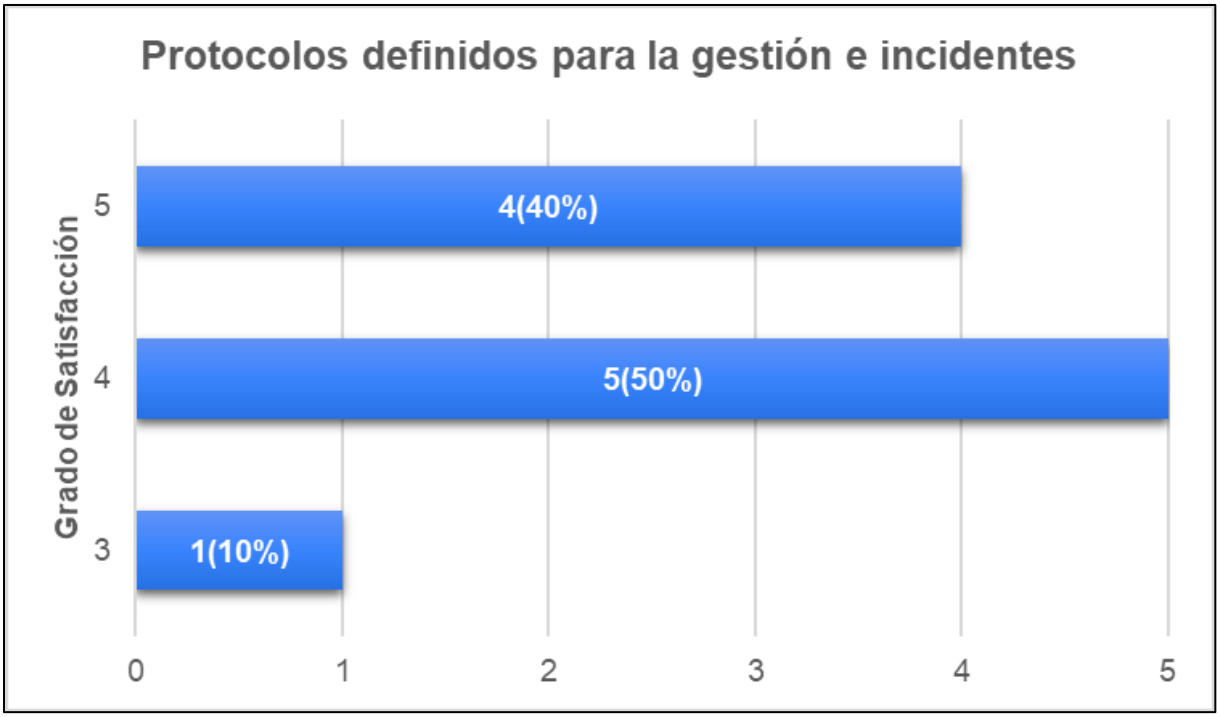
Gráfica 9: Grado de conocimiento sobre ISO 27001/NIST



Nota: Nadie de los participantes respondió Ninguna.

Análisis: La mayoría del personal del área de TI tienen conocimiento "Medio" sobre los estándares de la ISO 27001 y/o NIST, lo cual es algo muy positivo para la empresa. Sin embargo, solo el 20% del personal tienen conocimiento "Avanzado", esto hace que represente una debilidad en cuando su capacidad para implementar, mantener y optimizar eficazmente un programa de seguridad de la información (**SI**) y alineado hacer mejores practicas

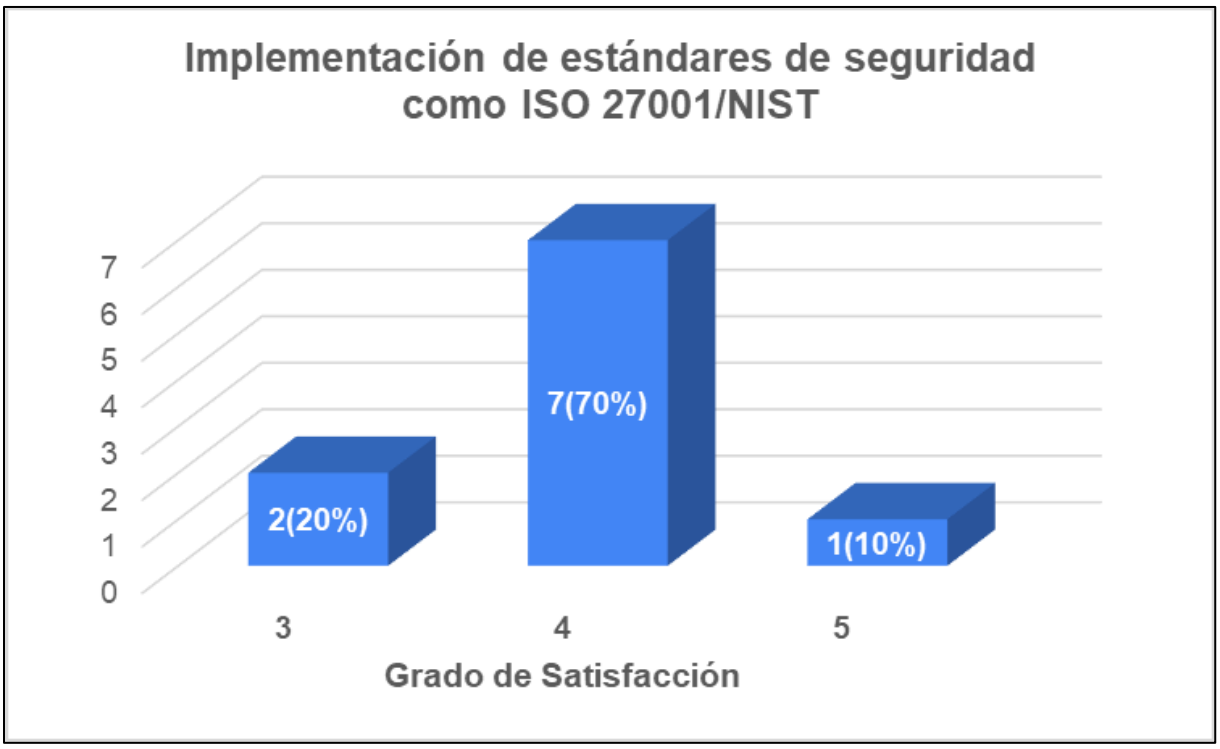
Gráfica 10: Protocolos definidos para la gestión e incidentes



Nota: No hubo ninguna respuesta de satisfacción 1 (Totalmente en desacuerdo) y 2 (En desacuerdo)

Análisis: Se obtuvieron 10 respuestas donde el 50% están de acuerdo, el 40% están totalmente de acuerdo y un 10% están en neutro. Esto significa que existe una percepción positiva, pero se requiere una mayor concentración y formalización de los protocolos existentes para que se tenga una mayor preparación a la hora de que suceda un incidente de seguridad informática, lo cual es muy importante para proteger los datos sensibles de los pacientes y que el Hospital María opere eficazmente.

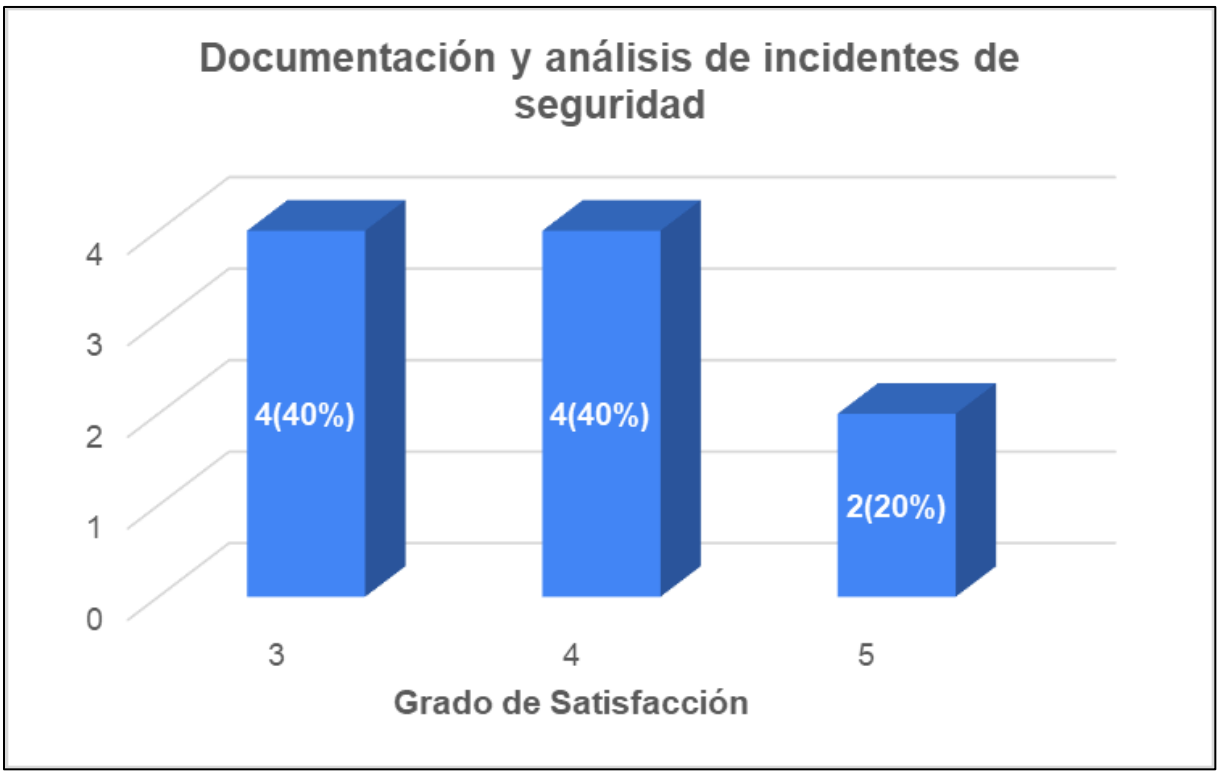
Gráfica 11: Implementación de estándares de seguridad



Nota: No hay ninguna respuesta que esté en 1 (totalmente desacuerdo) o 2 (desacuerdo)

Análisis: La mayoría del personal que es el 70% respondió que, si se implementan estándares de seguridad como la ISO 27001/NIST, esto quieres decir que la empresa está en buen camino, pero aún quedan persona que no les queda claro que se implemente ya que el 20% está en neutral. Esto es un llamado para que el jefe del área se comunique bien con el personal y que hablen con claridad sobre los estándares que se utilizan y motivándole a aprender con una capacitación o charla para comprender lo que significa mantenerse seguro.

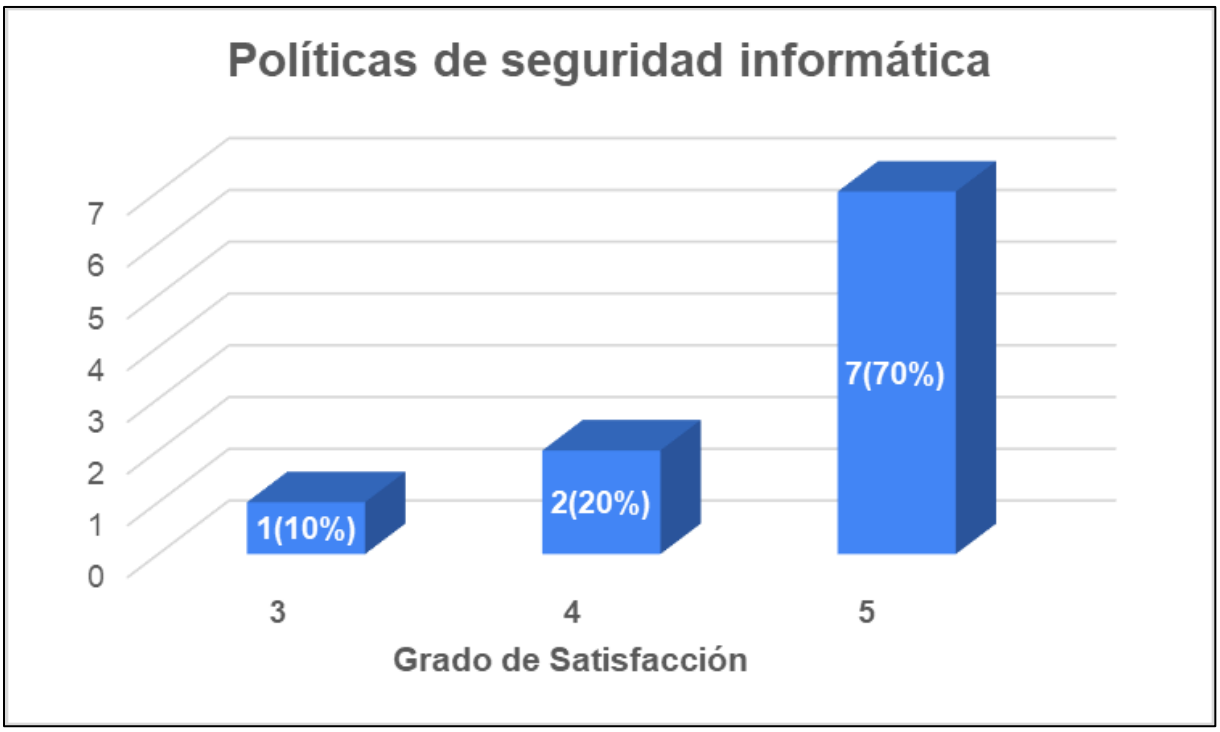
Gráfica 12: Documentación y análisis de incidentes



Nota: No hay respuestas negativas respecto al grado de satisfacción 1 (Totalmente desacuerdo) y 2 (Desacuerdo).

Análisis: Los resultados de esta pregunta revelan una brecha en la percepción y/o la práctica de la documentación y el análisis de incidentes de seguridad. Aunque un 60% cree que se documentan y analizan los incidentes de seguridad el 40% de respuestas son neutrales, esto revela que estos procesos no son consistentes, visibles o efectivos para el personal. Para mejorar la postura de seguridad y aprender de la experiencia, el hospital debe asegurar que la documentación y el análisis de incidentes sean procesos rigurosos, bien comunicados y que generen lecciones aprendidas aplicables para toda la organización.

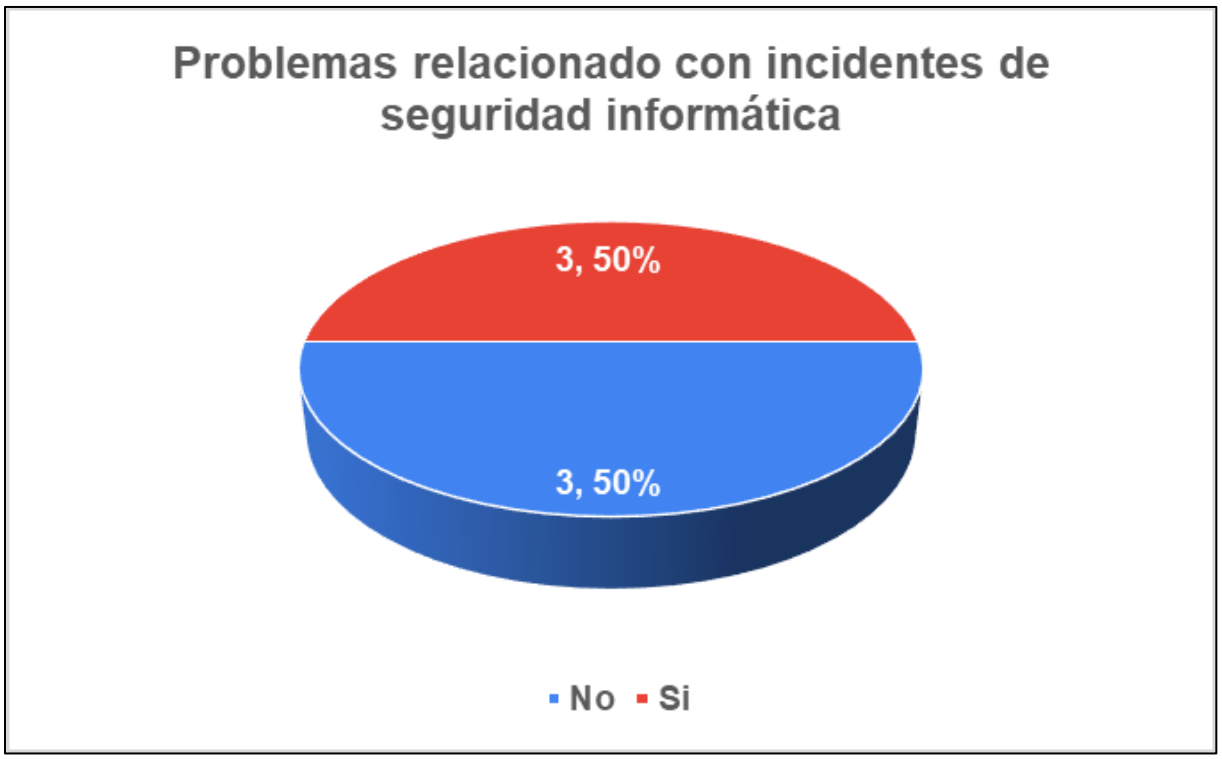
Gráfica 13: Políticas de seguridad informática



Nota: Grado de satisfacción positiva, sin ninguna respuesta negativa, solo una respuesta neutral.

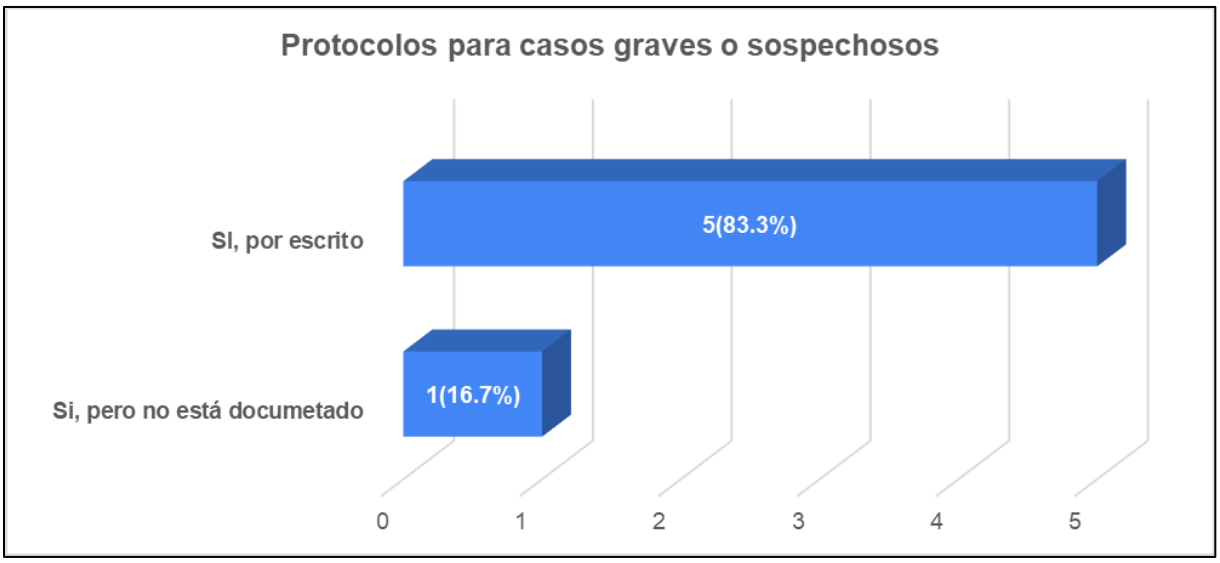
Análisis: La gráfica nos indica que el 90% del personal afirma que siguen las políticas de seguridad informática en sus actividades. Esto quiere decir que el hospital tiene una buena cultura de seguridad donde se demuestra un poco del compromiso hacia la seguridad de los datos. Para poder mantener asegurado el cumplimiento, es importante que el hospital siga reforzando lo valioso que son los datos, además de ser valiosos hacer auditorías para asegurar que se estén cumpliendo las políticas.

Gráfica 14: Problemas relacionado con incidentes de seguridad informática



Análisis: Tres de los seis encuestados respondieron afirmativamente, indicando haber enfrentado incidentes relacionados directamente con la seguridad informática. Esto representa el 50% de los participantes, una cifra significativa considerando el reducido tamaño de la muestra. La experiencia directa con incidentes reales sugiere que, si bien los protocolos pueden no estar claramente definidos, sí se han presentado amenazas tangibles que requieren atención estructurada. Este hallazgo refuerza la urgencia de formalizar un plan de respuesta documentado para incidentes de este tipo.

Gráfica 15: Protocolos para casos graves o sospechosos



Análisis: Se observa en el gráfico que el 100% del personal respondieron que sí existen protocolos para casos graves o sospechosos, pero que existan no significa que estén por buen camino ya que se muestra en el gráfico que el 16.7% respondieron que existen, pero no está documentado. Esto indica que no son claros los protocolos y se necesita de mejorar la comunicación para resolver el problema de la documentación y dejarlo visible para que sea más eficaz al momento de estar frente a un riesgo o incidente de seguridad.

Gráfica 16: Importancia de la seguridad informática

Nota: No hubo ninguna respuesta negativa en esta pregunta

Análisis: Todos los participantes asignaron la máxima calificación (5) a esta afirmación, lo cual refleja una fuerte conciencia sobre la relevancia de la seguridad informática. Esta percepción positiva es una oportunidad clave para implementar iniciativas de mejora, ya que el personal reconoce el valor de proteger la infraestructura y los datos. El alto grado de concienciación también sugiere un terreno fértil para programas de formación, reforzamiento de políticas y empoderamiento del personal en la primera línea de defensa digital.

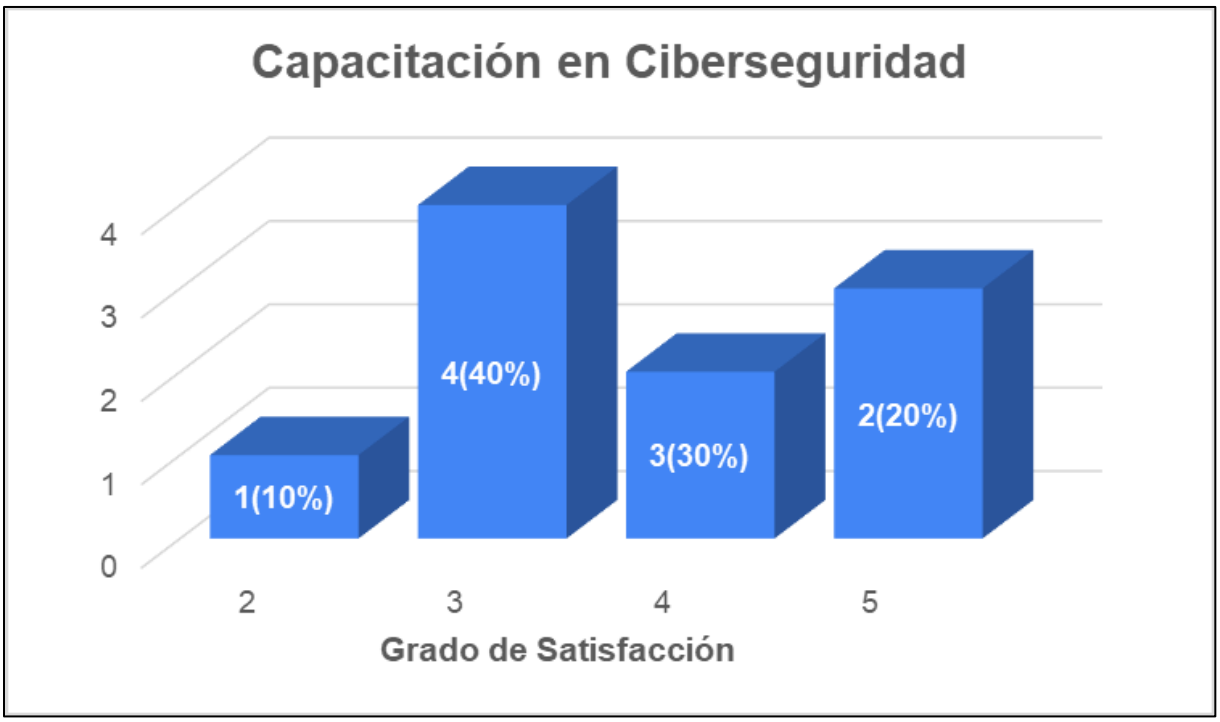
4.3 RECURSOS Y CAPACIDADES DEL HOSPITAL MARÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD

Un 76% del personal considera que el hospital no cuenta con suficientes recursos técnicos ni humanos para hacer frente a incidentes informáticos. Este resultado es preocupante, ya que además de la falta de normativa, existe una limitación en la capacidad de acción.

La combinación de escasos recursos con la ausencia de procesos formales genera un entorno altamente vulnerable. Además, este hallazgo sugiere que cualquier propuesta metodológica debe ser realista y adaptable a las limitaciones existentes, utilizando herramientas y capacidades actuales, o bien proponiendo mejoras progresivas.

Si bien el hospital puede no contar con herramientas automatizadas de monitoreo y respuesta, una metodología adecuada podría establecer protocolos simples con herramientas disponibles (como scripts, formularios manuales, o uso de Excel para registros), mientras se gestiona la adquisición de soluciones más robustas.

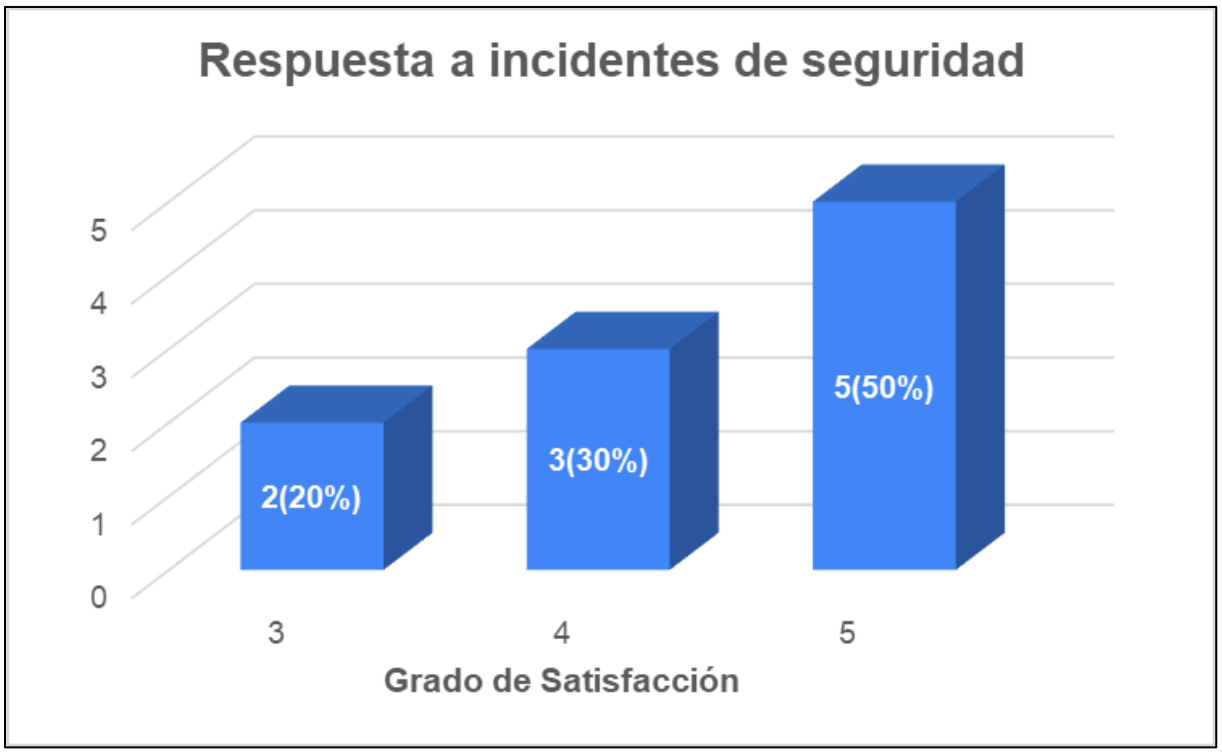
Gráfica 17: Capacitación en Ciberseguridad



Nota: Ninguno de los encuestados respondió con grado de satisfacción 1 (Totalmente en desacuerdo)

Análisis: La mitad del personal cree haber recibido formación en ciberseguridad en estos últimos 12 meses, mientras un significativo 40% se mantiene neutral y un 10% considera que no la ha recibido. Esta distribución mixta es preocupante, ya que la capacitación regular es vital para proteger a la organización, a menudo esto toma un impacto crítico ya que es factor de ciberataques. Es fundamental que fortalezca su programa de concientización, asegurando que la formación sea constante, efectiva y llegue a todo el personal para mitigar vulnerabilidades y reforzar su postura de seguridad.

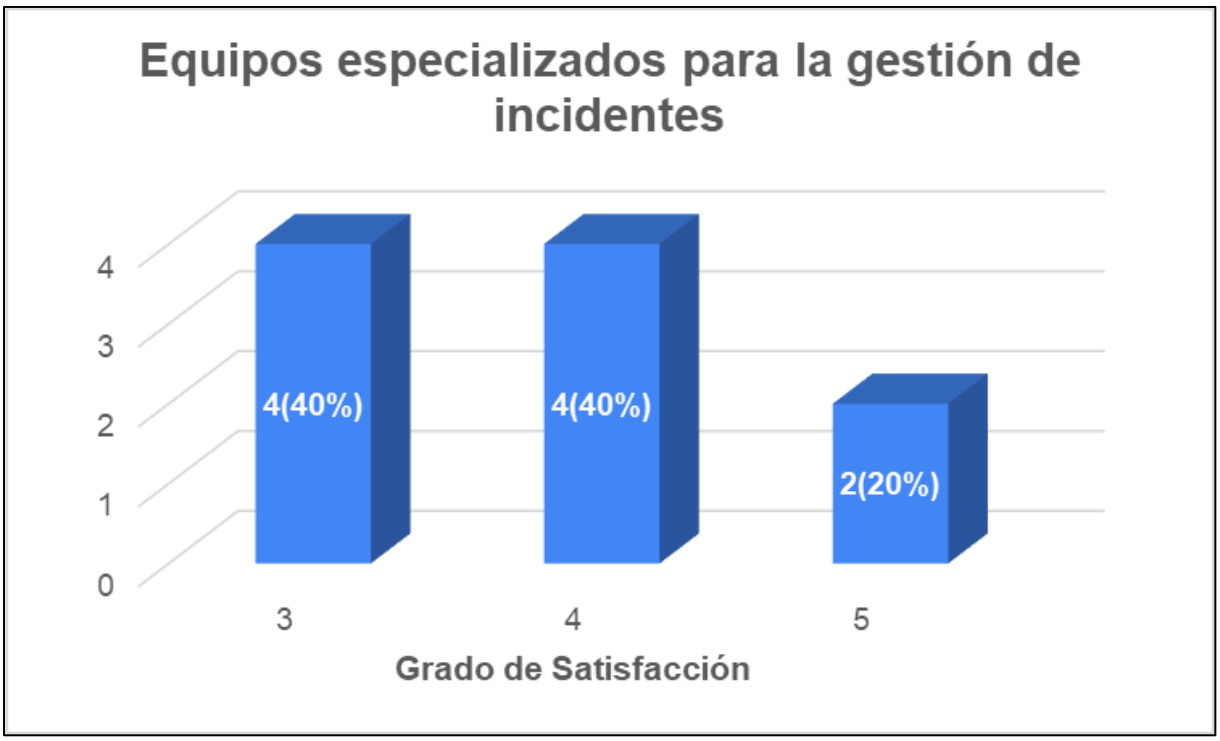
Gráfica 18: Respuesta a incidentes de seguridad



Nota: No se obtuvo respuesta negativa de desacuerdo.

Análisis: El 80% del personal piensan que las respuestas ante incidentes de seguridad informática son muy efectivas, lo cual es una señal de buenas prácticas ya que permite mantener seguros todos sus datos, pero el 20% se mantiene en neutro lo que pueda significar que no tienen idea si está funcionando o no o que no tienen tanto conocimiento acerca de la gestión de incidentes. Así mismo se recomienda que se tener una charla respecto a las respuestas a incidente para mayor efectividad al momento de aplicarlo.

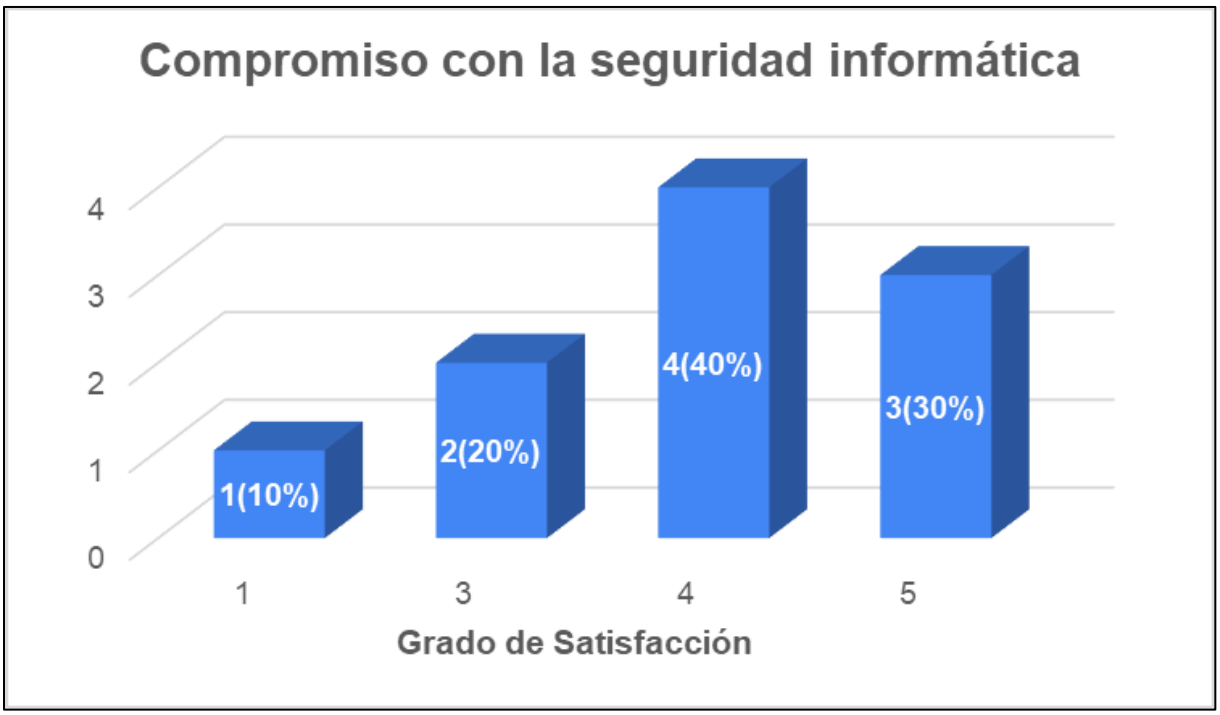
Gráfica 19: Equipos especializados para la gestión de incidentes



Nota: No hay respuestas que esté en desacuerdo

Análisis: Aunque el hospital cuenta con un equipo especializado en gestión de incidentes (percibido por el 60% del personal), la alta proporción de respuestas neutrales (40%) es una señal de que la existencia y el rol de este equipo no son ampliamente conocidos o comprendidos. Se necesita fortalecer la capacidad de respuesta a incidente de seguridad, donde deben centrarse en mejorar la comunicación sobre los equipos especializados para combatir contras amenazas y asegurar que todo el personal sepa sobre estos equipos para que así se puede colaborar de mejor manera.

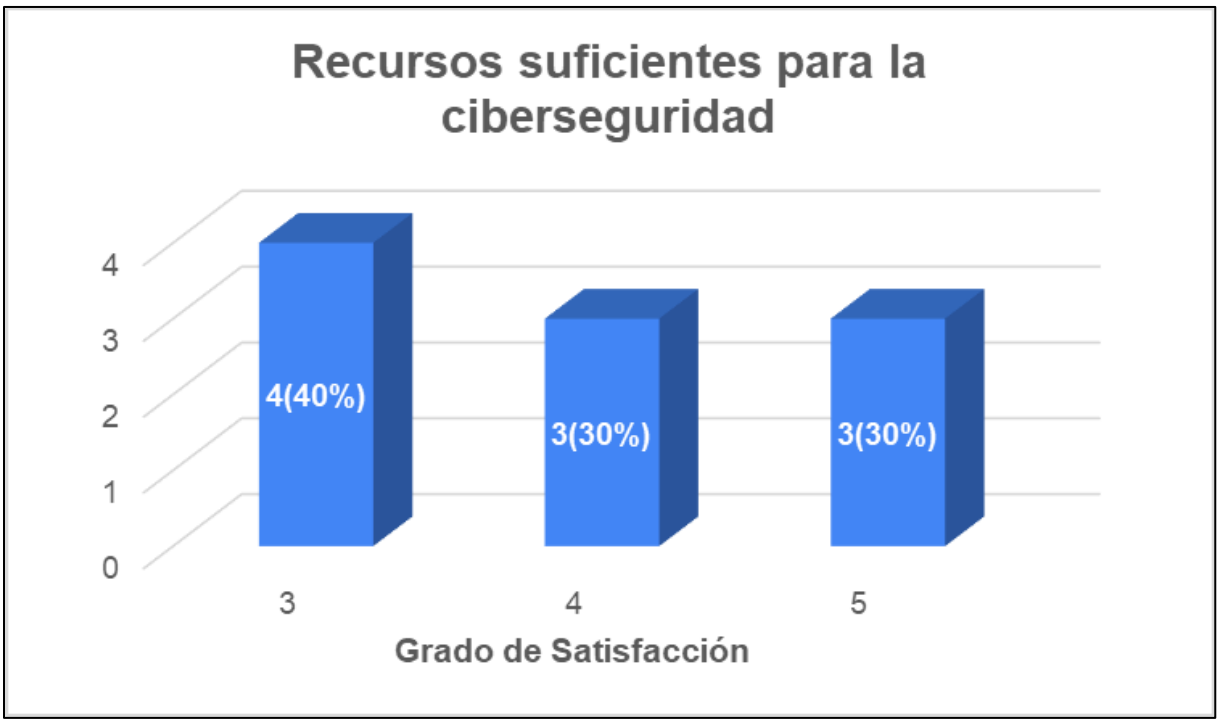
Gráfica 20: Compromiso con la seguridad informática



Nota: No hay ninguna respuesta de grado de satisfacción 2 (desacuerdo)

Análisis: El 70% del personal respondieron que están comprometidos con la administración del hospital, haciendo uso de políticas de ciberseguridad. Sin embargo, ese 10% y 20% no están comprometido. Es importante que la administración comunique y demuestre ese compromiso con acciones y creando políticas claras para poder asegurar que todo el personal se sienta apoyados y que la ciberseguridad es parte fundamental para la empresa.

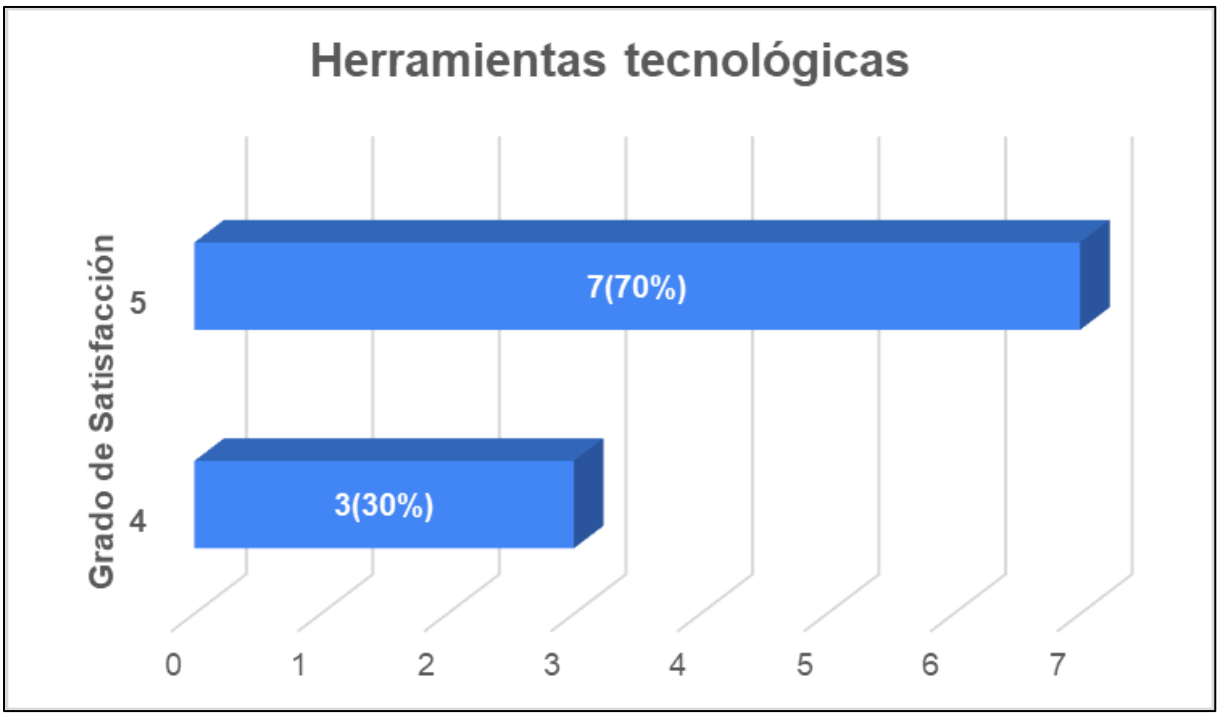
Gráfica 21: Recursos suficientes para la ciberseguridad



Nota: No hay respuestas negativas.

Análisis: Aunque la mayoría del personal (60%) cree que se asignan suficientes recursos para mejorar la ciberseguridad, la alta proporción de respuestas neutrales del 40% es una señal importante para dejar claro políticas de recursos. Esto indica que el conocimiento sobre la suficiencia de estos recursos no es universal. Para fortalecer su postura de seguridad, el hospital debe no solo asegurar una asignación adecuada de recursos, sino también mejorar la transparencia y la comunicación sobre estas inversiones, demostrando cómo contribuyen directamente a una ciberseguridad más robusta y eficaz para toda la organización.

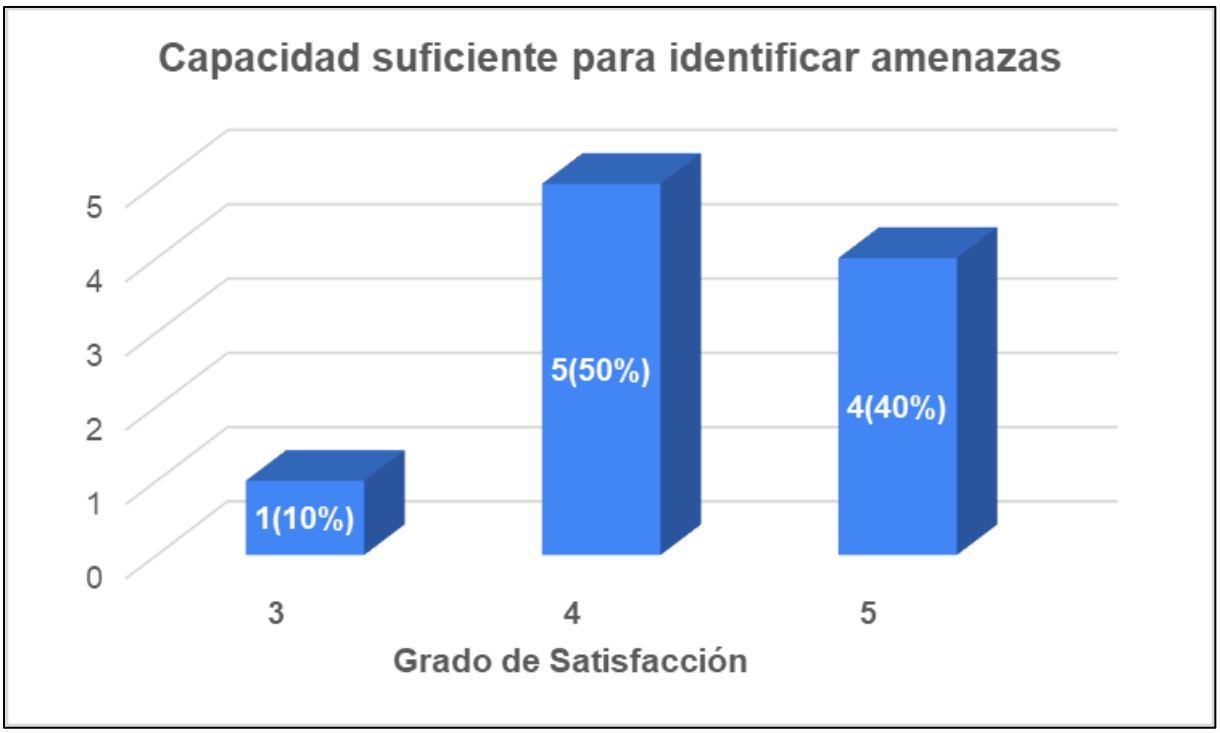
Gráfica 22: Herramientas tecnológicas



Nota: Grado de Satisfacción muy positiva, sin respuestas negativas ni neutrales

Análisis: El 100% del personal percibiendo que las herramientas tecnológicas que utiliza son seguras y confiables. Esta alta confianza es una fortaleza significativa para la postura de ciberseguridad del hospital. Para mantener este nivel de confianza y asegurar la seguridad continua, es crucial que el hospital siga invirtiendo en el mantenimiento, la actualización y la evaluación de sus herramientas tecnológicas, y que comunique estos esfuerzos a su personal.

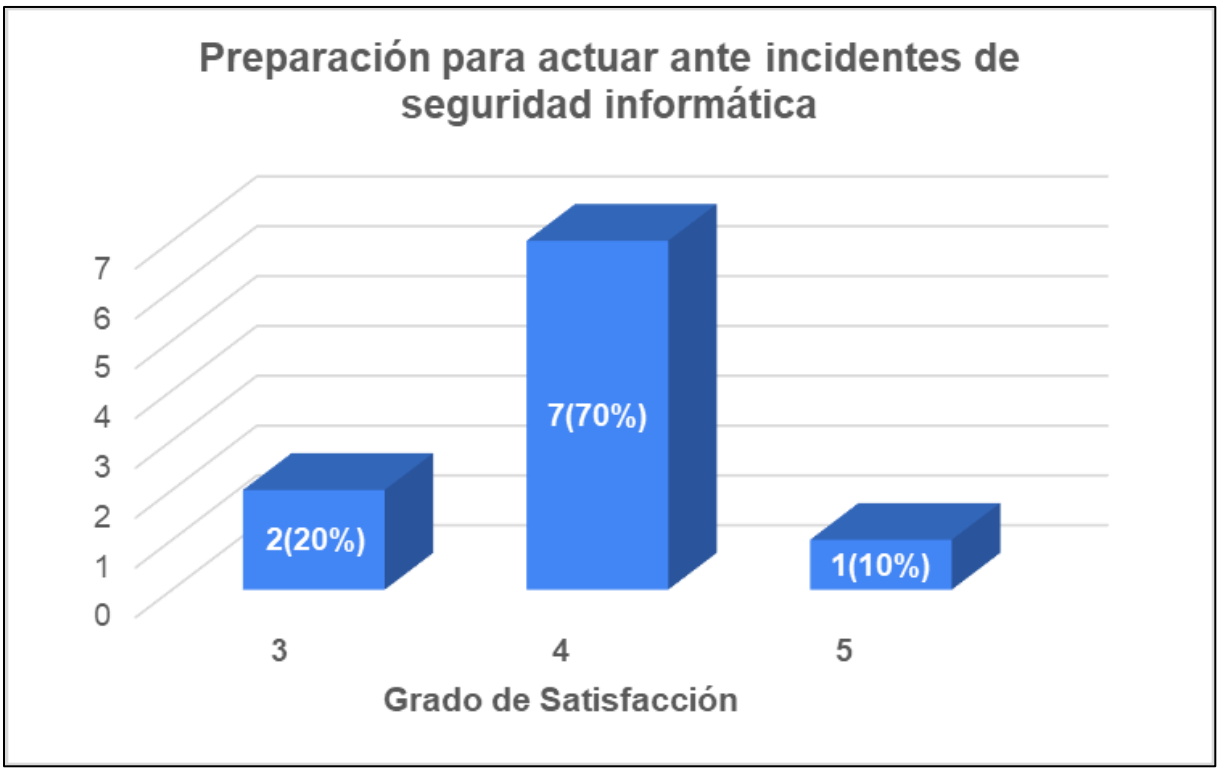
Gráfica 23: Capacidad suficiente para identificar amenazas



Nota: No hay respuestas negativas.

Análisis: Los resultados obtenidos de esta gráfica es decente, con un 90% del personal indicando haber recibido capacitación para detectar amenazas como el phishing. Esto demuestra un compromiso del hospital con la concienciación de su personal, que es vital para defenderse de esta ciberamenaza más comunes, pero aún queda un 10% que no se le ha proporcionado y es vital que el personal sepa sobre amenazas respecto al phishing para reforzar más a seguridad y evitar riesgos y desastres.

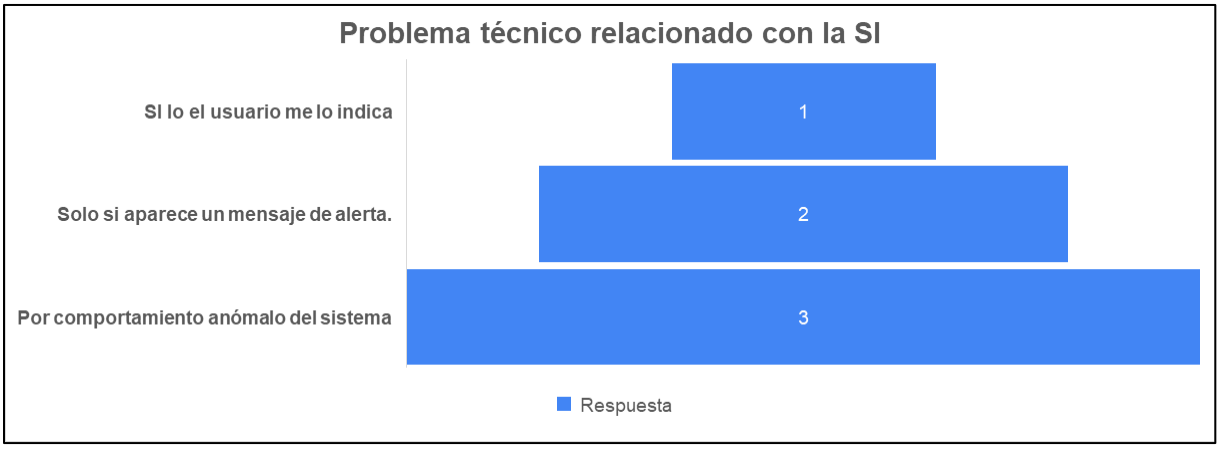
Gráfica 24: Preparación para actuar ante incidentes de seguridad informática



Nota: No hay respuesta que muestre un desacuerdo en esta pregunta.

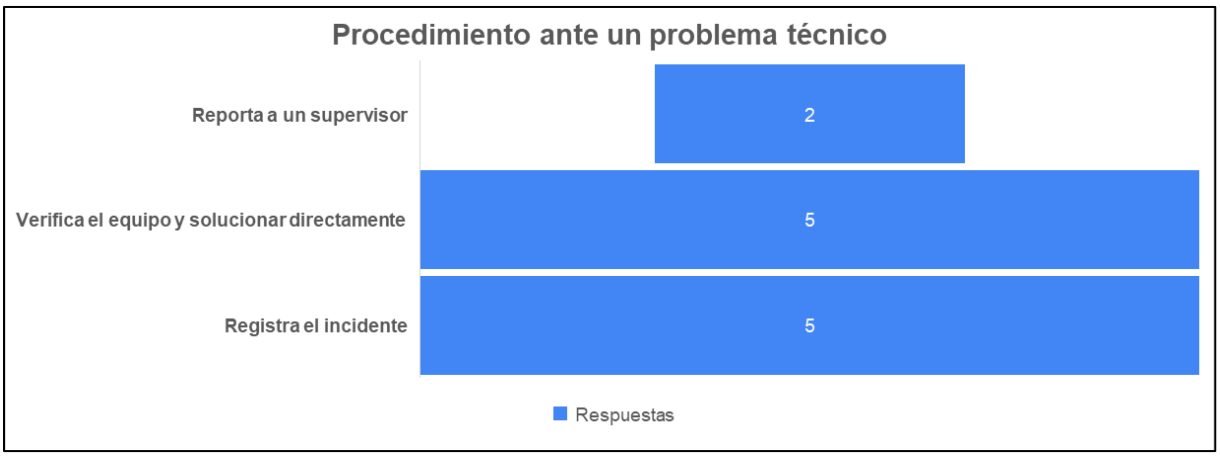
Análisis: Los resultados obtenidos de esta pregunta nos muestra que un 90% del personal se siente muy preparada para actuar ante un incidente. Esto indica que hay un excelente grado d madurez para responder ante un incidente según dicta la política de la empresa. También es unas de las fortalezas significativa para lograr la protección del hospital ante cualquier riesgo, ya que tienen todos los conocimientos para mantenerse seguros y listos, haciendo simulacros clave para operar de mejor forma.

Gráfica 25: Problema técnico relacionado con la seguridad informática



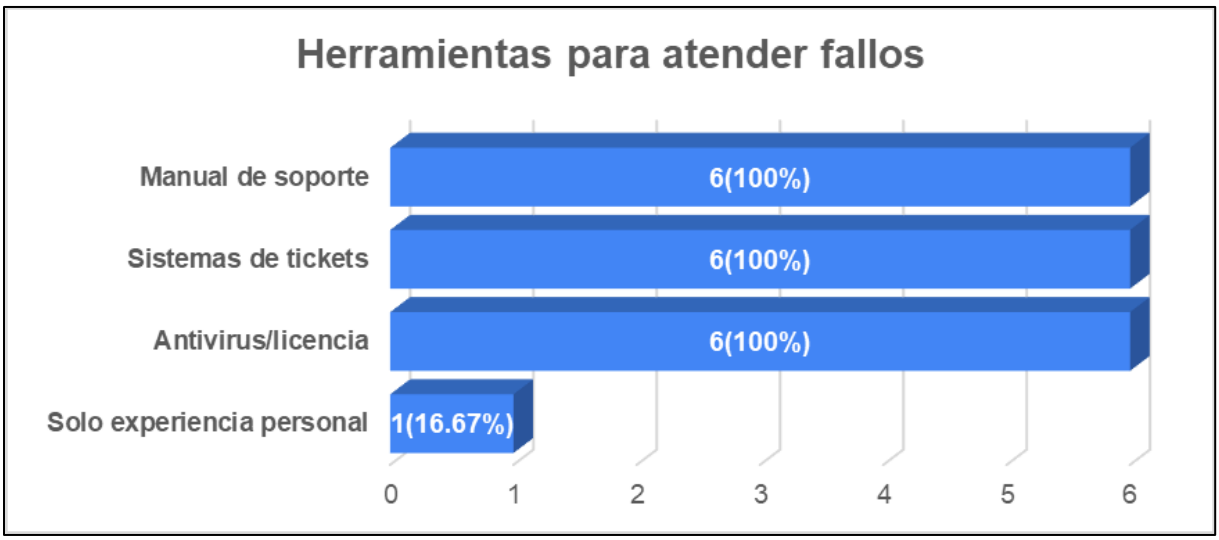
Análisis: El gráfico contiene 6 respuestas obtenidas que revelan tres criterios principales de identificación: comportamiento anómalo del sistema con un 50%, mensajes de alerta con un 33.33 y notificación del usuario con un 16.67%. Aunque el "comportamiento anómalo" fue la opción más común, algunos técnicos dependen únicamente de la notificación del usuario, lo que representa una debilidad crítica. Este comportamiento sugiere que la identificación de incidentes aún depende de métodos subjetivos o reacciones tardías. Por ello, urge implementar indicadores de riesgo basados en monitoreo sistemático y alertas automatizadas, así como entrenar al personal para reconocer patrones sospechosos sin esperar una señal externa.

Gráfica 26: Procedimiento ante un problema técnico



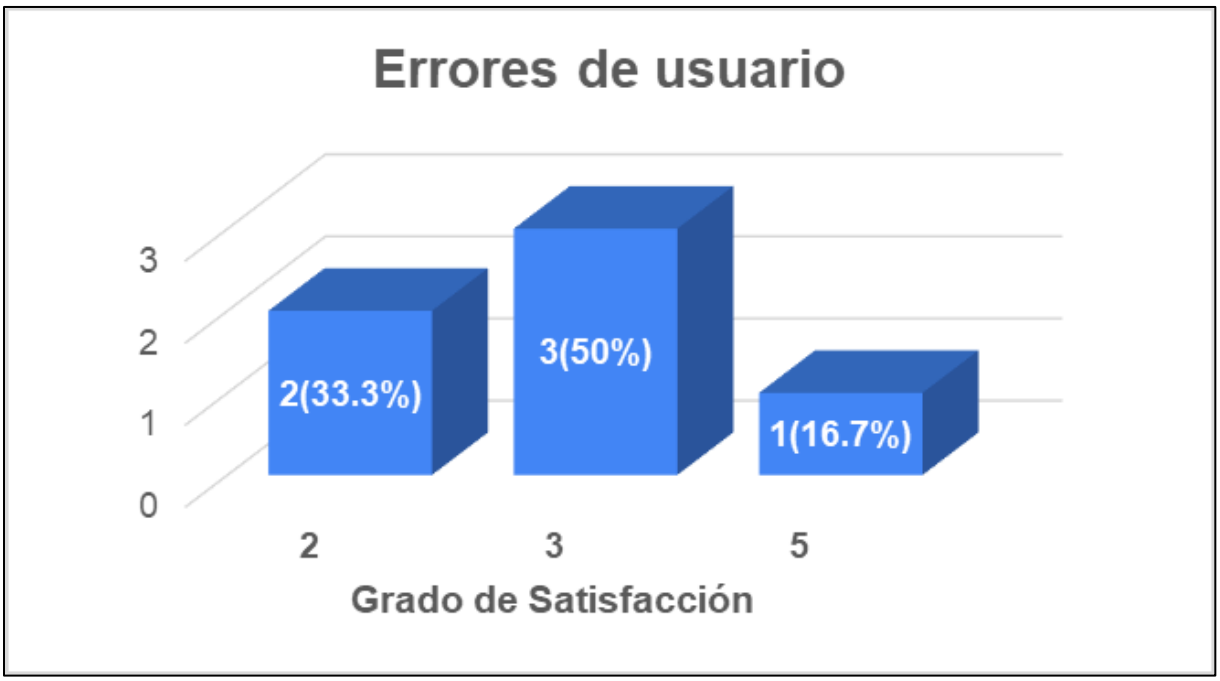
Análisis: Este gráfico contiene 6 respuestas donde la siguiente información nos indica que: Reporta a un supervisor tiene un 33.33%, tanto verificar equipo y registrar el incidente contiene una cantidad del 83.33%. Donde da a entender que los procedimientos más comunes son las verificaciones y los registros de incidentes, lo cual es una buena práctica, pero poco habitual entre el resto del equipo para poder cumplir los objetivos ante un incidente. La falta de uniformidad en los procedimientos sugiere la ausencia de una política estandarizada de gestión de incidentes. Esto puede llevar a acciones inconsistentes, pérdida de evidencia digital o demoras en la contención de amenazas. Por lo tanto, se recomienda desarrollar un protocolo claro de actuación para problemas técnicos con enfoque en seguridad.

Gráfica 27: Herramientas para atender fallos



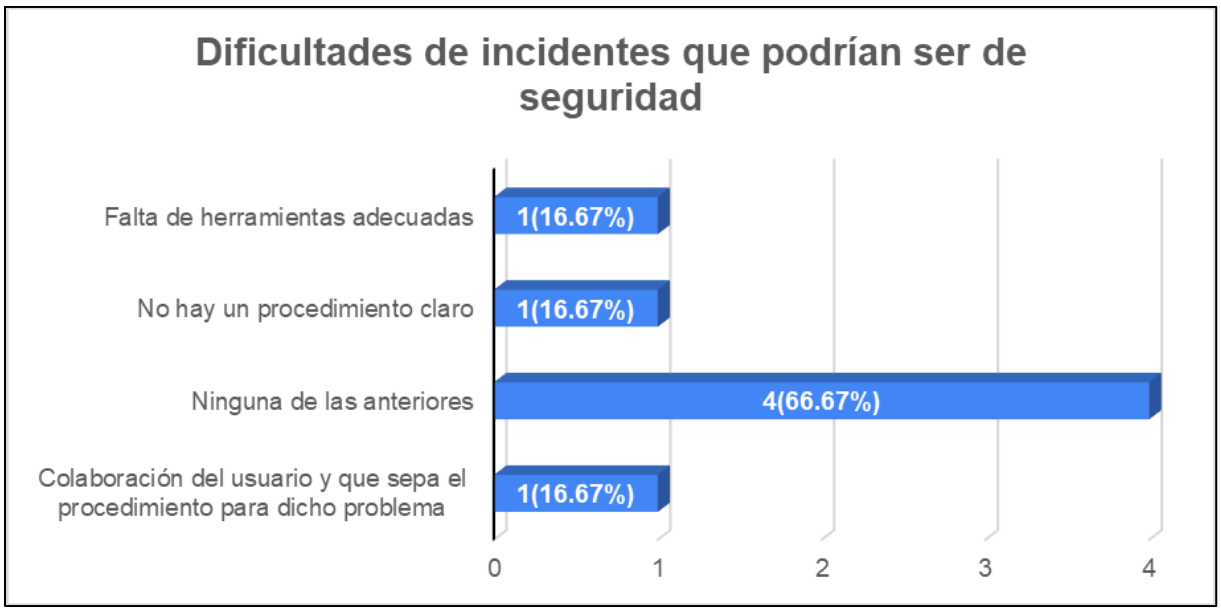
Análisis: Todos los encuestados señalaron contar con antivirus, sistemas de tickets y manuales internos, lo que indica cierta estructura básica para enfrentar incidentes. Sin embargo, no se mencionaron herramientas específicas de detección de intrusiones (IDS/IPS), SIEM o sistemas de respaldo automatizados. Aunque hay una base técnica funcional, el nivel actual de herramientas parece limitado para enfrentar ciberamenazas complejas. Sería prudente realizar una evaluación del estado tecnológico actual e invertir en herramientas de monitoreo, trazabilidad y análisis forense que respalden una política robusta de seguridad.

Gráfica 28: Errores de usuario que afecta el funcionamiento seguro de los equipos



Análisis: En la gráfica se muestran respuestas variadas entre 2(desacuerdo) y 5(totalmente de acuerdo). La desigualdad en las respuestas podría reflejar diferencias en los contextos de trabajo o el grado de interacción con usuarios finales. De cualquier modo, existe consenso en que el factor humano tiene un impacto en la seguridad operativa. Esto subraya la necesidad de campañas de concienciación, guías de uso seguro y capacitación para usuarios finales en prácticas digitales seguras.

Gráfica 29: Dificultades que enfrentan al atender incidentes que podrían ser de seguridad



Análisis: Este gráfico se puede interpretar que la mayoría respondieron ninguna de las anteriores, pero solo se tuvo una respuesta de las demás. Esto quiere decir que, aunque sea una percepción positiva, también podría deberse a una falta de concientización sobre limitaciones reales o a la normalización de la informalidad. Esto refuerza la necesidad de establecer procesos formales que permitan identificar obstáculos reales y superarlos mediante políticas de seguridad claras, adquisición de tecnología y definición de roles.

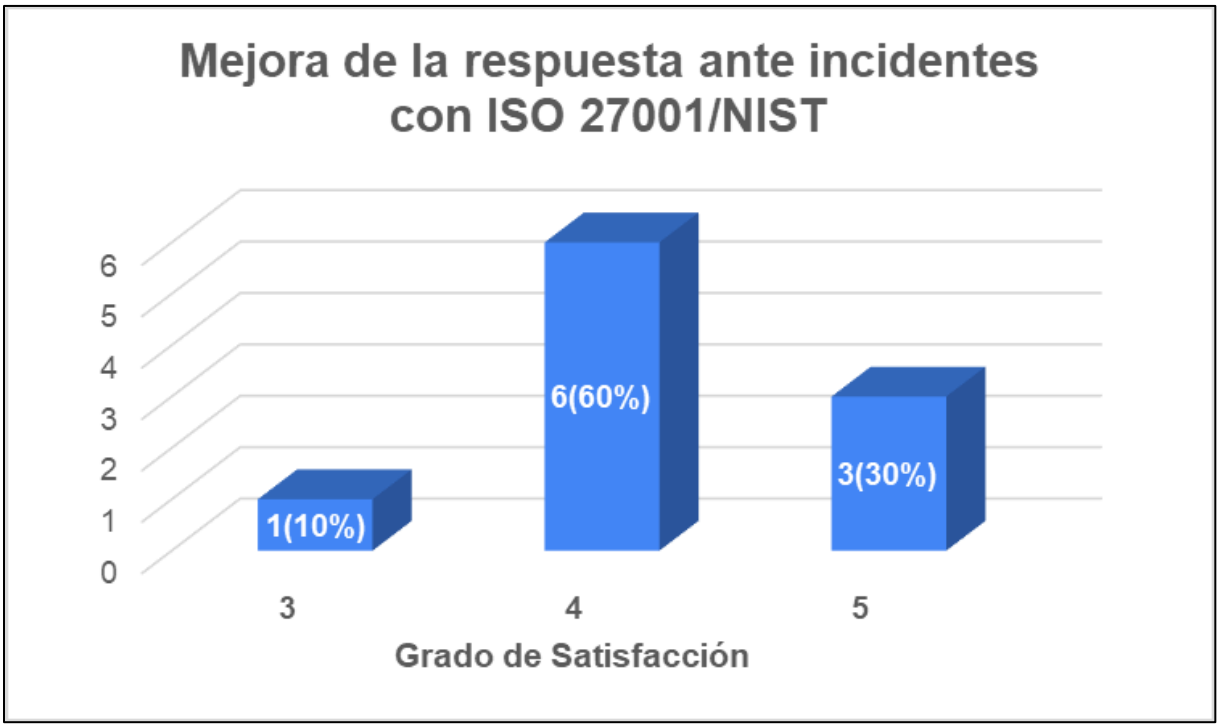
4.4 DISEÑO DE UNA METODOLOGÍA DE GESTIÓN DE INCIDENTE DE SEGURIDAD INFORMÁTICA

El diseño metodológico propuesto responde directamente a las debilidades identificadas. Se estructura en fases: preparación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas. Cada fase responde a un hallazgo concreto del análisis anterior. La metodología no se plantea como un documento estático, sino como un mecanismo vivo, adaptable a la realidad del hospital. Por ejemplo, la falta de recursos técnicos se aborda mediante

procedimientos claros y roles bien definidos, que permiten que incluso un equipo pequeño actúe coordinadamente ante un incidente.

Además, el componente de lecciones aprendidas busca impulsar la mejora continua, algo esencial en entornos donde las amenazas evolucionan rápidamente.

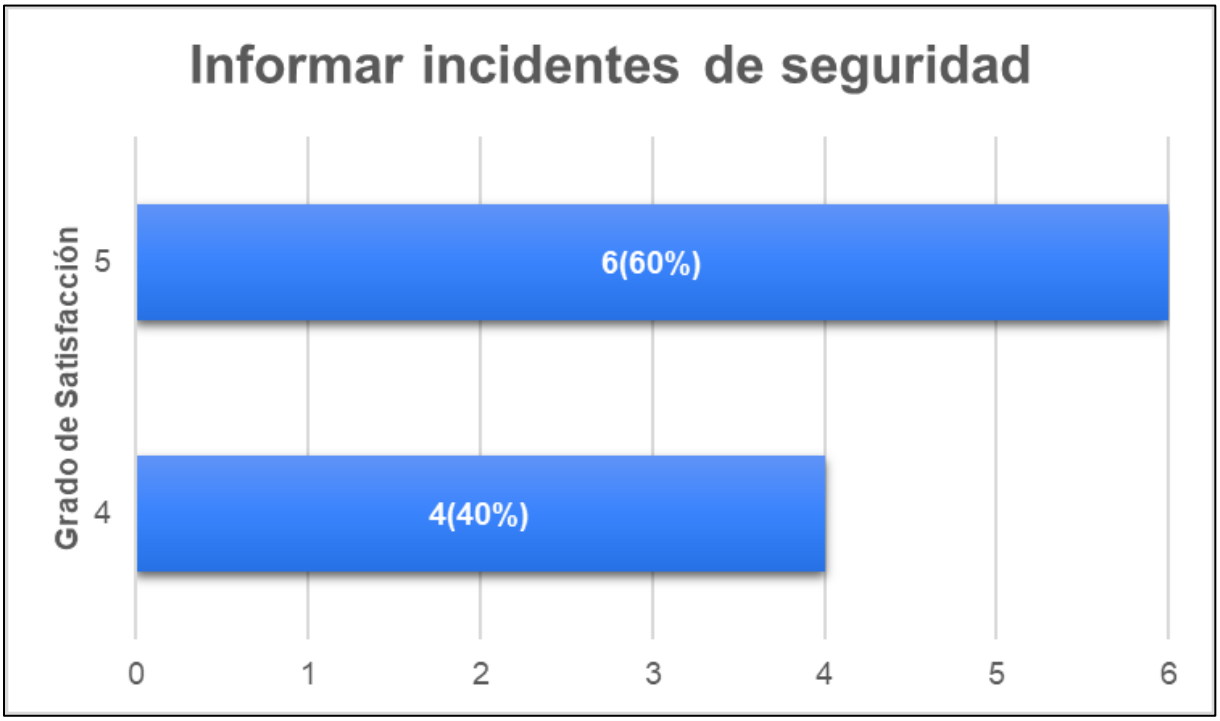
Gráfica 30: Mejora de la respuesta ante incidentes con ISO 27001/NIST



Análisis: Existe un consenso muy alto el 90% entre el personal de que la implementación de estándares de seguridad como ISO/NIST mejoraría significativamente la capacidad del hospital para responder a incidentes. Esta fuerte creencia positiva representa una oportunidad dorada para la organización: hay una comprensión interna del valor estratégico de estos marcos, lo que facilitaría enormemente cualquier iniciativa para formalizar y madurar la gestión de la seguridad de la información. El hospital debería capitalizar esta percepción para impulsar activamente la implementación de ISO/NIST, asegurando que los beneficios esperados puedan mejorar en gran

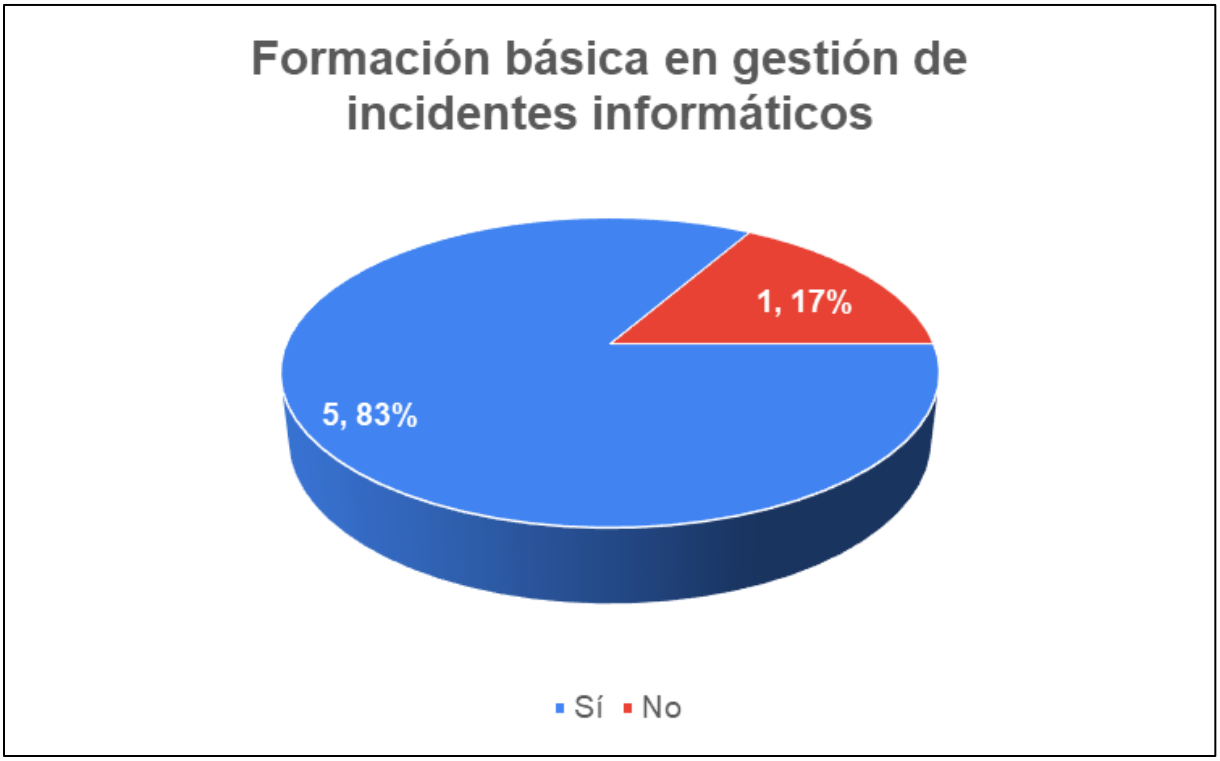
manera la respuesta a incidentes.

Gráfica 31: Informar incidentes de seguridad al área correspondiente



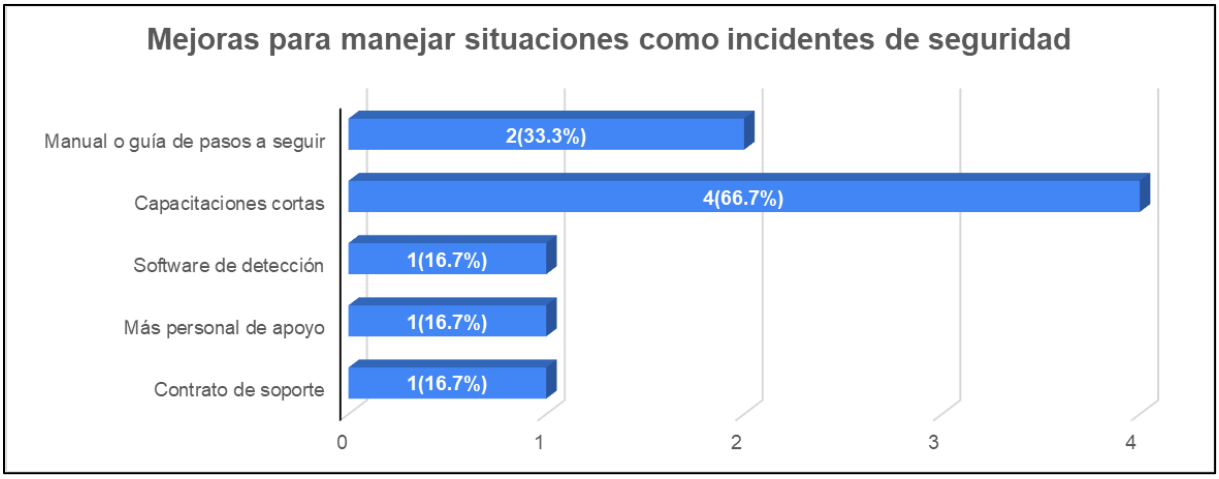
Análisis: Los resultados de esta pregunta son excepcionalmente positivos, con el 100% del personal afirmando que informan los incidentes al área correspondiente. Esto es un testimonio de una cultura de seguridad muy fuerte y de una alta conciencia sobre la importancia del reporte de incidentes en el hospital. Mantener esta proactividad es crucial, lo que implica asegurar que los canales de reporte sigan siendo accesibles y que el personal reciba retroalimentación, reforzando así su papel vital en la postura de seguridad del hospital.

Gráfica 32:Formación básica en gestión de incidentes informáticos



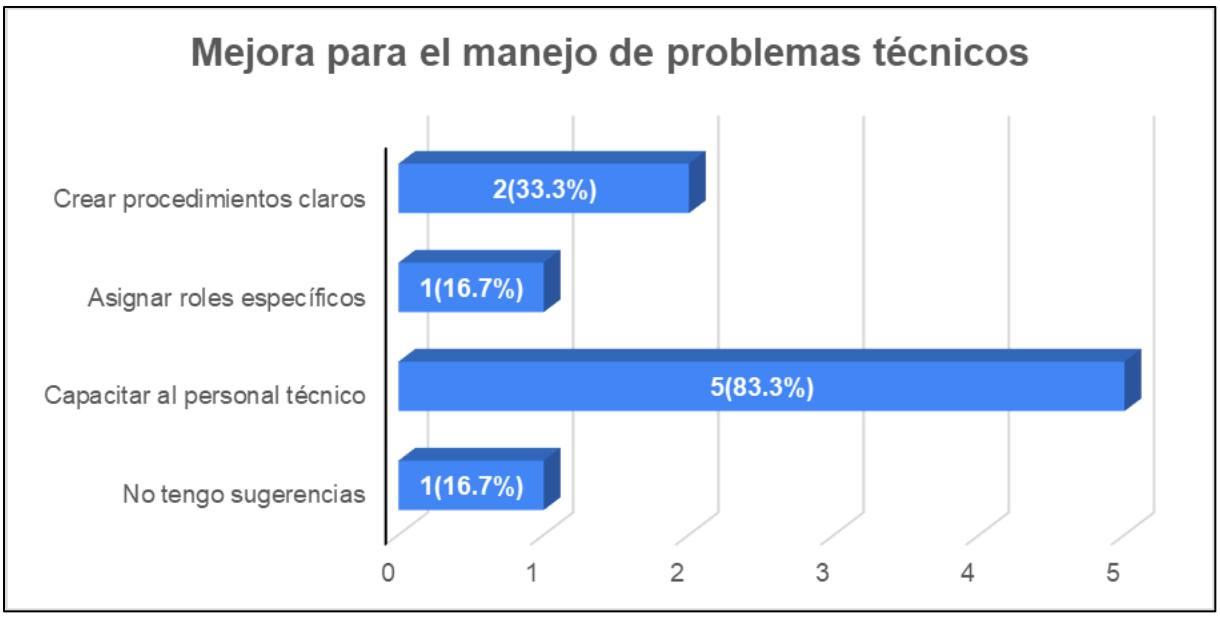
Análisis: Cuatro de los cinco encuestados respondieron afirmativamente. Esta mayoría muestra disposición para participar en procesos formativos y reconoce que su preparación actual no es suficiente para responder eficazmente ante incidentes. Esta disposición puede aprovecharse para implementar programas de formación en normas ISO 27035, NIST y buenas prácticas de seguridad, fortaleciendo las capacidades del equipo desde dentro.

Gráfica 33: Mejora para manejar situaciones como incidentes de seguridad



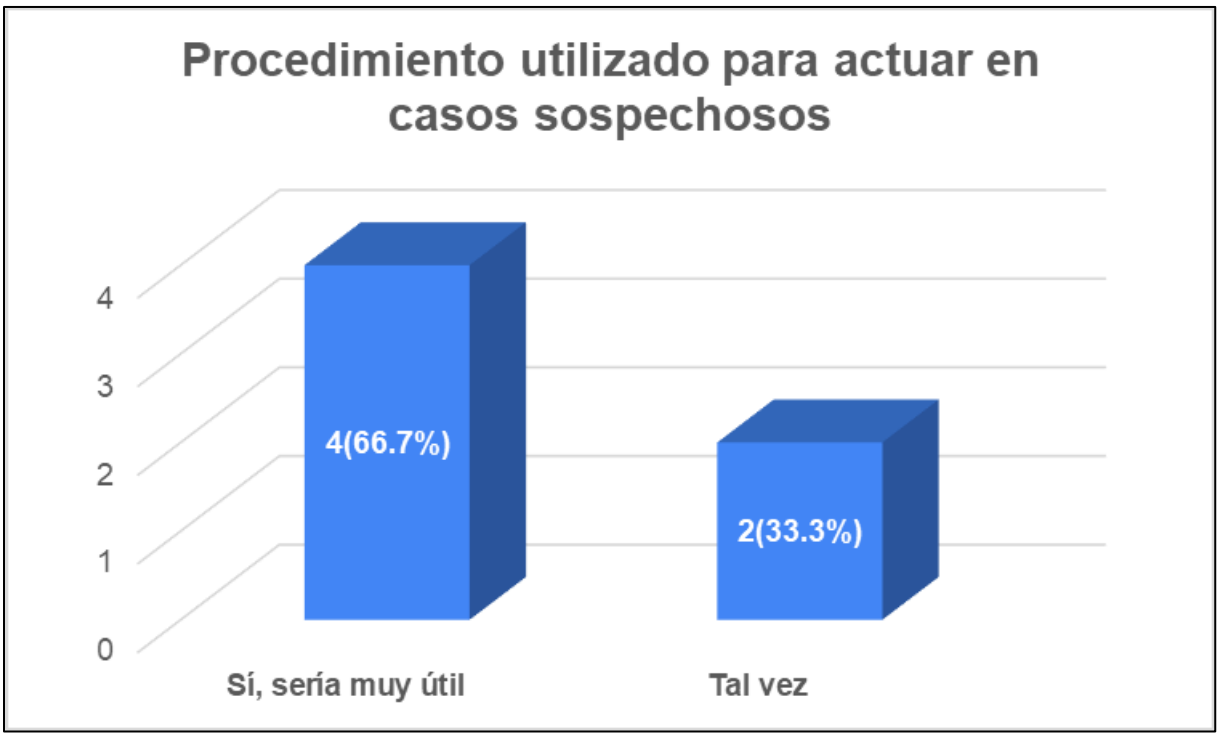
Análisis: Las respuestas variaron entre capacitaciones, manuales, apoyo técnico externo y más personal. Esto demuestra que el equipo reconoce múltiples carencias, tanto en conocimiento como en recursos. Esta diversidad de necesidades debe tomarse en cuenta para diseñar una estrategia integral que combine capacitación técnica, manuales prácticos y refuerzo estructural en personal e infraestructura.

Gráfica 34: Mejora para el manejo de problemas técnicos relacionados con seguridad informática



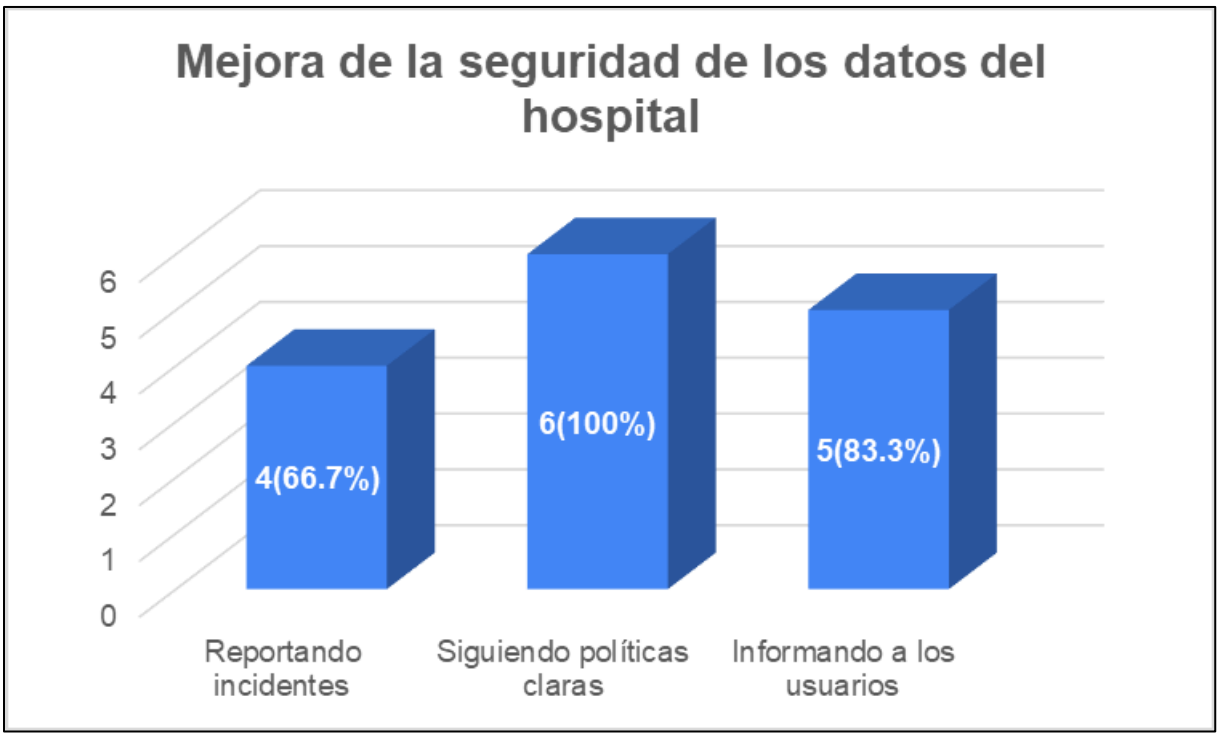
Análisis: La gráfica muestra que la mayoría respondieron que se deben mejorar las capacitaciones técnicas del personal, ya que según indica hay un cierto grado de poco conocimiento para atender ante estos tipos de problemas y eso afecta el rendimiento efectivo de las Hospital María, además de eso también se debe de mejorar los procedimientos, ya que al parecer son pocos claros para llevarlo a cabo de manera eficaz.

Gráfica 35: Procedimiento utilizado para actuar en casos sospechosos



Análisis: Cuatro de cinco consideran que un procedimiento que se detalle paso a paso el seguimiento sería muy útil. Esta percepción confirma que los técnicos necesitan una guía clara y estructurada para actuar eficazmente ante posibles incidentes de seguridad. Esto valida el desarrollo de protocolos operativos normalizados (PON) que sirvan como referencia rápida y alineen las acciones del personal técnico con estándares internacionales como ISO 27001 y NIST.

Gráfica 36: Mejora de la seguridad de los datos del hospital



Análisis: Las respuestas más comunes fueron: seguir políticas claras, reportar incidentes e informar a usuarios. Esta disposición para actuar proactivamente muestra que el personal tiene conciencia del valor de su rol en la cadena de seguridad. Con este capital humano, una estrategia basada en cultura organizacional, políticas claras y canales de reporte efectivos permitiría mejorar significativamente la postura de seguridad del hospital.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

El análisis realizado permitió confirmar que el Hospital María carece actualmente de una metodología estructurada para la gestión de incidentes de seguridad informática. Esta deficiencia pone en evidencia un alto grado de vulnerabilidad operativa, dado que la respuesta ante eventos adversos como accesos no autorizados, ransomware o pérdida de información depende en gran medida de la improvisación y la experiencia individual. En el contexto hospitalario, donde la información médica es altamente sensible, esta situación puede derivar en interrupciones críticas del servicio, exposición de datos personales y pérdida de confianza institucional.

Los resultados también reflejan un bajo nivel de madurez normativa dentro de la institución en cuanto a ciberseguridad. A pesar de la existencia de marcos internacionales como ISO 27001, ISO 27035 y el NIST SP 800-61r2, estos no han sido traducidos en políticas o lineamientos operativos que orienten al personal en la prevención, detección y tratamiento de incidentes. La desconexión entre el conocimiento general y su aplicación concreta refuerza la necesidad de establecer normativas internas adaptadas a las características específicas del hospital, fomentando así una cultura de seguridad organizacional más robusta.

Por otro lado, el estudio permitió identificar limitaciones importantes en los recursos humanos y tecnológicos disponibles para enfrentar ciberincidentes. La escasez de personal especializado y la falta de herramientas tecnológicas adecuadas reflejan una infraestructura aún incipiente en términos de seguridad informática. Ante esta situación, la metodología propuesta se diseñó con criterios de realismo y escalabilidad, permitiendo su implementación progresiva de acuerdo con las capacidades actuales del hospital, sin comprometer su efectividad.

A pesar de estas debilidades, se evidencia que es factible implementar una metodología propia, basada en estándares reconocidos internacionalmente, que responda al contexto específico del Hospital María. La propuesta metodológica planteada en este estudio establece fases claras, responsabilidades definidas, acciones correctivas y mecanismos de mejora continua, contribuyendo así al fortalecimiento institucional en materia de gestión de incidentes. Esta metodología representa una guía práctica y estructurada que puede elevar significativamente el nivel de preparación del hospital frente a amenazas informáticas.

Sin embargo, la viabilidad de esta implementación no depende únicamente de su diseño técnico, sino también de la disposición institucional para adoptar un cambio cultural. Es indispensable gestionar adecuadamente la transición hacia una cultura organizacional centrada en la ciberseguridad. Esto incluye la participación activa de todos los niveles jerárquicos, el respaldo de la alta dirección y la generación de conciencia respecto al valor de la información clínica y los riesgos asociados a su pérdida o exposición. Una estrategia de implementación sin acompañamiento humano e institucional corre el riesgo de ser ignorada o aplicada de forma parcial e ineficaz.

Finalmente, la sostenibilidad de esta estrategia solo será posible si se refuerza con un proceso constante de formación y sensibilización. La capacitación del personal técnico, administrativo y clínico debe convertirse en una práctica recurrente, orientada a fortalecer la responsabilidad compartida frente a la seguridad digital. La construcción de una cultura institucional resiliente ante las amenazas informáticas representa un componente fundamental para garantizar la continuidad operativa del Hospital María, proteger los datos sensibles de los pacientes y asegurar el cumplimiento de las buenas prácticas en ciberseguridad a nivel organizacional.

5.2 RECOMENDACIONES

Con base en los hallazgos obtenidos y en referencia a marcos internacionales de buenas prácticas, se proponen las siguientes recomendaciones para fortalecer la gestión de incidentes de seguridad informática en el Hospital María.

A partir de los hallazgos obtenidos y con el objetivo de fortalecer la gestión de incidentes de seguridad informática en el Hospital María, se proponen las siguientes recomendaciones estratégicas y operativas, todas adaptadas a la realidad del entorno hospitalario y alineadas con estándares internacionales:

Es fundamental diseñar e implementar una metodología de gestión de incidentes que se ajuste al contexto específico del hospital, contemplando desde la detección temprana de eventos hasta su recuperación y documentación final. Esta metodología debe estructurarse en fases claramente definidas —detección, análisis, respuesta, erradicación, recuperación y lecciones aprendidas— e integrar la asignación de roles específicos, flujos de comunicación efectivos y criterios de priorización. Por ejemplo, ante un intento de intrusión en el sistema de historias clínicas, debe activarse un protocolo de análisis inmediato, aislamiento del sistema afectado, documentación del incidente y notificación a los responsables.

Asimismo, se recomienda formalizar y difundir procedimientos operativos normalizados que orienten al personal técnico en la actuación ante incidentes. Estos protocolos deben especificar paso a paso qué hacer en escenarios comunes como infecciones por malware, caídas de servicios o accesos no autorizados. La elaboración de manuales operativos, infografías y guías prácticas puede facilitar su comprensión y aplicación diaria. Socializar estos documentos mediante talleres o reuniones breves fortalecerá su apropiación por parte del equipo de TI.

Otra acción prioritaria es ampliar la capacitación técnica y organizacional mediante un plan

de formación continua. Este debe abarcar tanto al personal TIC como a usuarios finales (médicos, administrativos, técnicos), e incluir temas como identificación de amenazas, uso de herramientas de respuesta, análisis forense básico y principios de seguridad según ISO 27001 y NIST SP 800-61r2. Las capacitaciones pueden combinarse con guías rápidas de escritorio o cápsulas informativas digitales, asegurando un aprendizaje constante y contextualizado.

En paralelo, es indispensable reforzar las capacidades operativas del equipo técnico mediante la evaluación y actualización de las herramientas disponibles. Se sugiere incorporar tecnologías como sistemas de detección de intrusos (IDS), mecanismos de respaldo automático con monitoreo, tableros (dashboards) de incidentes que permitan visualizar y dar seguimiento a eventos críticos, y plataformas que garanticen la trazabilidad y conservación de evidencias digitales en caso de análisis posteriores o auditorías.

Dado que la ciberseguridad es una responsabilidad compartida, se debe involucrar activamente a los usuarios en la protección del sistema institucional. Para ello, se proponen campañas internas de sensibilización sobre buenas prácticas digitales, así como la realización de simulacros prácticos —por ejemplo, sobre cómo actuar ante correos de phishing o mensajes sospechosos—. También se pueden distribuir materiales educativos como afiches, videos breves o instructivos impresos cerca de estaciones de trabajo, fomentando el reporte temprano de anomalías.

Complementariamente, se sugiere la creación de un comité institucional de seguridad de la información, integrado por personal de TI, representantes de la dirección y áreas clave del hospital. Este comité debe liderar y coordinar la ejecución de la metodología propuesta, dar seguimiento a incidentes, evaluar riesgos emergentes y promover la mejora continua. Además, debe generar espacios de retroalimentación interna tras cada incidente significativo, sistematizando lecciones

aprendidas y fortaleciendo la preparación institucional.

Por último, es urgente asignar recursos técnicos y humanos dedicados exclusivamente a funciones de ciberseguridad. La contratación o capacitación de personal especializado en gestión de incidentes, análisis forense digital y cumplimiento normativo permitirá responder de forma más oportuna y eficaz ante eventos críticos. Este fortalecimiento del equipo debe acompañarse de la provisión de recursos económicos y tecnológicos que garanticen la sostenibilidad de la estrategia en el tiempo.

Estas recomendaciones buscan no solo responder a las debilidades identificadas, sino también impulsar una transformación cultural en el hospital, posicionando la ciberseguridad como un eje transversal para la protección de los servicios clínicos y la integridad de la información institucional.

5.3 CONSIDERACIONES FINALES

La presente investigación permitió evidenciar que el Hospital María enfrenta desafíos significativos en la gestión de incidentes de seguridad informática. Si bien existe conciencia sobre la importancia de proteger los activos digitales, la falta de procedimientos estandarizados, herramientas especializadas y una cultura organizacional madura en ciberseguridad limita la capacidad institucional para prevenir, detectar, responder y recuperarse ante incidentes.

Los resultados obtenidos mediante la encuesta aplicada al personal técnico revelan una estructura operativa enfocada mayoritariamente en la atención de fallas técnicas comunes, sin una diferenciación clara entre problemas operativos y eventos de seguridad. Aunque el personal demuestra buena disposición para aprender y contribuir activamente a la protección de los sistemas, su formación es heterogénea, y la mayoría expresa la necesidad de contar con

procedimientos paso a paso, capacitaciones formales y mayores recursos para enfrentar amenazas cibernéticas.

Este contexto evidencia la urgencia de adoptar un enfoque proactivo y estructurado basado en estándares reconocidos internacionalmente como ISO/IEC 27001, ISO 27035 y el marco NIST. Desarrollar una metodología de gestión de incidentes ajustada a la realidad del hospital no solo permitirá fortalecer las capacidades técnicas del equipo TIC, sino que también contribuirá a mejorar la resiliencia institucional, garantizar la continuidad de los servicios médicos y proteger la información sensible de los pacientes.

En este sentido, la gestión de la seguridad informática no debe entenderse como una función aislada del área de tecnología, sino como un compromiso transversal que requiere el involucramiento de todos los actores institucionales, desde los usuarios hasta los niveles directivos. La construcción de una cultura organizacional orientada a la seguridad, apoyada en la formación continua, la planificación estratégica y la asignación adecuada de recursos, es indispensable para enfrentar con éxito los riesgos del entorno digital en el ámbito hospitalario.

CAPÍTULO VI. APLICABILIDAD

6.1 NOMBRE DE LA PROPUESTA

Desarrollo de una metodología de gestión de incidentes de seguridad informática para el Hospital María, basada en las normas ISO 27001 e ISO 27035 y los protocolos del NIST.

6.2 JUSTIFICACIÓN DE LA PROPUESTA

La presente propuesta metodológica se fundamenta en los hallazgos obtenidos a partir del desarrollo de los objetivos específicos establecidos en esta investigación, los cuales se abordaron sistemáticamente en el capítulo IV. En primer lugar, en lo relacionado con la identificación de vulnerabilidades y amenazas presentes en el Hospital María, los resultados de las encuestas y entrevistas aplicadas al personal técnico revelaron una alta frecuencia de incidentes de seguridad informática, como accesos no autorizados, errores de configuración, infecciones por malware y fallos recurrentes en los equipos. A pesar de estos eventos, no se dispone de una política formal ni de procedimientos estandarizados para su gestión. Esta situación pone en evidencia la necesidad de establecer una metodología institucional que permita al hospital adoptar mecanismos preventivos, de respuesta y recuperación ante incidentes de ciberseguridad, en consonancia con el objetivo específico número uno.

Asimismo, en lo que respecta al segundo objetivo específico, orientado a examinar los marcos normativos y buenas prácticas aplicables en el contexto hospitalario, se determinó que, si bien existe conocimiento teórico sobre normativas como ISO 27001, ISO 27035 y los lineamientos del NIST, no se ha logrado institucionalizar su aplicación dentro del Hospital María. La propuesta que se formula en este estudio busca, por tanto, subsanar esa brecha mediante la adopción de dichos marcos como base estructural, de forma que se promueva la creación de políticas claras, roles

definidos y procedimientos formalizados para la gestión de incidentes, en concordancia con estándares internacionales.

En relación con el tercer objetivo específico, enfocado en el análisis de los recursos y capacidades institucionales, el estudio evidenció deficiencias relevantes en infraestructura tecnológica, herramientas de detección de incidentes, monitoreo en tiempo real y capacitación del personal técnico. Se identificó la inexistencia de soluciones como sistemas SIEM, respaldos automáticos, protocolos de análisis forense, así como una limitada asignación presupuestaria para fortalecer estos aspectos. En este sentido, la propuesta metodológica incorpora medidas que permiten optimizar el uso de los recursos disponibles y plantea acciones que pueden ser implementadas progresivamente según las capacidades institucionales, haciendo viable su aplicación en el entorno hospitalario.

Finalmente, el diseño metodológico presentado responde al cuarto objetivo específico, el cual consistió en estructurar una propuesta adaptada a las necesidades del Hospital María. Esta metodología considera las características particulares de la institución, tales como su nivel de madurez organizacional en materia de ciberseguridad, los roles y funciones del personal técnico y los desafíos propios del sector salud. Por lo tanto, la propuesta se justifica plenamente como un mecanismo técnico-práctico orientado a mejorar la capacidad institucional de prevención, detección, respuesta y recuperación ante incidentes de seguridad informática, fortaleciendo así la protección de los datos clínicos, la continuidad de los servicios médicos y el cumplimiento normativo.

6.3 ALCANCE DE LA PROPUESTA

La propuesta está dirigida a fortalecer el área de tecnología de la información del Hospital María, aplicando una metodología de gestión de incidentes que abarque todo el ciclo de vida del

incidente: desde la identificación hasta la recuperación. Esta metodología será aplicable a todas las unidades que utilicen sistemas informáticos y manejen datos sensibles, incluyendo áreas clínicas, administrativas y de soporte técnico. Asimismo, incluye procesos de capacitación continua y evaluación para garantizar su sostenibilidad a largo plazo.

6.4 DESCRIPCIÓN Y DESARROLLO

6.4.1 DESCRIPCIÓN

La metodología propuesta integra los elementos esenciales del ciclo de respuesta a incidentes del NIST, adaptados a la realidad tecnológica y organizacional del Hospital María. Se estructura en seis fases principales: preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas, con una gestión transversal del riesgo y de la evidencia digital.

6.4.2 DESARROLLO

El desarrollo de la propuesta metodológica se estructura a partir de las fases esenciales del ciclo de vida de la gestión de incidentes de seguridad informática, tomando como base los lineamientos del NIST, las normas ISO/IEC 27001 e ISO/IEC 27035, y adaptándolos al contexto operativo del Hospital María. Esta propuesta se organiza en seis fases: preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas. A continuación, se detalla cada fase, acompañada de estrategias operativas y elementos gráficos que facilitan su implementación.

Fase 1: Preparación

En esta fase se establecen las condiciones necesarias para responder a un incidente. Incluye la identificación de activos críticos, el establecimiento del Equipo de Respuesta ante Incidentes (ERI), y la formalización de políticas de seguridad informática.

Tabla 1. Elementos clave de la preparación

Tabla 6: Elementos claves de la preparación

Elemento	Acción propuesta
Inventario de activos críticos	Servidores, estaciones clínicas, bases de datos, redes
Conformación del ERI	Asignación de líder, analista forense, técnico de mitigación, responsable legal
Capacitación	Formación en NIST, ISO 27001/27035, análisis forense
Documentación	Manual de funciones, flujogramas, bitácoras

Fase 2: Identificación

Busca detectar eventos que podrían constituir incidentes. Se propone el uso de herramientas SIEM, antivirus con alertas automatizadas y monitoreo continuo de logs.

Figura 10: Proceso de identificación de incidentes

Fase 3: Contención

Se enfoca en limitar la propagación del incidente. Esta fase requiere acciones inmediatas como el aislamiento del sistema afectado, cambios de contraseñas y bloqueo de accesos.

Tabla 2. Niveles de respuesta y acciones de contención

Tabla 7: Niveles de respuesta y acciones de contención

Nivel del incidente	Ejemplo	Acción inmediata
Crítico	Ransomware	Aislar sistema, activar ERI completo
Moderado	Malware detectado	Contención por técnico y validación del ERI
Bajo	Intento fallido de acceso	Registro en bitácora, monitoreo continuo

Fase 4: Erradicación

En esta etapa se eliminan las amenazas detectadas. Se realiza limpieza de sistemas, eliminación de software malicioso, análisis de logs y corrección de configuraciones vulnerables.

Actuaciones clave:

- Uso de herramientas de análisis forense.
- Escaneo completo del sistema comprometido.
- Refuerzo de configuraciones de seguridad.

Fase 5: Recuperación

Se restauran los servicios afectados desde respaldos seguros y se valida su integridad. Esta fase incluye pruebas de funcionamiento y monitoreo post-incidente.

Tabla 3. Acciones de recuperación

Tabla 8: Acciones de recuperación

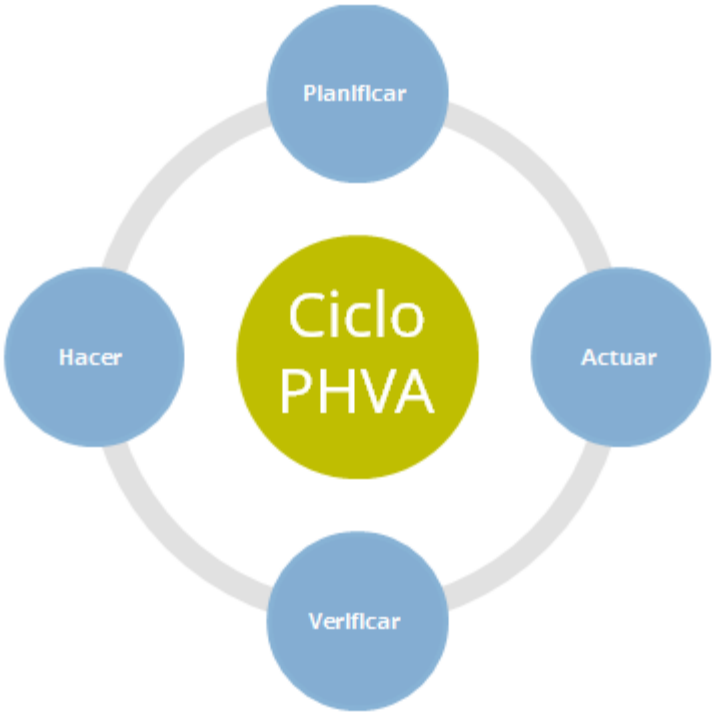
Sistema comprometido	Acción
Base de datos	Restauración desde backup diario y verificación de integridad
Red interna	Segmentación temporal y revisión de políticas de firewall
Estaciones clínicas	Reconfiguración y reinstalación con imagen verificada

Fase 6: Lecciones aprendidas

Consiste en documentar todo el proceso del incidente, generar informes, actualizar políticas y reforzar la capacitación del personal. Este paso garantiza la mejora continua del sistema de gestión.

Ciclo de mejora continua post-incidente (PDCA adaptado a NIST)

Figura 11: Ciclo de vida PHVA



Se han detallado procesos que facilitarán el acoplo del personal técnico a los procesos recomendados y para lograr estandarizar el cómo mitigar los sucesos de forma efectiva, a continuación se detallan los mismos:

1. Diagnóstico inicial de activos críticos y vulnerabilidades

Tabla 9: Diagnóstico inicial de activos

Etapa	Acción o Actividad
Proceso	- Inventario de activos tecnológicos (servidores, redes, estaciones, bases de datos, sistemas clínicos). - Evaluación de vulnerabilidades mediante escaneo de red y entrevistas. - Identificación de amenazas potenciales (ransomware, accesos no autorizados, phishing, etc.).
Solución	- Elaboración de una matriz de riesgo. - Clasificación de activos por nivel de criticidad.
Nivel de respuesta	- Alta prioridad: Sistemas que gestionan datos clínicos y pacientes. - Media prioridad: Sistemas administrativos. - Baja prioridad: Sistemas auxiliares no críticos.
Actuación	- Aplicar parches de seguridad y segmentar redes vulnerables de inmediato en activos de alta prioridad.

2. Elaboración de políticas y procedimientos de respuesta a incidentes

Tabla 10: Elaboración de políticas y procedimientos de respuesta a incidentes

Etapa	Acción o Actividad
Proceso	Redacción de un Plan de Respuesta a Incidentes (PRI). (Ver Anexo 3) Establecimiento de protocolos de detección, reporte, análisis y mitigación.
Solución	- Políticas claras de seguridad informática (uso de contraseñas, acceso remoto, respaldo de información). - Manual operativo para respuesta a eventos de seguridad.
Nivel de respuesta	- Incidente leve (ej. intento de acceso no autorizado): respuesta en menos de 24 horas. - Incidente moderado (ej. malware detectado): contención inmediata y análisis forense básico. - Incidente severo (ej. ataque ransomware): respuesta inmediata, escalamiento al Comité de Seguridad.
Actuación	- Activar el PRI según clasificación. - Documentar cada paso del proceso.

3. Asignación de roles y responsabilidades dentro del equipo de respuesta

Tabla 11: Asignación y roles y responsabilidades

Etapa	Acción o Actividad
Proceso	- Definición del Equipo de Respuesta ante Incidentes (ERI). - Asignación de funciones específicas: líder de incidentes, analista forense, responsable de comunicación, técnico de mitigación.
Solución	- Manual de funciones para cada miembro del ERI (Ver Anexo 4). - Integración con personal administrativo y legal cuando sea necesario.
Nivel de respuesta	- Activación total del ERI en incidentes severos. - Delegación parcial en eventos menores (líder + técnico).
Actuación	Cada miembro debe seguir protocolos establecidos y reportar en la bitácora digital del incidente.

4. Integración de herramientas tecnológicas para detección y monitoreo continuo

Tabla 12: Integración de herramientas tecnológicas

Etapa	Acción o Actividad
Proceso	- Implementación de un Sistema de Detección de Intrusos (IDS/IPS). - Configuración de alertas de seguridad en tiempo real. - Integración con software de monitoreo de logs y SIEM.
Solución	Herramientas automatizadas que detecten comportamientos anómalos. - Correlación de eventos en un panel de control centralizado.
Nivel de respuesta	Nivel 1: Alerta informativa – seguimiento. Nivel 2: Alerta de advertencia – evaluación del riesgo. Nivel 3: Alerta crítica – respuesta inmediata.
Actuación	- Verificación manual por el analista de seguridad. - Aplicación de contención o desconexión del sistema según criticidad.

5. Capacitación del personal técnico en el uso de protocolos de gestión de incidentes

Se recomienda realizar la ejecución de talleres especializados enfocados en la norma ISO 27001, el marco NIST y el manejo efectivo de incidentes de seguridad informática, con el objetivo de fortalecer el conocimiento teórico y práctico del personal. Además, se brindará capacitación práctica que incluirá procedimientos detallados de contención, análisis y mitigación de incidentes, asegurando que el equipo esté preparado para responder de manera eficiente ante cualquier

eventualidad. Como parte fundamental de la solución, se elaborará un manual de respuesta rápida ante incidentes (ver Anexo 5), que servirá como guía oficial para estandarizar los procesos de actuación. También se implementarán cursos recurrentes, tanto virtuales como presenciales, para mantener actualizados los conocimientos y habilidades del personal a lo largo del tiempo.

Para medir el nivel de respuesta y efectividad de las capacitaciones, se establecerán mecanismos de evaluación que incluirán pruebas de competencias antes y después de cada ciclo formativo, además del registro detallado de asistencia y desempeño en simulaciones prácticas de incidentes. De esta manera, se garantizará que el personal no solo participe, sino que también adquiera y demuestre las capacidades necesarias para manejar situaciones reales.

En cuanto a la actuación, se adoptará un enfoque proactivo en el que, si algún miembro del equipo no demuestra un dominio adecuado de los protocolos críticos durante las evaluaciones, se procederá a la reasignación de funciones o a la realización de capacitaciones adicionales específicas, con el fin de asegurar que todos los integrantes del equipo cumplan con los estándares requeridos para una respuesta rápida y efectiva frente a incidentes de seguridad.

6. Simulación de escenarios de ataque

Se recomienda llevar a cabo la creación y ejecución de ejercicios de simulacro que recrearán incidentes reales, tales como ataques de ransomware, fugas de datos y ataques de denegación de servicio distribuido (DDoS), con el propósito de evaluar la capacidad de respuesta del equipo ante situaciones críticas. Durante estos simulacros, se medirá cuidadosamente el tiempo de respuesta y las acciones tomadas para identificar fortalezas y áreas de mejora en los procedimientos establecidos.

Como parte de la solución, se deberá elaborar un informe de evaluación posterior a cada

simulacro, en el cual se detallarán los resultados obtenidos, los fallos detectados y las recomendaciones necesarias para corregirlos. Este informe servirá como base para la actualización continua del Plan de Respuesta a Incidentes, asegurando que se mantenga vigente y adaptado a las amenazas actuales.

Para mantener un nivel óptimo de preparación, se realizarán simulacros de forma semestral con el objetivo de mantener al equipo en constante alerta y medir su eficiencia ante posibles incidentes. Además, se implementarán simulacros sorpresivos, que permitirán evaluar la preparación real y la capacidad de reacción inmediata sin previo aviso.

En cuanto a la actuación, el Equipo de Respuesta ante Incidentes (ERI) responderá a cada simulacro como si se tratara de un evento real, aplicando todos los protocolos establecidos. Se documentará de manera completa cada acción realizada y se proporcionará retroalimentación inmediata para fortalecer el desempeño del equipo y mejorar los procesos de respuesta futuros.

7. Documentación y generación de informes post-incidente

Se recomienda establecer un proceso sistemático para la redacción de informes detallados tras la ocurrencia de cada incidente de seguridad o simulacro realizado. Estos informes serán fundamentales para el análisis posterior y la toma de decisiones estratégicas. Además, se implementará un sistema de registro centralizado en una base de datos que almacenará todos los incidentes históricos, permitiendo su consulta y análisis en futuras auditorías o revisiones de seguridad.

Como parte de la solución, se utilizarán formatos estándar para la recolección de datos clave, que incluirán información como la hora del incidente, el sistema afectado, la causa raíz, las acciones correctivas aplicadas y las lecciones aprendidas. Este enfoque estructurado garantizará

uniformidad en la documentación y facilitará el análisis comparativo entre diferentes eventos.

El nivel de respuesta determinará que la elaboración de estos informes será obligatoria para todos los incidentes clasificados como moderados o severos, dado el impacto potencial que representan. Esto permitirá enfocar los esfuerzos de documentación en aquellos eventos que realmente comprometan la seguridad operativa del hospital.

En cuanto a la actuación, el líder del Equipo de Respuesta ante Incidentes (ERI) será el responsable de generar el informe técnico y presentarlo formalmente ante la Dirección General del hospital y el Comité de Seguridad Informática. Asimismo, se incorporará una fase de mejora continua, en la cual se aplicarán los aprendizajes obtenidos durante la gestión de incidentes y se realizarán auditorías periódicas conforme a los lineamientos de la norma ISO/IEC 27001. Esta fase permitirá ajustar y perfeccionar constantemente los procesos de respuesta, fortaleciendo la postura de seguridad institucional.

Conclusión del desarrollo:

La metodología propuesta constituye una guía técnica y operativa viable para ser adoptada por el Hospital María. Cada fase responde directamente a los riesgos identificados en el capítulo IV y contribuye a fortalecer la resiliencia institucional frente a incidentes de seguridad informática. Se recomienda su implementación gradual, acompañada de monitoreo, auditoría periódica y formación continua del personal técnico.

6.4.2.1 MATRIZ DE CORRESPONDENCIA ENTRE LA METODOLOGÍA PROPUESTA Y ESTÁNDARES ISO/NIST

Matriz de Vinculación: Metodología vs ISO 27001 / ISO 27035 / NIST 800-61r2

Fase de la Metodología	ISO/IEC 27001	ISO/IEC 27035	NIST SP 800-61r2
1. Preparación y planificación	A.6.1.1, A.7.2.2, A.12.6.1, A.18.2.3	Parte 1: Sección 6.1 y 6.2 – Preparación para incidentes	Sección 3.1 – Preparación
2. Detección e identificación del incidente	A.12.4.1, A.16.1.2, A.16.1.4	Parte 1: Sección 6.3 – Detección y notificación de eventos	Sección 3.2 – Detección y análisis
3. Análisis y evaluación del incidente	A.16.1.5	Parte 1: Sección 6.4 – Evaluación y decisión de respuesta	Sección 3.2 – Detección y análisis
4. Contención del incidente	A.16.1.5, A.17.1.2	Parte 1: Sección 6.5 – Contención	Sección 3.3 – Contención, erradicación y recuperación
5. Erradicación y recuperación	A.17.1.1, A.17.2.1	Parte 1: Sección 6.6 – Erradicación y recuperación	Sección 3.3 – Contención, erradicación y recuperación
6. Lecciones aprendidas y mejora continua	A.16.1.6, A.18.1.1	Parte 1: Sección 6.7 – Revisión post-incidente	Sección 3.4 – Actividades post-incidente

6.4.3 GESTIÓN DEL CAMBIO PARA LA IMPLEMENTACIÓN DE LA METODOLOGÍA

La implementación de la metodología de gestión de incidentes de seguridad informática en el Hospital María requiere un enfoque estructurado de gestión del cambio que facilite la transición desde los procesos actuales hacia una cultura organizacional más proactiva y alineada con los estándares internacionales (ISO/IEC 27001, ISO/IEC 27035 y NIST SP 800-61r2). Para ello, se propone un plan de gestión del cambio con las siguientes acciones clave:

1. **Comunicación Efectiva:** se informará de forma clara y continua a todo el personal involucrado en tecnologías de la información y ciberseguridad sobre los beneficios, alcances y responsabilidades asociadas con la nueva metodología.

2. **Capacitación y Sensibilización:** se impartirán sesiones de formación específicas sobre el nuevo proceso de gestión de incidentes, el uso de formatos estandarizados, tiempos de respuesta, y responsabilidades individuales y grupales. También se abordarán temas de concienciación para reducir la resistencia al cambio.
3. **Participación Activa del Personal:** se fomentará la participación de los equipos técnicos en la validación e implementación piloto de la metodología, asegurando así mayor apropiación del proceso.
4. **Gestión de la Resistencia al Cambio:** se identificarán posibles focos de resistencia y se atenderán mediante acompañamiento directo, retroalimentación constante y generación de evidencia sobre los beneficios operativos de la metodología.
5. **Seguimiento y Mejora Continua:** la unidad de TI, en coordinación con la jefatura de ciberseguridad, dará seguimiento continuo a la adopción del nuevo proceso, midiendo su efectividad mediante indicadores previamente definidos (número de incidentes gestionados, tiempo de respuesta, calidad de los informes, etc.).
6. **Apoyo de la Alta Dirección:** el compromiso de la Dirección del hospital será esencial para legitimar el cambio, asignar los recursos necesarios y mantener la metodología como un proceso institucionalizado.

Este enfoque busca asegurar que la metodología no solo sea adoptada formalmente, sino que genere un cambio real en la cultura de gestión de incidentes, elevando el nivel de madurez de ciberseguridad institucional.

6.4.4 ANÁLISIS FODA

Un análisis FODA (Fortaleza, Oportunidades, Debilidades y Amenazas) es una herramienta muy importante que permite poder analizar todos los puntos clave de la empresa para gestionar mejorar las estrategias del proyecto, en este caso se utiliza para mejorar las estrategias del área de TI con el propósito de identificar e identificar las vulnerabilidades y hacer frente a ellos. Para ello se elaboró lo siguiente:

- **Estrategia FO (Fortalezas y Oportunidades):** Como se puede utilizar esas fortalezas para convertirlo en oportunidades y hacer frente a ciberataques.
- **Estrategia FA (Fortaleza y Amenaza):** Como se puede disminuir o evitar las amenazas utilizando las fortalezas.
- **Estrategia DO (Debilidades y Oportunidades):** Cuales oportunidades pueden hacer frentes a las debilidades para corregir errores y conseguir mejores resultados
- **Estrategia DA (Debilidades y Amenazas):** Identificar que debilidades puedes convertirse en una gran amenaza y corregirlo de manera inmediata

Estas estrategias ayudan a poder hacer una buena toma de decisiones ante un incidente y evitar riesgos algunos, maximizando optimizaciones, respuesta ante incidentes, capacitaciones y mejorando la buena comunicación.

Tabla 13: Estrategias de Análisis FODA

ANÁLISIS FODA	**Fortaleza**	**Debilidades**
	1. Conocimiento amplio de estándares como ISO/NIST. 2. Buena práctica de documentación y análisis de incidentes de seguridad. 3. Una cultura que fomenta la seguridad sin temor a represalias. 4. Personal preparada para actuar ante un incidente informático.	1. La falta de auditoría no es constante ni sistemático. 2. Sus políticas no son claras para el seguimiento de task. 3. Falta de comunicación entre empleados. 4. Fallos en controles de seguridad.
	Oportunidades	**Amenazas**
	1. Equipos especializado para la detección de incidentes. 2. Se asignan los recursos suficientes para la ciberseguridad. 3. Informan de manera inmediata los incidentes de seguridad. 4. Capacitaciones sobre ciberseguridad.	1. Ciberataques. 2. Riesgos de fallos por falta de claridad. 3. Aprovechamiento de vulnerabilidad. 4. Sabotaje de datos.
ESTRATEGIAS ORIENTADAS A LAS FORTALEZAS	**Estrategia FO**	**Estrategia FA**
	1. Implementar tecnologías avanzadas para más protección en la seguridad de los datos, como firewall de nueva generación y detección de amenazas. 2. Fortalecer la cultura organizacional de seguridad para promover buenas prácticas y capacitaciones alineada a los estándares internacionales como ISO 27001/NIST.	1. Desarrollar protocolos de defensas proactiva aprovechando el conocimiento del personal en ciberseguridad para afrontar ataques e incidentes. 2.Utilizar la ventaja de los equipos especializados para resistir o prevenir ataques como phishing y malware.
ESTRATEGIAS ORIENTADA A LAS DEBILIDADES	**Estrategia DO**	**Estrategia DA**
	1. Mejorar el sistema de control y auditoría interna implementando normativas emergentes. 2. Formalizar políticas de seguridad cibernética basada en ISO/NIST para compensar la falta de normativa interna estructurada.	1. Elaborar un plan de respuesta ante incidentes que compense la falta de protocolos ante amenazas. 2. Buscar comunicación con transparencia para disminuir la baja concienciación del personal ante ataques o incidentes.

6.4.5 GESTIÓN DE RIESGOS

Para la propuesta de desarrollar una metodología de gestión de incidentes se hicieron unos análisis en el *capítulo 4 en la sección 4.1.3 Análisis de matriz de riesgos* para identificar sus activos y disminuir el riesgo del Hospital María. Para esto se elaboró una tabla de estrategia, tomando en

cuenta el estado como en este caso, se obtuvieron 2 resultados que impacta: El primero es el estado de nivel crítico y el segundo el estado de nivel medio alta. A continuación, se muestra el plan de desarrollo.

Tabla 14: Tabla de estrategia de los riesgos

ESTRATEGIAS O PLANES PARA DISMINUIR LOS RIESGOS	
NIVEL CRÍTICO	
Computadoras	Aumentar el uso de monitoreos, teniendo también un buen software de detección contra malware
Servidor	Hacer monitoreo continuo, mantenimiento cada 3 o 4 días para verificar el estado de funcionamiento
Base de datos	Hacer copia de seguridad a diario por cada cambio que se hace en el sistema
NIVEL MEDIO ALTA	
Almacenamiento	Hacer copia de seguridad para prevenir el riesgo y verificar el estado actual del almacenamiento
Redes	Mantener un monitoreo en tiempo real para mantener segura la red y creando políticas claras respecto al uso de la red

6.5 MEDIDAS DE CONTROL

Para garantizar la efectividad y sostenibilidad de la propuesta, se propone implementar las siguientes medidas de control:

- Políticas de seguridad aprobadas por la alta dirección.
- Controles de acceso basados en roles.
- Sistemas de respaldo y recuperación periódica de datos.
- Monitoreo en tiempo real de la red hospitalaria.
- Registro y análisis forense de todos los incidentes detectados.
- Indicadores clave de rendimiento (KPI) para evaluar tiempos de respuesta, frecuencia de incidentes y efectividad de la recuperación.

Estas medidas permitirán una gestión proactiva y reactiva de incidentes, alineada con los objetivos de continuidad operativa del hospital.

6.6 CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO

Este plan se estructura en cinco fases secuenciales, cada una con objetivos específicos, áreas clave involucradas y responsables operativos sugeridos. La implementación está pensada para desarrollarse a lo largo de 6 a 12 meses, dependiendo de los recursos disponibles.

Cronograma de implementación (4 meses con 2 semanas – 18 semanas):

Tabla 15: Cronograma de implementación

TAREAS	OBJETIVOS	ACTIVIDADES CLAVES	ÁREAS INVOLUCRADAS	RESPONSABLE SUGERIDO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE
Fase 1: Preparación y Diagnóstico	Evaluar el estado actual de la seguridad informática, sensibilizar a las autoridades y conformar el equipo responsable.	• Revisión de políticas existentes. • Diagnóstico técnico y organizacional. • Reuniones iniciales con las jefaturas.	• Unidad de Tecnologías de la Información. • Dirección Administrativa. • Recursos Humanos.	Jefe del Departamento de TI, con apoyo del Coordinador de Calidad o Gestión Institucional.	2 SEMANAS				
Fase 2: Diseño y Aprobación de la Metodología	Construir formalmente la metodología institucional para la gestión de incidentes.	• Redacción de políticas y procedimientos. • Diseño de flujos operativos, roles y tiempos de respuesta. • Validación interna de la metodología.	• Departamento de TI. • Unidad Legal (para revisión normativa). • Unidad de Calidad. • Dirección General.	Coordinador de Seguridad Informática (o personal con formación en ciberseguridad), junto con un Comité Redactor.		4 SEMANAS			
Fase 3: Capacitación y Concienciación	Capacitar a todo el personal técnico y usuarios clave sobre la nueva metodología.	• Talleres técnicos para el equipo TIC. • Charlas de concienciación para usuarios finales. • Distribución de guías, protocolos y canales de reporte.	• Departamento de TIC. • Recursos Humanos. • Áreas Clínicas y Administrativas. • Comunicación Institucional.	Encargado de Capacitación en TIC, con apoyo del responsable de Recursos Humanos.		3 SEMANAS			
Fase 4: Implementación Técnica y Piloto	Aplicar la metodología en un entorno real controlado (fase piloto), configurando herramientas básicas de monitoreo y recolección de incidentes.	• Instalación de software (IDS, backup, registro de logs). • Simulación de incidentes. • Recolección de retroalimentación.	• Departamento de TIC. • Servicios Clínicos (en caso de piloto en área hospitalaria). • Mantenimiento y soporte técnico.	Administrador de Sistemas o Infraestructura TIC, con asistencia del Encargado de Seguridad Informática.			6 SEMANAS		
Fase 5: Evaluación y Ajustes	Evaluar los resultados de la implementación, realizar ajustes y definir el despliegue completo	• Auditoría interna del piloto. • Revisión del comité de seguridad. • Ajustes al protocolo. • Informe final y planificación de expansión.	• Comité de Seguridad de la Información. • Unidad de Calidad. • Dirección General. • Auditoría Interna (si aplica).	Coordinador del Comité de Seguridad, con acompañamiento del jefe de TI y el responsable de Calidad.				3 SEMANAS	

Nota: *Fechas aplicadas son de carácter ilustrativo*

A continuación, se detalla una estimación de los costos asociados a la ejecución del proyecto. Esta tabla contempla los recursos esenciales para asegurar la calidad, efectividad y sostenibilidad de la implementación. Cabe destacar que estos datos se presentan únicamente como una referencia presupuestaria que podría servir como punto de partida en caso de que la institución desee implementar este proyecto con apoyo externo o de terceros. Es importante aclarar que, en nuestro caso, no se está recibiendo ningún tipo de compensación económica por la elaboración de este trabajo, ya que forma parte del proyecto de graduación de nuestra maestría en Gestión de Tecnologías de la Información con orientación en Ciberseguridad.

Tabla 16: Presupuesto estimado

Escenario 1: Realista (Recomendado)

Este escenario contempla la inversión mínima necesaria para una implementación funcional y sostenible, incluyendo personal calificado, capacitación y herramientas esenciales.

Concepto	Costo estimado (USD)
Contratación de 1 especialista en ciberseguridad por 6 meses	**$4,200**
Capacitación técnica inicial para personal TIC (externa o virtual)	**$800**
Desarrollo de manuales y protocolos internos	**$500**
Licencias básicas (antivirus, monitoreo, backup)	**$1,500**
Implementación de herramienta IDS (open source + configuración técnica)	**$500**
Creación y gestión del Comité de Seguridad	**$300**
Campañas de concienciación (materiales, diseño)	**$200**
Evaluación y seguimiento (auditoría interna)	**$500**
Total estimado	**$8,500**

Esta propuesta considera una implementación profesional y práctica, adaptada al contexto del Hospital María con recursos limitados pero suficientes para garantizar una ejecución efectiva.

Se incluye la contratación de un especialista en ciberseguridad por un período determinado, capacitaciones técnicas para el personal, desarrollo de documentación formal, herramientas esenciales de seguridad (como antivirus, sistemas de respaldo e IDS) y acciones de concienciación interna. También contempla el establecimiento de un Comité de Seguridad y una auditoría interna para asegurar el cumplimiento de la metodología.

Incluye:

- Personal especializado.
- Capacitación técnica.
- Licencias básicas.
- Manuales y protocolos operativos.
- Comité institucional.
- Campañas educativas internas.
- Auditoría de seguimiento.

Ventajas:

- Alto impacto técnico y organizativo.
- Permite implementación inmediata y completa.
- Mayor control y autonomía institucional.

Escenario 2: Bajo costo con apoyo académico (pasantías)

Este escenario contempla la participación de estudiantes de maestría en ciberseguridad

mediante pasantías supervisadas, reduciendo drásticamente el gasto en personal técnico.

Concepto	Costo estimado (USD)
Estudiantes pasantes (2) durante 4 meses (ad honorem o con ayuda simbólica)	**$0 – $400**
Supervisión académica externa (consultoría ocasional)	**$300**
Capacitación interna y acceso a recursos digitales	**$500**
Documentación y elaboración de la metodología	**$300**
Implementación de herramientas gratuitas (Wazuh, OpenVAS, etc.)	**$0**
Concienciación y simulacros (material interno)	**$150**
Comité de seguridad y reuniones mensuales	**$200**
Evaluación final del proceso	**$200**
Total estimado	**$1,650 – $2,050**

Esta propuesta se enfoca en aprovechar el talento de estudiantes de maestría en ciberseguridad o informática a través de pasantías ad honorem o apoyos simbólicos. El trabajo técnico de implementación sería asumido por estos estudiantes bajo supervisión académica externa, reduciendo significativamente los costos. El hospital proveería orientación institucional, espacios de trabajo, acceso a sistemas y apoyo logístico. Es una alternativa viable para comenzar con recursos muy limitados sin perder calidad en la ejecución.

Incluye:

- Pasantes de universidades aliadas.
- Supervisión académica mínima.
- Capacitación básica interna.
- Implementación de herramientas gratuitas.
- Concienciación interna con recursos propios.

- Comité funcional con personal actual.
- Evaluación final del proceso.

Ventajas:

- Costos casi nulos.
- Genera vínculo academia-institución.
- Buen punto de partida para validar la metodología.
- Promueve experiencia práctica para estudiantes.

Escenario 3: Escalable y progresivo (implementación por fases)

Este escenario permite dividir el proceso en fases trimestrales, según disponibilidad presupuestaria institucional. Ideal para gestionar desde el POA del hospital.

Fase	Acciones clave	Costo estimado (USD)
Fase 1 (meses 1-3): Planificación y capacitación	Diagnóstico, plan de acción, primeros talleres	**$2,000**
Fase 2 (meses 4-6): Implementación técnica básica	Configuración de herramientas y elaboración de políticas	**$2,500**
Fase 3 (meses 7-9): Concienciación y pruebas piloto	Simulacros, retroalimentación, revisión de roles	**$1,200**
Fase 4 (meses 10-12): Auditoría interna y ajustes	Evaluación final, mejora de procesos	**$1,300**
Total estimado anual	–	**$7,000**

Este enfoque plantea una implementación dividida en cuatro fases distribuidas a lo largo de un año. Cada fase tiene objetivos concretos y actividades específicas que se van ejecutando según la disponibilidad de recursos. Se inicia con la planificación y formación del personal,

seguido de la implementación técnica mínima, luego se incorporan actividades de concienciación y simulación, y finalmente una etapa de evaluación y ajuste. Esta opción permite adaptar el proceso a presupuestos institucionales anuales o semestrales, sin comprometer la calidad.

Incluye:

- Fase 1: Diagnóstico, planificación y talleres introductorios.
- Fase 2: Instalación de herramientas y redacción de políticas.
- Fase 3: Capacitación extendida, campañas internas y simulacros.
- Fase 4: Evaluación, auditoría interna y mejora de procesos.

Ventajas:

- Flexible y adaptable a recursos variables.
- Facilita seguimiento por etapas.
- Posibilita ajustes según resultados parciales.
- Ideal para entornos con planificación presupuestaria anual.

Consideraciones finales:

1. **El Escenario 1** ofrece un punto de partida realista con impacto inmediato.
2. **El Escenario 2** es ideal si se cuenta con alianzas académicas o universidades dispuestas a colaborar.
3. **El Escenario 3** permite escalar según recursos institucionales disponibles sin descuidar la planificación.

6.7 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

Tabla 17: Concordancia de segmentos de tesis

Capítulo I	Capítulo II	Capítulo III	Capítulo V	Capítulo VI
Título Investigación: Desarrollo de una metodología para la gestión de incidentes en seguridad informática con aplicación de la ISO 27001 y protocolos NIST.	**Teorías/Metodologías de sustento:** NIST Cybersecurity Framework, ISO 27001, ISO 27035, SANS, Resiliencia Organizacional e Informática Forense.	**Variables:** Gestión de incidentes, estándares de seguridad, continuidad operativa, capacitación en seguridad.	**Conclusiones:** Se confirma la necesidad de implementar una metodología para gestionar incidentes, mejorar la respuesta ante amenazas y proteger los datos del hospital.	**Nombre de la propuesta:** Desarrollo de una metodología de gestión de incidentes de seguridad informática para el Hospital María, basada en las normas ISO 27001 e ISO 27035 y los protocolos del NIST.
Objetivo General: Proponer una metodología estandarizada para la gestión de incidentes de seguridad informática en el Hospital María.		**Poblaciones:** Personal técnico y administrativo del área de TI del Hospital María.		**Objetivos de la propuesta:** Implementar una metodología estructurada que incluya diagnóstico, diseño, capacitación, ejecución, control y mejora continua en la gestión de incidentes de seguridad.
Objetivos Específicos: Identificar vulnerabilidades, analizar marcos normativos, evaluar recursos actuales y diseñar una metodología adaptada.		**Técnicas:** Encuestas, entrevistas, análisis documental, matriz de riesgo, cronograma, simulaciones.		

REFERENCIA BIBLIOGRÁFICA

Andino R, R. J. (2022). *dialnet.unirioja.es*. Obtenido de dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=5797266

Ayuso, S. (15 de 01 de 2025). *El Pais*. Obtenido de El Pais: https://elpais.com/sociedad/2025-01-16/bruselas-quiere-crear-un-centro-de-ciberseguridad-paneuropeo-para-proteger-a-hospitales-de-ataques-online.html?

Bromiley, M. (2019). *Google Scholar*. Obtenido de Google Scholar: https://assets.extrahop.com/whitepapers/SANS-2019-Incident-Response-Survey.pdf

Ciberseguridad. (2025). *Ciberseguridad*. Obtenido de Ciberseguridad.com: https://ciberseguridad.com/guias/sanidad/

Ciber-seguridad. (2025). *Ciber-seguridad.blog*. Obtenido de Ciber-seguridad.blog: https://ciber-seguridad.blog/ciberseguridad-en-el-sector-salud

Coll, B. (07 de 11 de 2024). *El Pais*. Obtenido de El Pais: https://elpais.com/espana/catalunya/2024-11-07/la-generalitat-concluye-que-el-clinic-no-tenia-medidas-de-seguridad-minimas-para-contener-el-ciberataque-de-2023.html?

Cybersecurity Ventures. (24 de 06 de 2024). *cybersecurity ventures*. Obtenido de cybersecurityventures.com: https://cybersecurityventures.com/cybersecurity-almanac-2024/

Editora El Sol, S. d. (19 de Abril de 2024). *ProQuest Central*. Obtenido de proquest.com: https://www.proquest.com/newspapers/fortalecer-la-resiliencia-factor-clave/docview/3047830278/se-2?accountid=35325

Ellinger, E. (3 de Julio de 2024). *AXA Venture Partners.* Obtenido de axavp.com: https://www.axavp.com/how-can-software-investors-turn-nist-csf-2-0-updates-into-opportunities-in-cybersecurity-and-risk-management/

ENISA. (05 de 07 de 2023). *ENISA*. Obtenido de ENISA: https://www.enisa.europa.eu/publications/health-threat-landscape

Global Trust Association. (11 de Febrero de 2025). *Global Trust Association*. Obtenido de globaltrustassociation.org: https://globaltrustassociation.org/es/la-relevancia-de-la-ciberseguridad-en-la-era-digital-iso-270322023/

González, J. D. (25 de 01 de 2025). *incibe*. Obtenido de incibe.es: https://www.incibe.es/incibe-cert/blog/ciberseguridad-en-el-sector-salud-caracteristicas-amenazas-y-recomendaciones

Hernández, R. F. (2021). *Metodología de la investigación.* McGraw-Hill (7a ed).

Informatics, H. (07 de 2016). *iso.org*. Obtenido de iso.org: https://www.iso.org/standard/62777.html

ISO/IEC. (2022). *ISO.* Obtenido de iso.org: https://www.iso.org/standard/27001

ISO/IEC 27002. (2022). *ISO/IEC.* Obtenido de iso.org: https://www.iso.org/standard/75652.html

John W. Creswell, J. D. (2022). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* sage publications.

Legapin. (01 de 2025). *Legapin*. Obtenido de Legapin: https://www.legalpin.com/wp-content/uploads/2025/01/para-salud-hospitales-guia-de-ciberseguridad-para-tratamiento-de-datos-personales.pdf

Martínez, P. S. (2022). *Universidad Nacional Autónoma de Honduras*. Obtenido de Universidad Nacional Autónoma de Honduras: https://scholar.google.com/scholar?q=Políticas+ciberseguridad+hospitales+Honduras

Maus, B. (11 de Abril de 2024). *Soluciones de Software OTRS*. Obtenido de OTRS: https://otrs.com/es/otrsmag/gestion-de-incidentes-significado-objetivos-y-proceso/

Medina Astudillo, I. D. (23 de 09 de 2022). *dspace*. Obtenido de dspace: https://dspace.ups.edu.ec/handle/123456789/26727

NIST. (26 de Febrero de 2024). *National Institute of Standards and Technology*. Obtenido de nist.gov:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
Pablo A. Vaca, E. R. (28 de Noviembre de 2024). *Scielo.* Obtenido de scielo.org.co: http://www.scielo.org.co/scielo.php?pid=S0123-77992024000200300&script=sci_arttext
Parrales, H. (23 de Noviembre de 2023). *Aprovados*. Obtenido de aprobados.net: https://aprobados.net/matriz-de-congruencia/
Patton, M. Q. (Noviembre de 2014). *sage*. Obtenido de sagepub.com: Sage Publications https://us.sagepub.com/en-us/cam/qualitative-research-evaluation-methods/book232962
SafetyCulture. (15 de Enero de 2024). *safetyculture*. Obtenido de safetyculture.com: https://safetyculture.com/es/temas/gestion-de-incidentes/
Schwab, K. (2016). *World Economy Forum.* Obtenido de weforum.org: https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab/
Tomé, E. (01 de 2019). *IPANDETEC*. Obtenido de IPANDETEC: https://ipandetec.org/wp-content/uploads/2019/01/EDP_Honduras.pdf
Villar, B. (29 de Noviembre de 2024). *ProQuest Central*. Obtenido de proquest.com: Infobae https://www.proquest.com/newspapers/cómo-funciona-el-software-forense-que-permite/docview/3134441517/se-2?accountid=35325

ANEXOS

ANEXO 1 ENCUESTA

MAESTRÍA EN GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN

DESARROLLO DE UNA METODOLOGÍA PARA LA GESTIÓN DE INCIDENTES EN SEGURIDAD INFORMÁTICA CON APLICACIÓN DE LA ISO 27001 Y PROTOCOLOS NIST

Objetivo:

Recopilar datos para analizar la información y comprobar la seguridad del Hospital maría para así dar un seguimiento al desarrollo de una metodología para la gestión de incidentes en seguridad informática

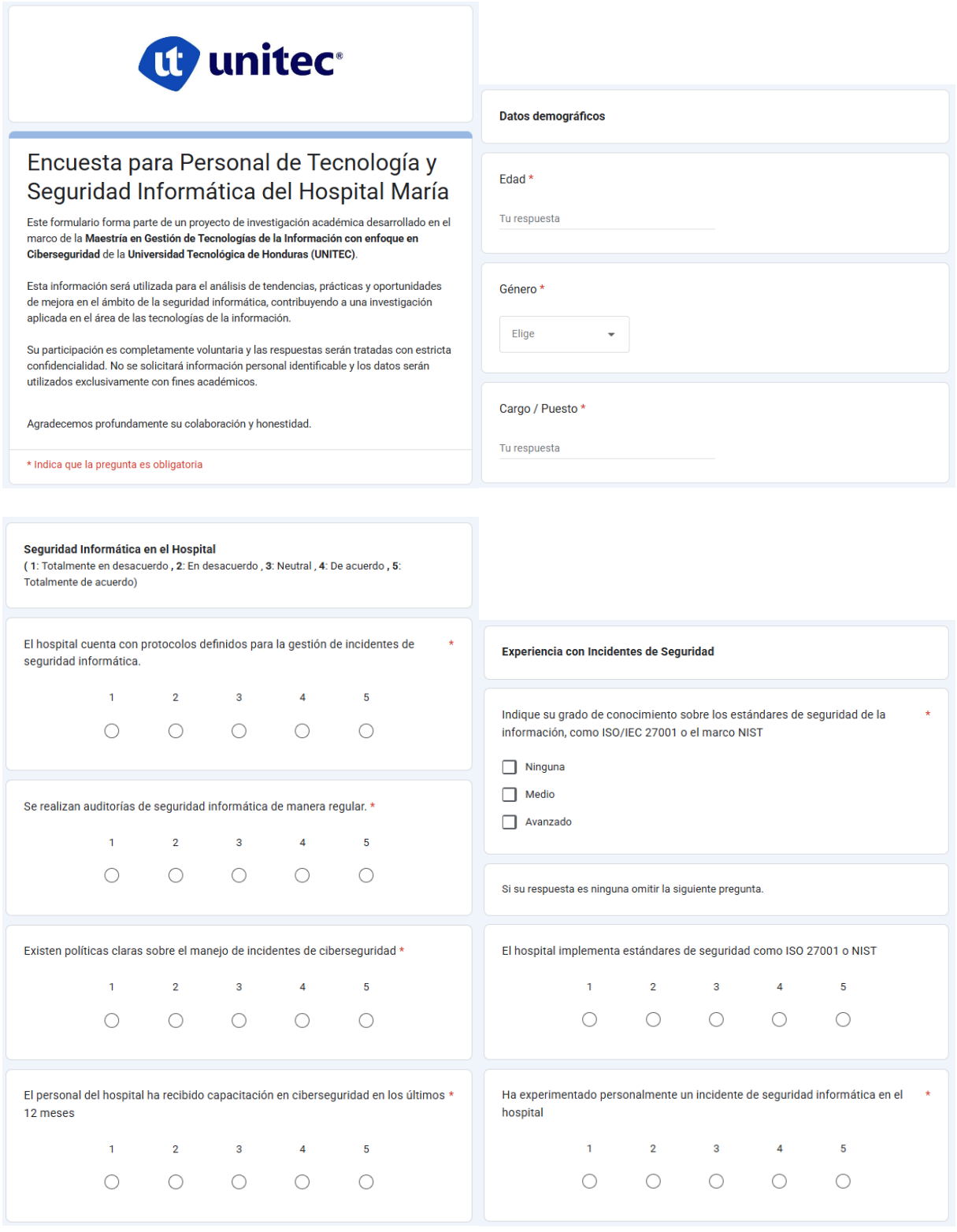
Contexto:

El contexto de esta encuesta es poder evaluar el estado actual de la seguridad informática en el Hospital María y recopilar percepciones del personal relacionado con tecnología y ciberseguridad. El propósito es estar enfocado en identificar áreas de mejora y fortalecer prácticas relacionadas con la gestión de incidentes y la implementación de normas de seguridad internacionalmente reconocidas, como ISO 27001 o NIST.

Confidencialidad:

Toda la información recolectada de la encuesta será privada y solo utilizada por el fin de

ayudar a la empresa a mejorar y resolver el problema solicitado, además los resultados de las encuestas serán anónimos sin identificar que persona lo respondió.



unitec

Encuesta para Personal de Tecnología y Seguridad Informática del Hospital María

Este formulario forma parte de un proyecto de investigación académica desarrollado en el marco de la **Maestría en Gestión de Tecnologías de la Información con enfoque en Ciberseguridad** de la **Universidad Tecnológica de Honduras (UNITEC)**.

Esta información será utilizada para el análisis de tendencias, prácticas y oportunidades de mejora en el ámbito de la seguridad informática, contribuyendo a una investigación aplicada en el área de las tecnologías de la información.

Su participación es completamente voluntaria y las respuestas serán tratadas con estricta confidencialidad. No se solicitará información personal identificable y los datos serán utilizados exclusivamente con fines académicos.

Agradecemos profundamente su colaboración y honestidad.

* Indica que la pregunta es obligatoria

Datos demográficos

Edad *

Tu respuesta

Género *

Elige

Cargo / Puesto *

Tu respuesta

Seguridad Informática en el Hospital
(**1**: Totalmente en desacuerdo , **2**: En desacuerdo , **3**: Neutral , **4**: De acuerdo , **5**: Totalmente de acuerdo)

El hospital cuenta con protocolos definidos para la gestión de incidentes de seguridad informática. *

1 2 3 4 5

Se realizan auditorías de seguridad informática de manera regular. *

1 2 3 4 5

Existen políticas claras sobre el manejo de incidentes de ciberseguridad *

1 2 3 4 5

El personal del hospital ha recibido capacitación en ciberseguridad en los últimos 12 meses *

1 2 3 4 5

Experiencia con Incidentes de Seguridad

Indique su grado de conocimiento sobre los estándares de seguridad de la información, como ISO/IEC 27001 o el marco NIST *

- Ninguna
- Medio
- Avanzado

Si su respuesta es ninguna omitir la siguiente pregunta.

El hospital implementa estándares de seguridad como ISO 27001 o NIST

1 2 3 4 5

Ha experimentado personalmente un incidente de seguridad informática en el hospital *

1 2 3 4 5

Cree que la respuesta del hospital a incidentes de seguridad es eficiente *

1 2 3 4 5

Se documentan y analizan los incidentes de seguridad ocurridos *

1 2 3 4 5

Considera que los incidentes de seguridad han afectado la continuidad de los servicios médicos *

1 2 3 4 5

Se cuenta con un equipo especializado para la gestión de incidentes *

1 2 3 4 5

Percepción sobre la Implementación de una Metodología de Gestión de Incidentes

Cree que la implementación de una metodología basada en ISO 27001/NIST mejoraría la respuesta ante incidentes *

1 2 3 4 5

Considera que la administración del hospital está comprometida con la seguridad informática *

1 2 3 4 5

Se asignan suficientes recursos para mejorar la ciberseguridad en el hospital *

1 2 3 4 5

Dimensión: Comportamiento y cultura organizacional
Evalúa la actitud del personal hacia la seguridad informática:

Sigo las políticas de seguridad informática en todas mis actividades laborales. *

1 2 3 4 5

Informo cualquier incidente de seguridad al área correspondiente. *

1 2 3 4 5

La cultura del hospital fomenta el reporte de incidentes sin temor a represalias. *

1 2 3 4 5

Las herramientas tecnológicas que uso en el hospital son seguras y confiables. *

1 2 3 4 5

Los sistemas del hospital cuentan con autenticación adecuada. *

1 2 3 4 5

He recibido capacitación suficiente para identificar amenazas comunes como phishing. *

1 2 3 4 5

Me siento preparado para actuar ante un incidente de seguridad informática. *

1 2 3 4 5

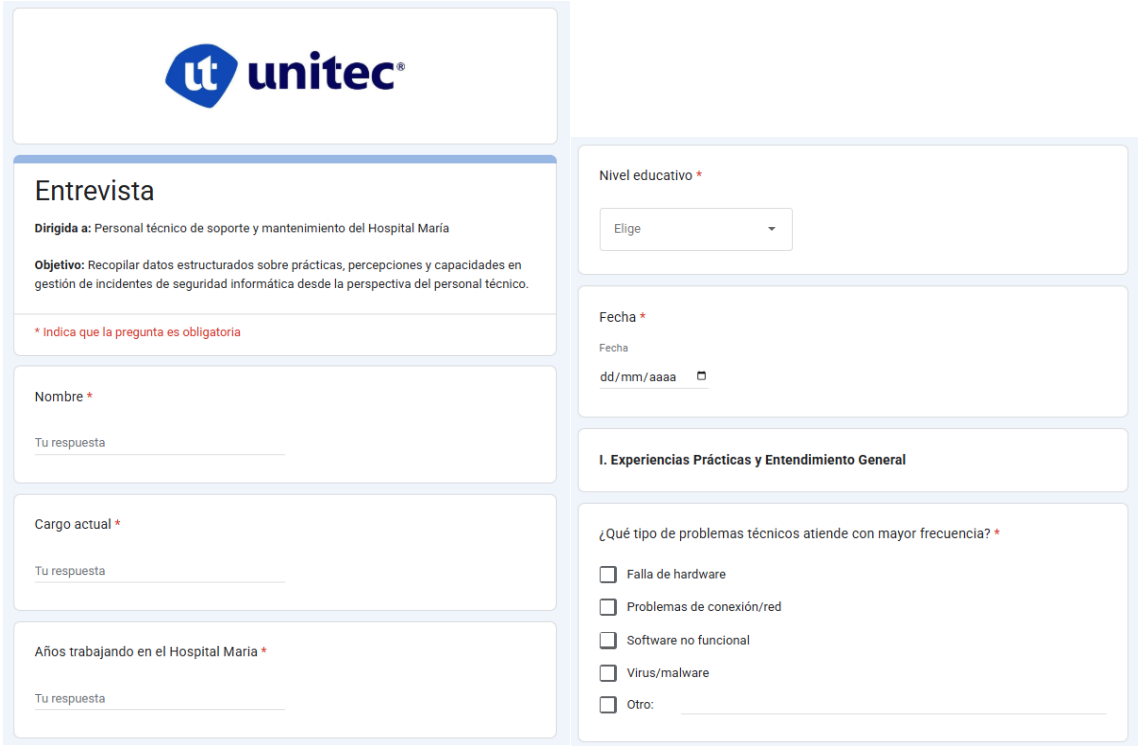
ANEXO 2 ENTREVISTA

Objetivo:

Recopilar datos estructurados sobre prácticas, percepciones y capacidades en gestión de incidentes de seguridad informática desde la perspectiva del personal técnico.

Confidencialidad:

Toda la información recolectada de la entrevista será privada y solo utilizada por el fin de ayudar a la empresa a mejorar y resolver el problema solicitado, además los resultados de las encuestas serán anónimos sin identificar que persona lo respondió.



unitec

Entrevista

Dirigida a: Personal técnico de soporte y mantenimiento del Hospital María

Objetivo: Recopilar datos estructurados sobre prácticas, percepciones y capacidades en gestión de incidentes de seguridad informática desde la perspectiva del personal técnico.

* Indica que la pregunta es obligatoria

Nombre *

Tu respuesta

Cargo actual *

Tu respuesta

Años trabajando en el Hospital Maria *

Tu respuesta

Nivel educativo *

Elige

Fecha *

Fecha

dd/mm/aaaa

I. Experiencias Prácticas y Entendimiento General

¿Qué tipo de problemas técnicos atiende con mayor frecuencia? *

- Falla de hardware
- Problemas de conexión/red
- Software no funcional
- Virus/malware
- Otro:

¿Alguna vez ha atendido un problema relacionado con virus, pérdida de información o acceso no autorizado? *

- ◯ Si
- ◯ No
- ◯ No estoy seguro

¿Cómo identifica si un problema técnico puede estar relacionado con seguridad informática? *

- ☐ Solo si aparece un mensaje de alerta
- ☐ Si el usuario me lo indica
- ☐ Por comportamiento anómalo del sistema
- ☐ No sé cómo identificarlo

II. Procedimientos y Recursos

Cuando ocurre un problema técnico, ¿qué procedimiento sigue? *

- ☐ Verifica el equipo y soluciona directamente
- ☐ Reporta a un supervisor
- ☐ Registra el incidente
- ☐ No hay un procedimiento definido

¿Existe un protocolo para casos que parecen graves o sospechosos? *

- ☐ Sí, por escrito
- ☐ Sí, pero no está documentado
- ☐ No
- ☐ No lo sé

¿Con qué herramientas cuenta para atender fallas o incidentes? *

- ☐ Antivirus/licencias
- ☐ Sistema de tickets
- ☐ Manuales de soporte
- ☐ Solo experiencia personal
- ☐ Ninguna de las anteriores

III. Percepción y Cultura de Seguridad
(Escala de Likert de 1 a 5, donde 1 = Totalmente en desacuerdo y 5 = Totalmente de acuerdo)

La seguridad informática es importante en mi trabajo diario. *

	1	2	3	4	5	
Totalmente en desacuerdo	◯	◯	◯	◯	◯	Totalmente de acuerdo

Me siento capacitado para identificar y actuar ante un posible incidente de seguridad. *

	1	2	3	4	5	
Totalmente en desacuerdo	◯	◯	◯	◯	◯	Totalmente de acuerdo

Los usuarios cometen errores que afectan el funcionamiento seguro de los equipos. *

	1	2	3	4	5	
Totalmente en desacuerdo	◯	◯	◯	◯	◯	Totalmente de acuerdo

IV. Limitaciones y Necesidades

¿Qué dificultades enfrenta al atender incidentes que podrían ser de seguridad? *

- ☐ Falta de herramientas adecuadas
- ☐ No hay un procedimiento claro
- ☐ No sé cómo actuar
- ☐ No contar con un escalamiento de soporte para revisión del incidente
- ☐ Ninguna de las anteriores
- ☐ Otro: _____

¿Cree que debería recibir formación básica en gestión de incidentes informáticos? *

- ☐ Sí
- ☐ No
- ☐ No lo sé

¿Qué necesitaría para manejar mejor este tipo de situaciones? *

- ☐ Manual o guía de pasos a seguir
- ☐ Capacitaciones cortas
- ☐ Software de detección
- ☐ Más personal de apoyo
- ☐ Otro: _____

V. Sugerencias y Recomendaciones

¿Qué sugerencia haría para mejorar el manejo de problemas técnicos relacionados con seguridad informática? *

- [ ] Crear procedimientos claros
- [ ] Asignar roles específicos
- [ ] Capacitar al personal técnico
- [ ] No tengo sugerencias

¿Cree que un procedimiento paso a paso le ayudaría a actuar en casos sospechosos? *

- [ ] Sí, sería muy útil
- [ ] Tal vez
- [ ] No

¿De qué forma podría usted contribuir a mejorar la seguridad de los datos del hospital? *

- [ ] Reportando incidentes
- [ ] Siguiendo políticas claras
- [ ] Informando a los usuarios
- [ ] No estoy seguro

MAESTRÍA EN GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN

DESARROLLO DE UNA METODOLOGÍA PARA LA GESTIÓN DE INCIDENTES EN SEGURIDAD INFORMÁTICA CON APLICACIÓN DE LA ISO 27001 Y PROTOCOLOS NIST

Objetivo:

Construir una base sólida para diseñar un plan más estructurado y eficaz en la gestión de incidentes en seguridad informática.

Contexto:

Este enfoque está orientado a desarrollar políticas y estrategias que garanticen la protección de la información sensible, la continuidad de los servicios médicos y el cumplimiento de normas internacionales. Es una base para crear un entorno más seguro y resiliente.

Confidencialidad:

Toda la información recolectada de la encuesta será privada y solo utilizada por el fin de ayudar a la empresa a mejorar y resolver el problema solicitado, además los resultados de las encuestas serán anónimos sin identificar que persona lo respondió.

Detalle e Información:

Guía de preguntas para entrevistas semiestructuradas con expertos en seguridad informática.

1. ¿Cómo describiría la situación actual de la seguridad informática en el hospital?

2. ¿Cuáles son las principales amenazas o vulnerabilidades que enfrenta el hospital en términos de ciberseguridad?
3. ¿Podría describir un incidente de seguridad reciente y cómo fue manejado?
4. ¿Qué estrategias considera que podrían mejorar la gestión de incidentes de seguridad en el hospital?
5. ¿Qué tan familiarizado está el personal con estándares como ISO 27001 y NIST?
6. ¿Cree que la falta de capacitación es un factor crítico en la ocurrencia de incidentes?
7. ¿Cuáles son las principales dificultades para implementar un plan estructurado de respuesta a incidentes?
8. ¿Cómo se podría mejorar la colaboración entre el equipo de TI y el personal administrativo en temas de seguridad?

Lista de Verificación para Evaluación del Cumplimiento de Normativas

¿El hospital cuenta con un equipo de respuesta a incidentes de seguridad informática?

¿Existen procedimientos documentados para la gestión de incidentes?

¿Se han implementado controles de acceso y autenticación?

¿Se llevan registros de intentos de acceso no autorizado?

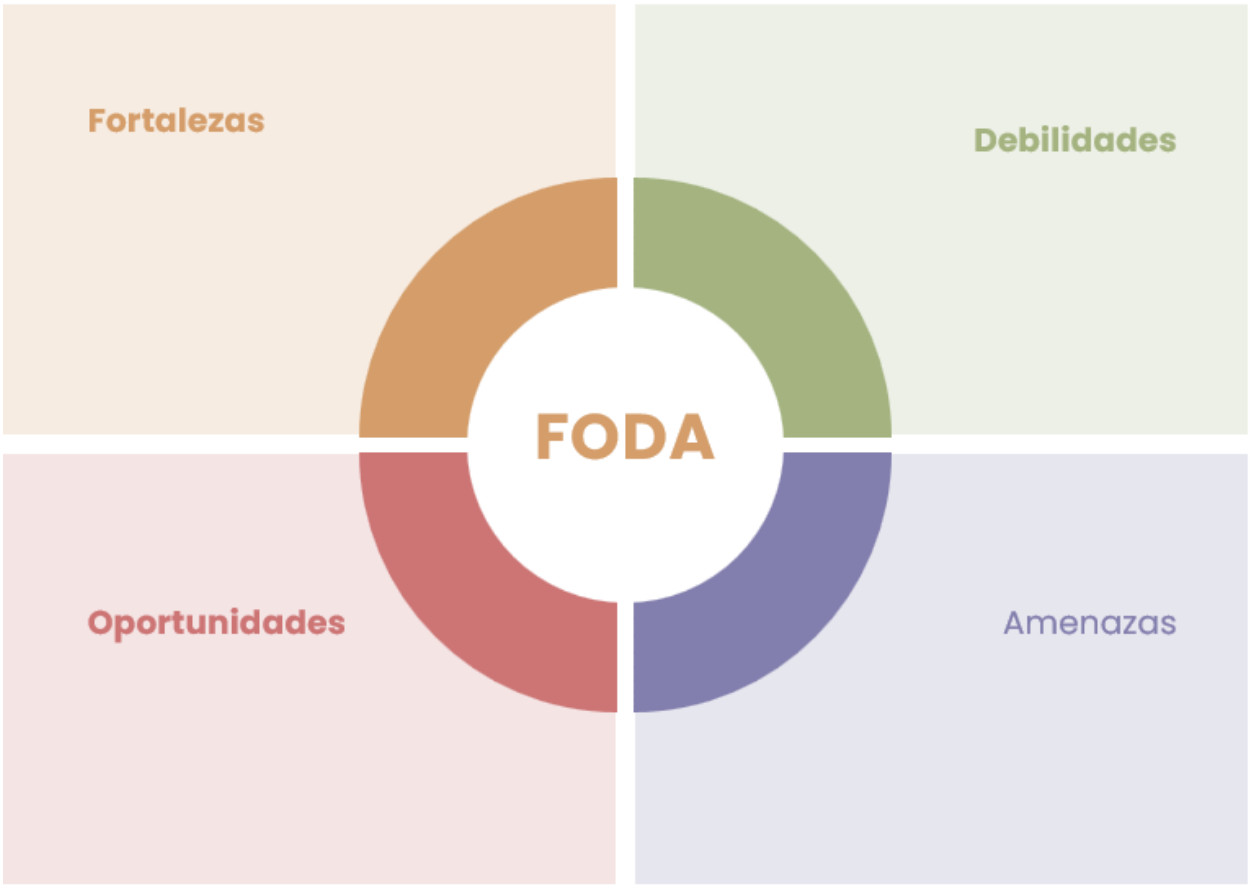
¿Se realizan pruebas de penetración o auditorías de seguridad?

¿Se aplica cifrado en el almacenamiento y transmisión de datos sensibles?

¿Existen planes de continuidad operativa en caso de ciberataques?

¿El personal ha recibido capacitación en protocolos de seguridad informática?

ANEXO 2 FODA



ANEXO 3 MATRIZ DE RIESGO

		Departamento u Área a analizar		
Matriz de Analisis de Riesgo		**P**		
Elemento de Información	**I**	**Amenaza 1**	**Amenaza 2**	**Amenaza 3**
Activos				
		0	0	0
		0	0	0
		0	0	0
		0	0	0
		0	0	0
		0	0	0

			Impacto			
			1	2	3	4
			Bajo	**Medio**	**Alto**	**Muy Alto**
Probabilidad	1	**Baja**	1	2	3	4
	2	**Media**	2	4	6	8
	3	**Alta**	3	6	9	12
	4	**Muy Alta**	4	8	12	16

Impacto	1 a 3	Bajo
	4 a 6	Media
	7 a 9	Alta
	12 a 16	Muy Alta

RT(Riesgo total) = Probabilidad x Impacto Promedio
I = Impacto
P= Probabilidad

Estrategia o plan para disminuir los riesgos	

ANEXO 4 PLAN DE RESPUESTA A INCIDENTES (PRI) DEL HOSPITAL MARÍA

1. Introducción

El presente Plan de Respuesta a Incidentes (PRI) establece un marco de actuación ante eventos que comprometan la seguridad de la información en el Hospital María. Tiene como objetivo minimizar el impacto de los incidentes, asegurar la continuidad operativa de los servicios médicos y proteger la confidencialidad, integridad y disponibilidad de los datos clínicos y administrativos.

2. Objetivos del PRI

- Detectar y responder eficazmente a los incidentes de seguridad informática.
- Contener y erradicar las amenazas identificadas.
- Recuperar los sistemas afectados de forma segura y oportuna.
- Aprender de cada incidente para prevenir su recurrencia.
- Cumplir con las normativas nacionales e internacionales en seguridad de la información.

3. Alcance

Este plan se aplica a todos los activos tecnológicos del Hospital María: servidores, estaciones de trabajo, redes, sistemas de gestión hospitalaria (HIS), bases de datos clínicas, correos electrónicos, dispositivos móviles y usuarios internos con acceso a sistemas de información.

4. Definiciones

- Incidente de seguridad informática: Evento que compromete la seguridad de la información o los sistemas tecnológicos.
- Equipo de Respuesta ante Incidentes (ERI): Grupo multidisciplinario encargado de ejecutar el PRI.
- Evento: Cualquier anomalía observable que podría constituir un incidente.

5. Clasificación de Incidentes

Categoría	Descripción	Ejemplo	Nivel de respuesta
Crítico	Impacto inmediato en servicios médicos y pérdida de datos	Ransomware, filtración masiva	Respuesta inmediata, activación total del ERI
Moderado	Impacto limitado en sistemas secundarios	Malware, acceso no autorizado	Evaluación, contención rápida
Bajo	Incidentes sin consecuencias evidentes	Intento fallido de acceso	Seguimiento y documentación

6. Fases del PRI

6.1. Preparación

- Identificación de activos y responsables.
- Implementación de políticas de seguridad y herramientas de monitoreo.
- Capacitación continua al personal técnico y administrativo.

6.2. Identificación

- Monitoreo en tiempo real de sistemas.
- Verificación de alertas por parte del personal de seguridad.

- Registro del incidente en la bitácora digital.

6.3. Contención

- Contención inmediata en caso de amenaza crítica (aislamiento del equipo, bloqueo de usuarios).
- Evaluación del alcance del incidente.
- Notificación al Comité de Seguridad y Dirección General.

6.4. Erradicación

- Eliminación del software malicioso.
- Revisión de configuraciones de seguridad.
- Análisis de logs y rastreo de vectores de ataque.

6.5. Recuperación

- Restauración de sistemas afectados desde respaldos seguros.
- Verificación de la integridad de los datos.
- Reincorporación controlada a la red institucional.

6.6. Lecciones aprendidas

- Elaboración del Informe de Incidente.
- Reunión de evaluación con el ERI.
- Actualización de controles y capacitación del personal.

7. Roles y Responsabilidades

Rol	Función
Coordinador de Respuesta	Dirigir las acciones del ERI y comunicar con la dirección.
Analista de Seguridad	Identificar y evaluar el incidente.
Técnico de TI	Aplicar acciones de contención, erradicación y recuperación.
Responsable Legal	Evaluar implicaciones jurídicas y redactar comunicaciones externas.
Comunicador Interno	Informar a las áreas afectadas y usuarios clave.

8. Canales de Notificación

- Correo electrónico oficial de incidentes: incidentes@hospitalmaria.hn
- Línea directa interna: Ext. 119 – Seguridad TI
- Formulario web: Intranet > Seguridad Informática > Reporte de Incidente

9. Indicadores de seguimiento

- Tiempo promedio de detección del incidente.
- Tiempo promedio de respuesta.
- Número de incidentes por tipo.
- Porcentaje de recuperación dentro del SLA.
- Número de eventos recurrentes mitigados tras lecciones aprendidas.

10. Revisión del PRI

Este plan será revisado semestralmente o tras un incidente crítico. Las actualizaciones serán aprobadas por el Comité de Seguridad de la Información.

ANEXO 5 MANUAL DE FUNCIONES PARA CADA MIEMBRO DEL ERI.

1. Introducción

El Equipo de Respuesta a Incidentes (ERI) es el cuerpo operativo responsable de gestionar, contener y resolver eventos de seguridad informática que amenacen los activos tecnológicos y la información institucional del Hospital María. Este manual define de forma precisa los roles, funciones y responsabilidades de cada miembro del equipo.

2. Objetivo

Establecer de forma clara las funciones operativas, técnicas y administrativas que deberá cumplir cada miembro del ERI para asegurar una gestión efectiva, oportuna y profesional de los incidentes de seguridad informática.

3. Composición del ERI

El ERI está conformado por personal técnico y administrativo con roles definidos, y puede ampliarse temporalmente según el tipo o gravedad del incidente.

4. Funciones por rol

4.1. Coordinador General del ERI

Cargo recomendado: jefe de Tecnología o Responsable de Seguridad Informática

Funciones:

- Activar oficialmente el equipo ante la notificación de un incidente.
- Dirigir estratégicamente la gestión del incidente en todas sus fases.
- Comunicar el estado del incidente a la Dirección General.
- Garantizar el cumplimiento del PRI y los protocolos establecidos.
- Aprobar el cierre del incidente y la emisión del informe final.
- Coordinar la revisión del PRI y las lecciones aprendidas.

4.2. Analista de Seguridad Informática

Cargo recomendado: Especialista en ciberseguridad o auditor de sistemas

Funciones:

- Validar la naturaleza del evento y confirmar si se trata de un incidente real.
- Clasificar el incidente según su gravedad y tipo.
- Realizar análisis forense de los sistemas afectados.
- Identificar vectores de ataque, origen y causa raíz.
- Recomendar medidas de mitigación y evitar recurrencias.
- Generar reportes técnicos para documentación interna.

4.3. Técnico de Soporte y Recuperación

Cargo recomendado: Técnico de redes/sistemas

Funciones:

- Ejecutar acciones inmediatas de contención (aislamiento de equipos, bloqueo de

usuarios o accesos).

- Aplicar soluciones de erradicación (desinfección, reinstalación, reconfiguración).
- Restaurar servicios a partir de respaldos seguros y validarlos con usuarios.
- Verificar la funcionalidad del sistema tras la recuperación.
- Documentar procedimientos técnicos aplicados durante la intervención.

4.4. Responsable de Documentación y Seguimiento

Cargo recomendado: Asistente técnico o administrativo en TI

Funciones:

- Registrar todos los detalles del incidente en la bitácora oficial.
- Completar y mantener actualizados los formularios de eventos de seguridad.
- Elaborar actas de reunión del ERI y cronogramas de respuesta.
- Apoyar en la redacción del informe final del incidente.
- Archivar evidencias digitales de forma segura y trazable.

4.5. Enlace de Comunicación Interna

Cargo recomendado: Encargado de comunicación institucional o administrativo de TI

Funciones:

- Redactar y emitir comunicados internos sobre incidentes, medidas preventivas o acciones tomadas.
- Canalizar información con las áreas afectadas (clínica, administración, dirección).

- Evitar rumores y mantener la claridad de la información oficial.
- Participar en campañas de concientización en ciberseguridad.

4.6. Asesor Legal (cuando aplique)

Cargo recomendado: Representante legal del hospital

Funciones:

- Evaluar implicaciones legales del incidente (ej. fuga de datos, uso indebido).
- Asesorar sobre comunicaciones externas o denuncias.
- Redactar notificaciones a entes reguladores si corresponde.
- Revisar políticas internas frente a riesgos legales identificados.

5. Principios operativos del ERI

- Confidencialidad: Todo incidente debe manejarse bajo reserva hasta su resolución.
- Trazabilidad: Cada acción debe ser registrada y auditada.
- Escalabilidad: El equipo puede adaptarse según la magnitud del incidente.
- Colaboración: Todas las funciones están interrelacionadas; el trabajo en equipo es esencial.

6. Capacitación y revisión de funciones

Los miembros del ERI deberán recibir capacitación semestral en gestión de incidentes, normativa ISO/NIST, análisis forense y uso de herramientas de respuesta. Las funciones asignadas deben revisarse anualmente y ajustarse en función de la evolución tecnológica del hospital.

ANEXO 6 MANUAL DE RESPUESTA RÁPIDA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA

1. Objetivo

Brindar una guía rápida, clara y accionable para el personal técnico del Hospital María ante la detección o sospecha de un incidente de seguridad informática, con el fin de mitigar su impacto, preservar evidencia y garantizar la continuidad operativa.

2. Alcance

Aplica a todos los sistemas, usuarios y equipos conectados a la red institucional del Hospital María. Es de uso obligatorio para todo el personal del Departamento de Tecnología de la Información y miembros del Equipo de Respuesta a Incidentes (ERI).

3. Procedimiento general de respuesta rápida

IMPORTANTE: Ante cualquier sospecha de incidente, NO reiniciar el equipo ni modificar archivos o configuraciones.

Paso 1: Identificación inicial

Verifica si el evento es real (pantalla de bloqueo, alertas del antivirus, comportamiento inusual del sistema, archivos cifrados, accesos no autorizados).

Documenta:

- Fecha y hora
- Usuario afectado
- Equipo o sistema comprometido

- Descripción breve del evento

Paso 2: Aislamiento inmediato

- Desconecta el equipo afectado de la red (Wi-Fi y cable Ethernet).
- No apagues el equipo, salvo que esté causando propagación masiva.
- Informa de inmediato al Coordinador del ERI o al Jefe de TI.

Paso 3: Activación del ERI

El Coordinador ERI evaluará si debe activarse la respuesta formal al incidente.

Se clasificará el incidente según su nivel de criticidad:

Tabla 18: Clasificación de incidente

Nivel	Ejemplo	Acción inmediata
Crítico	Ransomware, fuga de datos	Activación total del ERI
Moderado	Malware, accesos no autorizados	Contención por técnico + validación ERI
Bajo	Phishing, software desactualizado	Registro y seguimiento

Paso 4: Contención

- Cambiar contraseñas de usuarios comprometidos (si aplica).
- Bloquear cuentas sospechosas en el sistema de autenticación.
- Detener procesos o servicios maliciosos.

Paso 5: Preservación de evidencia

- No borrar archivos, logs, correos ni registros.
- Crear una copia forense si es posible.

- Registrar todo en la Bitácora de Incidentes.

Paso 6: Comunicación

- Informar al área afectada con lenguaje claro (sin detalles técnicos innecesarios).
- No divulgar el incidente fuera del personal autorizado.

4. Herramientas de apoyo

Tabla 19: Herramientas de apoyo

Herramienta	Uso
Antivirus corporativo	Escaneo y cuarentena
SIEM institucional	Revisión de logs y correlación de eventos
Consola de administración de red	Bloqueo de puertos/IP
Plantilla de bitácora	Registro cronológico del evento
Checklists impresos	Verificación de pasos realizados

5. Lista de verificación de acciones rápidas (Checklist)

- Verificar síntomas de incidente
- Aislar equipo afectado
- Notificar al Coordinador ERI
- Registrar fecha, hora y usuario
- Cambiar credenciales comprometidas
- Conservar evidencia
- Evitar la propagación

- Iniciar bitácora del incidente
- Informar a usuarios afectados
- Documentar cada acción

6. Contactos clave (internos)

Tabla 20: Contactos clave

Función	Nombre / Cargo	Extensión / Correo
Coordinador ERI	Ing. [Nombre]	Ext. 301 / ciberseguridad@hospitalmaria.hn
Técnico de soporte	[Nombre]	Ext. 215
Responsable Legal	Lic. [Nombre]	Ext. 120

7. Revisión del manual

Este manual será revisado cada 6 meses o después de cualquier incidente severo, y debe mantenerse accesible tanto en versión física (área de TI) como digital (intranet interna).

8. Anexos

ANEXO A: Plantilla rápida de Bitácora de Incidente

Plantilla Rápida de Bitácora de Incidente Hospital María – Unidad de Tecnología de la Información

1. Datos Generales del Incidente

Tabla 21: Datos generales del incidente

Campo	Descripción
Código de Incidente	(Ej. INC-2025-001)

Fecha y Hora de Detección	
Detectado por	(Nombre y cargo)
Medio de detección	(Sistema SIEM, usuario, antivirus, correo, otro)
Ubicación/Área afectada	(Ej. Unidad de Imagenología, Laboratorio, Administración)

2. Descripción del Incidente

Tabla 22: Descripción del incidente

Campo	Detalle
Tipo de incidente	(Malware, phishing, fuga de datos, acceso no autorizado, etc.)
Descripción del evento	(¿Qué ocurrió? ¿Qué sistemas se vieron afectados?)
Sistemas o activos comprometidos	(Ej. HIS, correo electrónico, red local, equipo X)
Usuario(s) afectado(s)	

3. Clasificación del Incidente

Tabla 23: Clasificación del incidente

Nivel	Marcar con ✓
Crítico (afecta servicios esenciales / datos clínicos)	
Moderado (impacto limitado / acceso no autorizado)	
Bajo (intento sin afectación / phishing bloqueado)	

4. Acciones Realizadas

Tabla 24: Acciones a Realizar

Hora	Acción realizada	Responsable
	Aislamiento del equipo	
	Cambio de contraseñas	
	Bloqueo de IP o usuario	
	Eliminación de amenaza	

	Restauración desde respaldo	
	Comunicación al área afectada	
	Informe a dirección	

5. Evidencia Preservada

Tabla 25: Evidencia preservada

Tipo de evidencia	Descripción / Ubicación	Responsable
Capturas de pantalla		
Archivos de logs		
Muestras de malware		
Reportes automáticos (SIEM/AV)		

6. Conclusiones del Incidente

Causa raíz identificada:

Sistemas restaurados:

Usuarios notificados:

Tiempo total de resolución:

Medidas preventivas implementadas:

7. Cierre del Incidente

Tabla 26: Cierre del incidente

Campo	Información
Fecha y hora de cierre	
Validado por (Coordinador ERI)	Nombre y firma
Revisión pendiente de mejoras (Sí / No)	

ANEXO B: Flujograma de respuesta ante incidentes

Flujograma de Respuesta ante Incidentes de Seguridad Informática – Hospital María

Etapas del Flujo:

- **Detección del Incidente**

  Se identifica un evento anómalo mediante monitoreo, alerta automática o reporte manual.

- **Reporte y Registro Inicial**

  Se documenta el evento en la bitácora. Se asigna un código único.

- **Clasificación del Incidente**

  Se evalúa el nivel de impacto (Crítico, Moderado, Bajo) para decidir la prioridad.

- **Acciones de Contención**

  Se aísla el sistema afectado para evitar propagación del daño.

- **Notificación al ERI**

  El Equipo de Respuesta a Incidentes es informado para activar protocolos formales.

- **Análisis y Preservación de Evidencia**

  Se identifican vectores, se recopila evidencia digital y se determina la causa raíz.

- **Erradicación**

  Se elimina la amenaza y se corrigen las vulnerabilidades detectadas.

- **Recuperación**

  Se restauran sistemas desde respaldos seguros. Se valida su funcionalidad.

Lecciones Aprendidas / Informe Final

Se elabora el informe técnico. Se actualizan políticas y se brinda retroalimentación al equipo.