Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Maestría en Telecomunicaciones

Propuesta de Modelo de gestión de seguridad de la información para el Hospital General Manuel Ygnacio Monteros IESS-LOJA, basado en la norma ISO 27799:2008

Trabajo de Titulación previa a la obtención del título de Magíster en Telecomunicaciones

AUTOR:

Ing. Cristian Vinicio Palacios Andrade

DIRECTOR:

Ing. Kleber Rolando Morillo Aguilar, Mg. Sc.

Loja – Ecuador

2023

Certificación

Loja, 26 de junio de 2023

Ing. Kleber Rolando Morillo Aguilar M.Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Propuesta de Modelo de gestión de seguridad de la información para el Hospital General Manuel Ygnacio Monteros IESS-LOJA, basado en la norma ISO 27799:2008,** de autoría del estudiante **Cristian Vinicio Palacios Andrade,** con cédula de identidad **1104751357**, previa a la obtención del título de **Magíster en Telecomunicaciones**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Firmado electrónicamente por:
KLEBER ROLANDO MORILLO AGUILAR

Ing. Kleber Rolando Morillo Aguilar M.Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

Autoría

Yo, **Cristian Vinicio Palacios Andrade**, declaro ser autor del Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación del Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma:

Autor: Cristian Vinicio Palacios Andrade.

Cédula de Identidad: 1104751357

Fecha: 19/06/2023

Correo electrónico: cristian.v.palacios@unl.edu.ec

Teléfono: 0989925792

Carta de autorización por parte del autor para la consulta, reproducción parcial o total y/o publicación electrónica de texto completo del Trabajo de Titulación.

Yo, **Cristian Vinicio Palacios Andrade**, declaro ser autor del Trabajo de Titulación denominado: **Propuesta de Modelo de gestión de seguridad de la información para el Hospital General Manuel Ygnacio Monteros IESS-LOJA, basado en la norma ISO 27799:2008**, como requisito para optar el título de **Magíster en Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del trabajo de investigación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los veintiséis días del mes de junio de dos mil veintitrés.

Firmado electrónicamente por:
CRISTIAN VINICIO PALACIOS ANDRADE

Firma:

Autor: Cristian Vinicio Palacios Andrade
Cédula: 1104751357
Dirección: Sauces Norte
Correo Electrónico: cristian.v.palacios@unl.edu.ec
Teléfono: 0989925792

DATOS COMPLEMENTARIOS:

DIRECTOR DE TRABAJO DE TITULACIÓN: Ing. Kleber Morillo Aguilar M.Sc.

Dedicatoria

A mis padres, quienes han sido mi guía y ejemplo a seguir, les agradezco de corazón por su sacrificio, esfuerzo y dedicación para brindarme una educación sólida y todas las oportunidades posibles. Su aliento y constante respaldo me han dado la fuerza y la confianza necesaria para superar cualquier obstáculo en mi camino. Esta dedicación es un tributo a su inquebrantable fe en mí y a su inagotable generosidad.

A mis hermanos, quienes han sido una fuente de fortaleza y consuelo en los momentos de mayor desafío. Su confianza en mis capacidades y sus palabras de aliento me han impulsado a dar lo mejor de mí en cada paso del camino.

Cristian Vinicio Palacios Andrade.

Agradecimiento

A mi familia, quienes han sido mi mayor fuente de inspiración y fortaleza, les agradezco desde lo más profundo de mi corazón por su constante aliento y amor incondicional. Gracias por creer en mis capacidades y por ser mi soporte emocional durante este arduo camino. Su paciencia, comprensión y sacrificio han sido fundamentales para que hoy pueda culminar esta etapa.

Al director del Trabajo de Titulación, quiero expresar mi más profundo agradecimiento por su sabiduría, dedicación y orientación durante todo el proceso de desarrollo de este Trabajo de Titulación. Agradezco su disposición, su crítica constructiva y su constante estímulo para explorar nuevos caminos de investigación. Su asesoría ha sido fundamental para mi crecimiento académico y profesional.

Cristian Vinicio Palacios Andrade.

Índice de contenidos

Índice de Tablas:

Índice de Figuras:

Índice de Anexos:

1. Titulo

Propuesta de Modelo de gestión de seguridad de la información para el Hospital General Manuel Ygnacio Monteros IESS-LOJA, basado en la norma ISO 27799:2008

2. Resumen

La incorporación de las tecnologías de la información en el ámbito de la salud ha propiciado una mejora significativa para la gestión y administración de la información de los pacientes, no obstante, la falta de conocimiento sobre las políticas de seguridad de la información, ha ocasionado que la información se vea vulnerada a causa de los errores, incidentes y descuido del personal en el manejo y acceso a los registros médicos electrónicos de los pacientes. La presente investigación tuvo como objetivo desarrollar una propuesta de Modelo de Gestión de Seguridad de la Información para el Hospital General Manuel Ygnacio Monteros IESS-LOJA basado en la norma ISO 27799:2008, para ello en la metodología se realizó un análisis de la situación actual del área de TI del HGMYM a través de la investigación cualitativa, observación participativa e investigación documental, además, se realizó un análisis de gestión de riesgos sobre los activos de información del área, para identificar el tratamiento de los riesgos y gestión de políticas de seguridad. Se obtiene como resultado un modelo de SGSI basado en una serie de directrices y actividades dirigidas a salvaguardar la información de los pacientes ante cualquier amenaza que se presente, preservando la disponibilidad, integridad y confidencialidad de la información que ahí se maneja y que sirve como una herramienta de control para garantizar la protección de la información. La propuesta de modelo de SGSI sirve como base para fortalecer la seguridad de la información en el HGMYM y cumplir con los estándares internacionales establecidos en la norma ISO 27799:2008

Palabras clave: *Normas ISO, SGSI, política de seguridad, confidencialidad de la información, gestión de riesgos.*

2.1. Abstract

Health Information Technology has caused a meaningful improvement for the management and administration of patients' data. However, the lack of knowledge about the data protection policy has provoked that the data turns vulnerable due to errors, incidents and staff neglect on the running and access of the patients' electronic medical records.

The present research objective was to develop a proposal of Data Security Management Model for the Manuel Ygnacio Monteros General Hospital IESS-LOJA based on the ISO 27799:2008 norm. Therefore, during the research methodology, there was an analysis of the current situation of the TI area of the MYMGH throughout the qualitative research, participant observation and documentary research. Moreover, there was an analysis of risk management about the information assets of the area in order to identify the risks and management treatment of security policies.

Finally, the result was a SGSI model based on a series of guidelines and activities conducted to protect the patients' data against any threat; preserving its availability, integrity and privacy of the data which is used as a control tool to secure the data. The proposal of the SGSI model works as basis to strength the data security in the MYMGH and to accomplish the international standards set on the ISO 27799:2008 norms.

Key words: *ISO Norms, SGSI, Security Policy, Data Privacy, risk management.*

3. Introducción

La seguridad de la información es esencial en diversos ámbitos y sectores para garantizar la protección de datos confidenciales. En el ámbito de la salud, es fundamental proteger la información de los pacientes para asegurar su privacidad y evitar posibles vulneraciones. En el sector financiero, la seguridad de la información se enfoca en evitar el robo de información bancaria y financiera. En el mundo empresarial, es importante proteger los secretos comerciales y la propiedad intelectual de una empresa. En el gobierno, la seguridad de la información se centra en proteger la información clasificada y garantizar la seguridad nacional. Asimismo, en el ámbito legal, la protección de la información confidencial de los clientes. En el ámbito educativo, se protegen los datos personales de estudiantes y personal de la institución educativa. En el campo de la investigación, la seguridad de la información es necesaria para proteger los resultados de investigación y los datos confidenciales. Finalmente, en la industria de la tecnología, se protege la propiedad intelectual y la información confidencial.

En el área de la salud, la información es un activo de gran importancia por la naturaleza de la información que se manejan en un hospital, se considera sensible la protección de datos personales, historias clínicas y registros médicos es esencial para garantizar la privacidad de los pacientes y el correcto funcionamiento del sistema de salud en su conjunto. Por esta razón, la seguridad de la información se ha convertido en un tema crucial en el ámbito de la salud, y su falta puede tener consecuencias graves y perjudiciales. En general, cualquier organización que maneje información sensible debe preocuparse por la seguridad de la información.

En la actualidad se ha producido un aumento significativo del índice de amenazas informáticas relacionadas con fallas humanas, con ataques malintencionados que buscan sustraer datos con el fin de llevar a cabo diversos tipos de delitos, en el campo médico no es la excepción, toda la información de historias clínicas y registros médicos electrónicos de los pacientes que maneja el área de Tecnologías de la Información del Hospital General Manuel Ygnacio Monteros, es de carácter privado.

El Área de TI del HGMYM posee una alta probabilidad de que la confidencialidad, integridad, disponibilidad de la información y la infraestructura se vean afectadas por la falta de una correcta administración y aplicación de políticas de gestión de seguridad de la información, lo cual minimiza la probabilidad de recuperación ante un siniestro o evento de intrusión interno o externo.

En este contexto, la propuesta de un modelo de gestión de seguridad de la información basado en la norma ISO 27799:2008 es una herramienta que permite reducir los riesgos de la fuga de información médica, el robo o mal uso de la información personal de los pacientes, así mismo garantizar la seguridad en los sistemas de cómputo utilizados en las unidades médicas mediante la elaboración de las políticas de seguridad basadas en el análisis del marco legal ecuatoriano, de esta manera asegurar la integridad, disponibilidad y confidencialidad de la información almacenada en el sistema MIS AS400, administrado por el área de TI del HGMYM.

Para desarrollar la propuesta de un modelo de SGSI se plantean tres objetivos específicos, realizar una evaluación de la situación actual de la gestión de seguridad de la información en el HGMYM, identificar los requisitos y lineamientos establecidos en la norma ISO 27799:2008 para la gestión de la seguridad de la información en el ámbito de la salud y finalmente proporcionar recomendaciones para la mejora continua del modelo de gestión de seguridad de la información en el Hospital General Manuel Ygnacio Monteros IESS-LOJA, con el objetivo de asegurar la protección de la información y la confianza de los pacientes y otros actores del sistema de salud.

En el presente trabajo se analizarán aspectos como la clasificación de la información, el control de acceso, la gestión de contraseñas y la respuesta ante incidentes, entre otros. Así mismo se establecen controles para para la gestión de la seguridad de la información en el área de TI del HGMYM teniendo en cuenta las necesidades particulares y los entornos operativos.

4. Marco Teórico

4.1. Gestión de la Información.

La información se puede describir como la secuencia ordenada de datos que han sido analizados y comprendidos por los seres humanos, y que ofrecen detalles y descripciones de teorías, sucesos o eventos. A medida que las tecnologías de la información se vuelven ampliamente utilizadas, surgen riesgos que amenazan la integridad de la información digital, por tanto, surge un nuevo enfoque conocido como Gestión de la Información, el cual implica una serie de procesos diseñados para facilitar la adquisición, producción y distribución de la información de manera eficiente. El objetivo es permitir un análisis rápido y globalmente accesible de la información, minimizando los costos (Puga-Jácome, 2019).

La gestión de información es una disciplina que se dedica a optimizar el uso de recursos clave, como los recursos económicos, físicos, humanos y materiales, con el fin de administrar la información de manera eficiente tanto dentro de una organización como para el beneficio de la sociedad a la que se sirve. En el entorno organizativo, es posible identificar distintos tipos de información en función de las actividades desempeñadas, y resulta fundamental gestionar y utilizar esta información de forma adecuada y sistemática con el objetivo de obtener los máximos beneficios para la institución (Contardi, 2005)

En las organizaciones de salud, la gestión de la información desempeña un papel crucial en la mejora de la calidad de la atención y la eficiencia de los servicios. Además, tiene un impacto significativo en la toma de decisiones, lo que la convierte en un área de atención prioritaria. En el actual escenario del sistema nacional de salud, existen cuatro premisas fundamentales para la gestión de la información. En primer lugar, se debe considerar la estructura informacional existente, es decir, cómo se organiza y se accede a la información en las organizaciones de salud. En segundo lugar, se destaca la importancia de capitalizar los recursos humanos, es decir, contar con personal capacitado en el manejo y análisis de la información para maximizar su valor. En tercer lugar, la disponibilidad de herramientas y plataformas tecnológicas que satisfagan las necesidades de gestión de la información y el conocimiento en el ámbito de la salud. Por último, las innovaciones requeridas para facilitar el proceso de dirección en relación con la gestión de la información. Esto implica buscar y adoptar nuevas tecnologías, prácticas y enfoques que mejoren la toma de decisiones, la calidad de la atención y la eficiencia de los servicios de salud (Torres-Fernández et al., 2017).

4.1.1. Seguridad de la información

La seguridad de la información se refiere a la protección de la información contra el acceso no autorizado, el uso, la divulgación, la interrupción, la destrucción o la modificación no autorizada. Es un campo que se ocupa de salvaguardar la confidencialidad, integridad y disponibilidad de los datos, así como de proteger los sistemas de información en su conjunto. Además, se vuelve especialmente relevante en la era digital, donde la información se almacena, procesa y transmite en entornos electrónicos. Incluye la protección de datos personales, secretos comerciales, información financiera, propiedad intelectual, entre otros (Valencia-Duque, 2017).

La seguridad de la información se enfoca en proteger tanto la información como los sistemas de información de amenazas y riesgos que puedan comprometer su confidencialidad, integridad y disponibilidad. Al adoptar procesos, buenas prácticas y metodologías de seguridad, podemos mitigar y prevenir el acceso no autorizado, el mal uso y la manipulación indebida de los datos y los recursos tecnológicos. En la actualidad, la información se ha convertido en un activo valioso tanto para las organizaciones como para los individuos. Existen ciber delincuentes, hackers y otras amenazas que buscan obtener acceso ilegal a la información con el fin de cometer fraude, robo de identidad, sabotaje o cualquier otro tipo de actividad delictiva. Por lo tanto, es esencial implementar medidas de seguridad adecuadas para protegerse contra estos riesgos.(Vega Briceño, 2021).

La seguridad de la información es la disciplina que se ocupa de implementar técnicas y tecnologías para proteger la información y garantizar su disponibilidad, integridad y confidencialidad. Esta disciplina se centra en identificar y mitigar los riesgos y amenazas que pueden afectar la información y los sistemas de información. El despliegue de tecnologías adecuadas es fundamental para establecer mecanismos de seguridad eficaces. Esto implica utilizar soluciones como firewalls, sistemas de detección de intrusiones, sistemas de cifrado, autenticación de usuarios, control de acceso, entre otros, para establecer barreras y controles que prevengan el acceso no autorizado y la manipulación indebida de la información. La seguridad de la información también implica realizar análisis de escenarios y evaluaciones de riesgos para identificar posibles vulnerabilidades y amenazas. Esto permite tomar medidas preventivas y correctivas para proteger los activos de información. Además, la adopción de buenas prácticas y el cumplimiento de los esquemas normativos y regulaciones pertinentes son fundamentales para elevar el nivel de confianza en la gestión de la información (Figueroa-Suárez et al., 2018).

La seguridad de la información va más allá de la protección de datos en los computadores; su enfoque principal es salvaguardar la propiedad intelectual y la información crucial para las organizaciones y las personas. Los riesgos asociados a la información surgen cuando se combinan las amenazas y las vulnerabilidades. Estos dos elementos están estrechamente relacionados, y para que se produzcan consecuencias negativas, deben estar presentes simultáneamente. También se centra en identificar y gestionar las amenazas potenciales, así como en fortalecer las vulnerabilidades existentes. Esto implica implementar medidas de seguridad, como sistemas de detección de intrusiones, firewalls, cifrado de datos, políticas de control de acceso y capacitación del personal. Además, es fundamental contar con un enfoque proactivo que involucre la evaluación continua de riesgos y la adopción de buenas prácticas para garantizar la confidencialidad, integridad y disponibilidad de la información (Figueroa-Suárez et al., 2018).

La seguridad de la información busca proteger la propiedad intelectual y la información esencial frente a las amenazas y vulnerabilidades. Para lograrlo, se deben implementar medidas de seguridad adecuadas y mantener una gestión proactiva de los riesgos. Según Tejena-Macías, (2018) las amenazas más comunes incluyen:

- Malware
- Ataques de hacking
- Ataques de phishing
- Ataques de denegación de servicio (DDoS)
- Fuga de información interna
- Vulnerabilidades de software y sistemas
- Acceso físico no autorizado
- Robo o pérdida de dispositivos
- Vulnerabilidades en la cadena de suministro
- Espionaje y ciberataques estatales

Estas son solo algunas de las muchas amenazas a la seguridad de la información. Es importante que las organizaciones y los individuos implementen medidas de seguridad adecuadas para protegerse contra estas amenazas y mantener la integridad de su información (Tejena-Macías, 2018).

4.1.2. Sistema de Gestión de Seguridad de la Información (SGSI)

Un SGSI es un sistema integral que busca proteger los activos de información de una organización mediante la aplicación de políticas, procedimientos y controles adecuados, en

línea con los objetivos del negocio y los requisitos de seguridad. El SGSI se basa en la evaluación de riesgos y en los niveles de aceptación de riesgos definidos por la organización, con el fin de abordar y gestionar eficazmente dichos riesgos. Con el objetivo de alcanzar este propósito, se examinan los requisitos relativos a la salvaguarda de los activos de información y se implementan las medidas de control adecuadas para garantizar su protección. El objetivo principal de un SGSI es garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la organización. Esto implica identificar y evaluar los riesgos, implementar controles de seguridad adecuados y establecer mecanismos de revisión y mejora continua (Córdoba, 2022).

Según Baena et al. (2019), la implementación de un Sistema de Gestión de Seguridad de la Información es una obligación para las empresas con el fin de gestionar los riesgos de manera lógica y sistemática, cumpliendo con las regulaciones establecidas. Con el fin de asegurar la eficacia de estas implementaciones, se busca respaldo en estándares internacionales relacionados con la Seguridad de la Información, como las normas ISO, para garantizar su cumplimiento. Un SGSI se basa en tres objetivos fundamentales que son esenciales para garantizar la protección de los datos:

Confidencialidad: Se refiere a asegurar que la información se mantenga privada y solo sea accesible por las personas autorizadas. Esto implica prevenir el acceso no autorizado, ya sea accidental o intencional, a la información sensible o confidencial de una organización. La confidencialidad se logra mediante el uso de mecanismos de autenticación, controles de acceso adecuados y la implementación de políticas y procedimientos que regulen el acceso y la divulgación de la información (Torres-León, 2018).

Integridad: Se refiere a mantener la precisión, exactitud y completitud de la información a lo largo de su ciclo de vida. Esto implica prevenir la modificación, alteración o eliminación no autorizada de los datos. La integridad se logra mediante el uso de mecanismos de control y validación de la información, como firmas digitales, registros de auditoría y controles de versiones. También implica establecer políticas y procedimientos para garantizar que los cambios en la información se realicen de manera autorizada y documentada (Baena et al., 2019).

Disponibilidad: Asegura que la información esté accesible y utilizable cuando sea necesaria. Esto implica prevenir interrupciones o denegaciones de servicio que puedan afectar la disponibilidad de los sistemas y la información. La disponibilidad se logra mediante la implementación de medidas de protección física y lógica, como copias de seguridad, redundancia de sistemas, planes de recuperación de desastres y medidas de seguridad contra

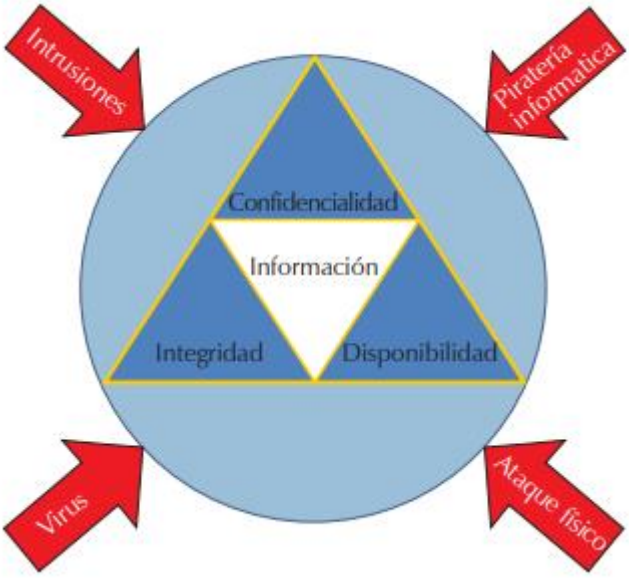
ataques cibernéticos. Además, implica mantener los sistemas actualizados y realizar un monitoreo constante para detectar y mitigar posibles amenazas o incidentes que puedan afectar la disponibilidad de la información (Torres León, 2018).

Estos tres objetivos, confidencialidad, integridad y disponibilidad, forman el núcleo del enfoque de seguridad de la información en un SGSI. Al enfocarse en estos objetivos, una organización puede establecer un marco sólido para proteger sus datos y garantizar la confianza, la continuidad del negocio y el cumplimiento de las regulaciones aplicables.

La Figura 1 ilustra los objetivos del SGSI, donde se destaca la combinación de confidencialidad, integridad y disponibilidad como elementos clave para establecer un marco de seguridad de la información. Esto tiene como propósito evitar intrusiones, ataques físicos, hacking y la propagación de virus.

Figura 1

Objetivos del Sistema de Gestión de Seguridad de la Información



Fuente:(Gutiérrez-Martínez et al., 2014)

4.1.3. Seguridad Informática

La seguridad informática se enfoca en minimizar los riesgos relacionados con el acceso y uso no autorizado, así como las acciones malintencionadas, en sistemas informáticos. Al igual que en otros entornos, el objetivo principal de la seguridad informática es proteger los valiosos recursos de información, hardware y software de una organización. Para lograr este objetivo, se implementan medidas de seguridad adecuadas que abarcan diversas áreas. Estas medidas incluyen la autenticación y control de acceso para garantizar que solo las personas autorizadas puedan acceder a los sistemas y la información sensible. Además, se implementan técnicas de

encriptación y cifrado para proteger la confidencialidad de la información mientras se transmite o almacena (Gil Vera y Gil Vera, 2017).

La seguridad informática también se ocupa de la protección física de los recursos informáticos, como el hardware y los servidores, para prevenir robos, daños o accesos no autorizados a estos activos críticos. Se establecen políticas y procedimientos para realizar copias de seguridad y restauración de datos, así como planes de recuperación ante desastres, con el fin de garantizar la disponibilidad de la información en caso de incidentes o fallas. Asimismo, la seguridad informática se ocupa de proteger los sistemas y las redes contra ataques cibernéticos, como virus, malware, ataques de denegación de servicio y hacking. Se implementan soluciones de seguridad, como firewalls, sistemas de detección y prevención de intrusiones, y se mantienen actualizadas las aplicaciones y los sistemas operativos para mitigar las vulnerabilidades conocidas (Gil Vera y Gil Vera, 2017).

La seguridad informática tiene como objetivo garantizar la ausencia de riesgos en todos los componentes de un sistema, que incluyen hardware, software, personal informático, redes, usuarios, datos y procedimientos. Su principal finalidad es prevenir el acceso no autorizado a la información que se encuentra en el sistema y evitar cualquier modificación, daño, alteración, eliminación o tratamiento no autorizado. Los activos que pueden estar en riesgo abarcan todos los elementos que componen el patrimonio y tienen valor para una empresa, gobierno o individuo. Esto incluye equipos, hardware, programas informáticos, así como patentes, procesos utilizados y actividades relacionadas con el negocio (Téllez-Carvajal, 2018).

La seguridad informática es un campo de amplio alcance que se encuentra estrechamente relacionado con el concepto general de seguridad. En su definición, la informática destaca que el activo principal es la información, la cual posee un gran poder. Por lo tanto, resulta evidente que todas las técnicas, métodos, procesos, almacenamientos y transmisiones que involucran el procesamiento de información deben implementarse de manera segura, con el objetivo de proteger la información de cualquier organización. En la actualidad, la seguridad informática desempeña un papel fundamental en el día a día, ya que se ha vuelto indispensable y primordial. Es por ello que las empresas que cuentan con redes y sistemas informáticos deben establecer políticas de seguridad efectivas. Estas políticas permiten una coordinación adecuada y proporcionan directrices que garantizan la protección de la información de manera conveniente (Durand-More, 2019)

4.2. El Sistema de Salud en el Ecuador

El sistema de salud en Ecuador se compone de dos sectores: el sector público y el sector privado. En el sector público, se encuentran instituciones como el Ministerio de Salud Pública

(MSP), el Ministerio de Inclusión Económica y Social (MIES), los servicios de salud municipales y las instituciones de seguridad social, que incluyen el Instituto Ecuatoriano de Seguridad Social (IESS), el Instituto de Seguridad Social de las Fuerzas Armadas (ISSFA) y el Instituto de Seguridad Social de la Policía Nacional (ISSPOL). El MSP proporciona servicios de atención médica a toda la población, mientras que el MIES y las municipalidades ofrecen programas y establecimientos de salud para aquellos que no tienen seguro médico. Las instituciones de seguridad social cubren a la población asalariada afiliada (Lucio et al., 2011).

En el sector privado, se encuentran entidades con fines de lucro como hospitales, clínicas, dispensarios, consultorios, farmacias y empresas de medicina prepagada. También existen organizaciones no lucrativas de la sociedad civil y de servicio social. Los seguros privados y las empresas de medicina prepagada brindan cobertura a aproximadamente el 3% de la población con ingresos medios y altos. Además, en Ecuador hay alrededor de 10,000 consultorios médicos particulares ubicados principalmente en las principales ciudades. Estos consultorios suelen contar con infraestructura y tecnología básica. En general, la población que recibe atención médica en estos consultorios realiza pagos directos de su bolsillo en el momento de recibir la atención (Lucio et al., 2011).

La Constitución de la República de Ecuador (2008), reconocida como la ley suprema del país, establece que la salud es un derecho garantizado para todos los ciudadanos. Su objetivo es asegurar que todas las personas tengan la oportunidad de alcanzar el más alto nivel posible de bienestar físico y mental. Además, la Constitución establece los mecanismos necesarios para hacer efectivo este derecho y define los principios esenciales en los que se fundamenta la creación del Sistema Nacional de Salud (SNS). Considerando lo anterior el artículo 32 de la Constitución de la República, en la sección séptima sobre la salud como un derecho garantizado por el Estado, manifiesta:

- «Art. 32.- La salud es un derecho que garantiza el Estado, cuya realización se vincula al ejercicio de otros derechos, entre ellos el derecho al agua, la alimentación, la educación, la cultura física, el trabajo, la seguridad social, los ambientes sanos y otros que sustentan el buen vivir» (Constitución de la República de Ecuador, 2008).

La Constitución de la República del Ecuador establece el SNS, describiendo sus principios, integrantes y obligaciones, así como designando una autoridad sanitaria nacional, tal como se especifica en los artículos 358, 359, 360, 361 y 362 de la sección dedicada a la salud:

- «Art. 358. El Sistema Nacional de Salud tendrá por finalidad el desarrollo, protección y recuperación de las capacidades y potencialidades para una vida saludable e integral, tanto individual como colectiva, y reconocerá la diversidad social y cultural. El sistema se guiará por los principios generales del sistema nacional de inclusión y equidad social, y por los de bioética, suficiencia e interculturalidad, con enfoque de género y generacional» (Constitución de la República de Ecuador, 2008)
- «Art. 359 El Sistema Nacional de Salud comprende las instituciones, programas, políticas, recursos, acciones y actores en salud, y que debe abarcar todas las dimensiones del derecho a la salud. Además, debe garantizar la promoción, prevención, recuperación y rehabilitación en todos los niveles, y propiciar la participación ciudadana y el control social» (Constitución de la República de Ecuador, 2008).

La Ley Orgánica del SNS establece los principios y normas generales para la organización y funcionamiento del SNS en todo el territorio nacional. Este sistema tiene como objetivo mejorar el nivel de salud y calidad de vida de la población ecuatoriana, garantizando el ejercicio efectivo del derecho a la salud en todas sus dimensiones (Ley Orgánica del Sistema Nacional de Salud, 2002).

En la Tabla 1 se detallan las cinco funciones fundamentales que ejerce el Sistema Nacional de Salud:

Tabla 1
Funciones del Sistema Nacional de Salud

Funciones del Sistema Nacional de Salud		
Rectoría	El Estado garantizará la rectoría del sistema a través de la Autoridad Sanitaria Nacional, será responsable de formular la política nacional de salud, y normará, regulará y controlará todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector	Constitución de la República del Ecuador Art. 361
Coordinación	Es la función del sistema que coordina el relacionamiento entre las demás funciones y entre los integrantes del Sistema. Su ejercicio es competencia del Ministerio Salud Pública, en todos sus niveles, como autoridad sanitaria nacional, apoyado por los Consejos de Salud.	Ley Orgánica del Sistema Nacional de Salud Art. 10
Provisión de servicios	La provisión de servicios de salud es plural y con participación coordinada de las instituciones prestadoras. El Sistema establecerá los mecanismos para que las instituciones garanticen su operación en redes y aseguren la calidad, continuidad y complementariedad de la atención.	Ley Orgánica del Sistema Nacional de Salud Art.11
Funciones del Sistema Nacional de Salud		

Aseguramiento	Es la garantía de acceso universal y equitativo de la población al Plan Integral de Salud en cumplimiento al derecho ciudadano a la protección social en salud. Se promoverá la ampliación de cobertura de salud de todas las entidades prestadoras de servicios y del Seguro General Obligatorio y Seguro Social Campesino, pertenecientes al IESS, de otros seguros públicos, como el ISSFA e ISSPOL.	Ley Orgánica del Sistema Nacional de Salud Art.12
Financiamiento	El financiamiento es la garantía de disponibilidad y sostenibilidad de los recursos financieros necesarios para la cobertura universal en salud de la población. El Consejo Nacional de Salud establecerá mecanismos que permitan la asignación equitativa y solidaria de los recursos financieros entre grupos sociales, provincias y cantones del país, así como su uso eficiente.	Ley Orgánica del Sistema Nacional de Salud Art. 13

Fuente: (Flores y Castillo, 2012)

4.2.1. Leyes y Reglamentos sobre confidencialidad de la información para el sector salud del Ecuador

Las leyes y reglamentos sobre confidencialidad de la información para el sector salud en Ecuador son normativas legales que establecen las pautas y responsabilidades para la protección de la información médica y personal de los pacientes. Estas leyes y reglamentos buscan salvaguardar la privacidad y confidencialidad de los datos de salud y garantizar que se cumplan los estándares de seguridad en el manejo de la información.

4.2.2. Ley Orgánica de Transparencia y acceso a la información pública.

Para los establecimientos de salud que reciben o administran fondos públicos la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), protege la información confidencial que en su artículo 6 señala:

- «Art. 6.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República» (Ley Orgánica de Transparencia y acceso a la Información Pública, 2004).

4.2.3. Ley Orgánica de Salud

La Ley Orgánica de Salud de los Derechos y deberes de las personas y del Estado en relación con la salud, salvaguarda la privacidad y confidencialidad de la información contenida en las historias clínicas, que en su artículo 7 señala:

- «Art. 7.- Toda persona, sin discriminación por motivo alguno, tiene en relación a la salud, los siguientes derechos (...) f) Tener una historia clínica única redactada en

términos precisos, comprensibles y completos; así como la confidencialidad respecto de la información en ella contenida» (Ley Orgánica de la Salud, 2006).

Esta legislación garantiza la protección de los datos sensibles de los pacientes, asegurando que su información médica sea tratada de manera confidencial y respetando sus derechos en relación con la salud.

4.2.4. Ley de Derechos y Amparo del paciente

Asimismo, la Ley de Derechos y Amparo del Paciente salvaguarda la confidencialidad de la información del Sistema Nacional de Salud en su artículo 4 que dispone:

- «Art. 4.- Derecho a la confidencialidad: Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial» (Ley de Derechos y Amparo del paciente, 2006)

Esta legislación garantiza la protección de la confidencialidad de la información de los pacientes que utilizan los servicios de las entidades adscritas al SNS preservando la privacidad de los datos médicos de los pacientes, asegurando que solo sean accesibles por personal autorizado y respetando sus derechos fundamentales en materia de salud.

4.2.5. Reglamento de Información confidencial en el Sistema Nacional de Salud

El MSP mediante Acuerdo Ministerial 5216 emitido en el año 2015 expide el Reglamento de Información Confidencial en el SNS que tiene como objetivo «Establecer las condiciones operativas de la aplicación de los principios de manejo y gestión de la información confidencial de los pacientes y sus disposiciones serán de cumplimiento obligatorio dentro del SNS» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015).

El reglamento, en sus artículos 2, 3, 4, 5 y 6, establece principios de Confidencialidad, Integridad, Disponibilidad, Seguridad en el manejo de la información y Secreto Médico.

- «Art. 2.- Confidencialidad. - Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)
- «Art. 3.- Integridad de la información. - Es la cualidad o propiedad de la información que asegura que no ha sido mutilada, alterada o modificada, por lo tanto, mantiene sus características y valores asignados o recogidos en la fuente. Esta

cualidad debe mantenerse en cualquier formato de soporte en el que se registre la información, independientemente de los procesos de migración entre ellos» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015).

- «Art. 4.- Disponibilidad de la información. - Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)
- «Art. 5.- Seguridad en el manejo de la información. - Es el conjunto sistematizado de medidas preventivas y reactivas que buscan resguardar y proteger la información para mantener su condición de confidencial, así como su integridad y disponibilidad. Inicia desde el momento mismo de la generación de la información y trasciende hasta el evento de la muerte de la persona (...)» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)
- «Art. 6.- Secreto Médico. - Es la categoría que se asigna a toda información que es revelada por un/a usuario/a al profesional de la salud que le brinda la atención de salud. Se configura como un compromiso que adquiere el médico ante el/la usuario/a y la sociedad, de guardar silencio sobre toda información que llegue a conocer sobre el/la usuario/a en el curso de su actuación profesional» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)

Dentro del manejo operativo en la prestación de servicios de salud es indispensable el uso y manejo de historias clínicas, como lo señala en el cuarto capítulo del Acuerdo Ministerial 5216 donde se establecen disposiciones relacionadas con la seguridad en la custodia de las historias clínicas.

- «Art. 14.- La historia clínica sólo podrá ser manejada por personal de la cadena sanitaria. Como tal se entenderá a los siguientes profesionales: médicos, psicólogos, odontólogos, trabajadoras sociales, obstetrices, enfermeras, además de auxiliares de enfermería y personal de estadística» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)
- «Art. 15.- El acceso a documentos archivados electrónicamente será restringido a personas autorizadas por el responsable del servicio o del establecimiento, mediante claves de acceso personales» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)

- «Art. 16.- La custodia física de la historia clínica es responsabilidad de la institución en la que repose. El personal de la cadena sanitaria, mientras se brinda la prestación, es responsable de la custodia y del buen uso que se dé a la misma, generando las condiciones adecuadas para el efecto» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)
- «Art. 17.- El archivo de historias clínicas es un área restringida, con acceso limitado solo a personal de salud autorizado, donde se guardan de manera ordenada, accesible y centralizada todas las historias clínicas que se manejan en el establecimiento. Se denomina activo cuando cuenta con historias activas, esto es con registros de hasta cinco años atrás y se denomina pasivo cuando almacena aquellas que tienen más de cinco años sin registros, tomando en cuenta la última atención al paciente» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)
- «Art. 18.- Los datos y la información consignados en la historia clínica y los resultados de pruebas de laboratorio e imagenología registrados sobre cualquier medio de soporte ya sea físico, electrónico, magnético o digital, son de uso restringido y se manejarán bajo la responsabilidad del personal operativo y administrativo del establecimiento de salud, en condiciones de seguridad y confidencialidad que impidan que personas ajenas puedan tener acceso a ellos» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)
- «Art. 19.- Todas las dependencias que manejen información que contenga datos relevantes sobre la salud de los/las usuarios/as deberán contar con sistemas adecuados de seguridad y custodia» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)
- «Art. 20.- Los documentos físicos que contengan información confidencial de los/las usuarios/as y que no requieran ser archivados, deberán ser destruidos evitando su reutilización, de conformidad a lo dispuesto en el Capítulo II del Manual del Manejo, Archivo de las Historias Clínicas» (Reglamento de Información confidencial en el Sistema Nacional de Salud, 2015)

4.2.6. Código Orgánico Integral Penal de Ecuador

El Código Orgánico Integral Penal de Ecuador define y sanciona delitos relacionados con la divulgación de información de carácter confidencial o reservada, tal como se lo señala en los siguientes artículos:

- «Art 179.- Revelación de secreto. - La persona que, teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año» (Código Orgánico Integral Penal, 2014).
- «Art. 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años» (Código Orgánico Integral Penal, 2014)
- «Art. 230.- Interceptación ilegal de datos. Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior» (Código Orgánico Integral Penal, 2014).

- «Art. 231.- Transferencia electrónica de activo patrimonial. La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o

sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona» (Código Orgánico Integral Penal, 2014)

- «Art. 232.- Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad» (Código Orgánico Integral Penal, 2014).

- «Art. 233.- Delitos contra la información pública reservada legalmente. La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele

dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad» (Código Orgánico Integral Penal, 2014)

- «Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años» (Código Orgánico Integral Penal, 2014).

4.2.7. Reglamento orgánico funcional del Instituto Ecuatoriano de Seguridad Social

El Reglamento Orgánico Funcional del IESS, expedido por el Consejo Directivo mediante Resolución CD 535 vigente desde el 06 de mayo de 2017, Art. 10, Numeral 4.2, entre otras, atribuciones y responsabilidades de la Dirección Nacional de Tecnologías de la Información dispone lo siguiente: (...) a) «Definir políticas, metodologías y procedimientos de gestión e implementación de tecnologías de la información a nivel institucional. (...)»; c) «Gestionar la formulación, implementación, seguimiento y evaluación del cumplimiento de la planificación estratégica y operativa de las actividades técnicas informáticas de las dependencias o unidades a nivel nacional y de los proyectos de innovación en el ámbito de tecnologías de la información. (...)»; e) «Definir, planificar, coordinar, desarrollar y controlar los proyectos de tecnología de la información y comunicación a nivel nacional. (...)»; g) «Generar lineamientos y directrices basados en estándares y mejores prácticas internacionales para la gestión de tecnología de la información. Adopción y i) desarrollo de nuevas plataformas y soluciones tecnológicas de base de datos, redes de comunicaciones, sistemas, desarrollo, mantenimiento de aplicaciones y soporte técnico a usuarios internos para la institución. (...)»; p) «Brindar apoyo a las dependencias y unidades de negocio en la definición de especificaciones técnicas y/o la gestión del componente tecnológico de los proyectos; (...)» (Reglamento orgánico funcional IESS, 2016)

4.3. Normas ISO de Seguridad de la Información.

Las normas ISO son estándares de seguridad desarrollados por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Estas normas proporcionan pautas y requisitos para diversos sistemas de gestión, y son aplicables a organizaciones tanto a nivel nacional como internacional. Su objetivo principal es facilitar el comercio, promover el intercambio de información y fomentar la transferencia de tecnología. Estas normas buscan establecer un marco común para garantizar la calidad, la eficiencia y la seguridad en diferentes áreas (Contero, 2019)

4.3.1. Norma ISO/IEC 27000

Está diseñada para asistir a las organizaciones en el establecimiento y mantenimiento de la seguridad de sus activos. Estos activos pueden incluir información financiera, propiedad intelectual, datos de empleados y otra información confidencial de terceros. La implementación de estos estándares permite a las organizaciones gestionar de manera efectiva la seguridad de estos activos, aplicando controles y medidas apropiadas para protegerlos contra amenazas y riesgos. Al seguir las directrices de la norma ISO/IEC 27000, las organizaciones pueden establecer un marco sólido de seguridad de la información, promoviendo la confidencialidad, integridad y disponibilidad de los datos, y generando confianza entre los clientes, socios comerciales y demás partes interesadas (Garcia Cruz, 2021)

4.3.2. Estándar ISO/IEC 27001

La Norma ISO/IEC 27001:2013 establece los requisitos para crear, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI basado en procesos. Es la norma principal de la familia ISO/IEC 27000 y se aplica a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Los requisitos genéricos definidos en esta norma garantizan la creación de un SGSI sólido y eficaz para proteger los activos de información críticos de la organización (Lachapelle & Bislimi, 2015).

La norma ISO 27001, emitida por la Organización Internacional de Normalización (ISO), es un estándar internacional que establece los requisitos para gestionar la seguridad de la información en una empresa. La última revisión de esta norma se publicó en 2013 y se conoce como ISO/IEC 27001:2013. La primera versión se lanzó en 2005 y se basó en la norma británica BS 7799-2. La ISO 27001 es aplicable a todo tipo de organizaciones, ya sean con o sin fines de lucro, públicas o privadas, pequeñas o grandes. Fue redactada por expertos de renombre en el campo y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. Además, permite que una empresa obtenga

la certificación, lo cual implica que una entidad de certificación independiente verifica que se ha implementado la seguridad de la información en cumplimiento con los requisitos de la norma ISO 27001 (Nieves, 2017).

La Norma ISO/IEC 27001:2013 se basa en el modelo PDCA (Figura 2), el mismo que consta de los siguientes pasos:

Planear: El primer paso del proceso de gestión de seguridad de la información es la planificación, que implica establecer políticas, objetivos, procesos y procedimientos del SGSI. Esto permite optimizar el manejo del riesgo y obtener una visión general del mejoramiento de la seguridad de la información en la organización.

Hacer: Poner en práctica las políticas, objetivos, procesos y procedimientos definidos en el SGSI, mediante la implementación de controles de seguridad y medidas de protección que permitan la gestión efectiva de los riesgos identificados en la fase de planificación.

Verificar: Realizar una evaluación para determinar si se ha cumplido con los objetivos establecidos en el SGSI, lo que resultará en un informe que incluya los resultados y las novedades identificadas durante el proceso.

Actuar: En base a los resultados de la auditoría interna del SGSI y la revisión gerencial o de otra índole relevante, se deben tomar medidas correctivas y preventivas para lograr la mejora continua del sistema. Estas acciones deben ser documentadas y monitoreadas para asegurar su efectividad y para identificar nuevas oportunidades de mejora.

Figura 2

Modelo PDCA aplicado a los procesos SGSI.

Fuente: (Cayambe Villa, 2020)

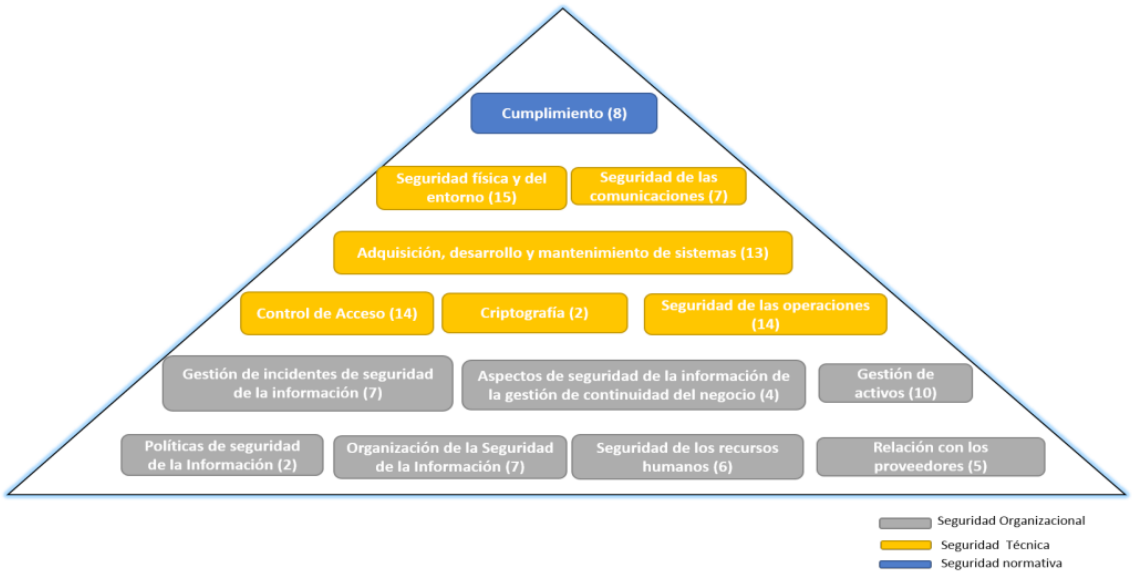
4.3.3. Estándar ISO/IEC 27002

La norma ISO/IEC 27002, formalmente conocida como Tecnología de la Información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información, ha sido desarrollada por ISO (2015) para ser utilizada por organizaciones que deseen lograr los siguientes objetivos: (a) Elegir controles en el proceso de implementación de un SGSI basado en la norma ISO/IEC 27001. (b) Efectuar controles de seguridad de la información ampliamente aceptados. (c) Desarrollar pautas de gestión de seguridad de la información. La norma ISO/IEC 27002 proporciona un conjunto de controles de seguridad de la información y prácticas recomendadas que las organizaciones pueden adoptar para proteger sus activos de información. Estos controles cubren áreas clave como la seguridad de la infraestructura tecnológica, la gestión de acceso, la gestión de incidentes de seguridad, la seguridad física y ambiental, entre otros.

Al seguir los principios y directrices establecidos en la norma ISO/IEC 27002, las organizaciones pueden fortalecer su postura de seguridad de la información y reducir los riesgos asociados con amenazas internas y externas. Además, al utilizar esta norma, las organizaciones pueden alinear sus prácticas de seguridad con estándares reconocidos internacionalmente y mejorar la confianza de sus clientes y socios comerciales en la protección de su información (Valencia-Duque, 2017). En la Figura 3 se muestra el contenido de la Norma ISO/IEC 27002:2013.

Figura 3

Contenidos de la norma ISO 27002:2013



Fuente: (Valencia-Duque, 2017)

4.3.4. Estándar ISO/IEC 27005

La norma ISO/IEC 27005, formalmente conocida como Tecnología de la Información - Técnicas de seguridad - Gestión del riesgo en la seguridad de la información, es una norma que ofrece directrices para la gestión del riesgo en el ámbito de la seguridad de la información.

Aunque no proporciona metodologías específicas, es un recurso clave para desarrollar un SGSI. El enfoque de gestión del riesgo es fundamental para proteger los activos de información de una organización. Si bien existen varios marcos de referencia disponibles, la mayoría comparten elementos comunes que son esenciales para llevar a cabo una gestión efectiva del riesgo. La norma ISO/IEC 27005 proporciona un marco general para identificar, evaluar y tratar los riesgos de seguridad de la información. A través de esta norma, las organizaciones pueden establecer un proceso sistemático y estructurado para comprender los riesgos, implementar medidas de control adecuadas y monitorear continuamente el entorno de seguridad (Valencia-Duque, 2017).

Al utilizar la norma ISO/IEC 27005, las organizaciones pueden mejorar su capacidad para tomar decisiones informadas en relación con la seguridad de la información, asignar recursos de manera efectiva y establecer una cultura de gestión proactiva del riesgo. Esto contribuye a proteger los activos de información, mitigar las amenazas y salvaguardar la integridad, confidencialidad y disponibilidad« de la información en la organización (Valencia-Duque, 2017).

4.3.5. Estándar ISO 27799

La norma internacional ISO 27799 proporciona orientación a las organizaciones del sector sanitario y a otros responsables de la información personal de salud sobre cómo proteger de manera efectiva la confidencialidad, integridad y disponibilidad de dicha información. Esta norma se basa en la implementación de la norma ISO/IEC 27001 y 27002. En particular, la norma ISO 27799 aborda las necesidades especiales de gestión de seguridad de la información en el sector sanitario y sus entornos operativos únicos. Si bien la protección y seguridad de la información personal son importantes para todos los individuos, corporaciones, instituciones y gobiernos, en el ámbito sanitario existen requisitos especiales que deben cumplirse para garantizar la confidencialidad, integridad, trazabilidad y disponibilidad de los datos personales de salud. Esta información se considera una de las más confidenciales de todos los tipos de datos personales (Cárdenas, 2018).

Mantener la privacidad de los pacientes es fundamental para la atención médica, por lo que es esencial proteger la confidencialidad de la información sanitaria. La integridad de la

información sanitaria debe ser protegida para brindar seguridad al paciente, y un componente importante de esta protección es asegurar que el ciclo de vida completo de la información sea totalmente auditable. Además, la disponibilidad de la información sanitaria es fundamental para una prestación de servicios de salud efectiva. Los sistemas informáticos en el ámbito sanitario deben cumplir con demandas únicas para mantenerse operativos frente a desastres naturales, fallas del sistema y ataques de denegación de servicio (Cárdenas, 2018).

La disponibilidad de la información sanitaria desempeña un papel crucial en la toma de decisiones por parte de los profesionales sanitarios, como los médicos. Los sistemas de información en la salud deben cumplir con exigencias únicas para garantizar su funcionamiento continuo frente a desastres naturales, fallos del sistema y ataques de denegación de servicio. Por tanto, la protección de la confidencialidad, integridad y disponibilidad de la información sanitaria requiere habilidades especializadas (Puga-Jacome, 2019).

Entre las mejores prácticas solicitadas por el ISO 27799 se encuentran:

- Controles de acceso a datos que incluye la gestión de acceso privilegiado
- Control criptográfico de datos confidenciales
- Administración y protección de las claves de cifrado
- Registrar y archivar «todos los eventos importantes relacionados con el uso y la gestión de las identidades de los usuarios y la información secreta de autenticación» y proteger esos registros de «alteraciones y accesos no autorizados». (Ley Orgánica del Sistema Nacional de Salud, 2002)

La norma ISO 27799:2008 es un documento complementario a la norma ISO/IEC 27002, y no tiene como objetivo suplantar a las normas ISO/IEC 27002 e ISO/IEC 27001, sino complementarlas con información específica para la gestión de la seguridad de la información en el sector de la salud. La norma ISO 27799:2008 proporciona directrices para la gestión de la seguridad de la información en las organizaciones del sector de la salud, incluyendo la privacidad, la seguridad y la gestión de riesgos (Puga-Jacome, 2019). En la Tabla 2 se presenta la estructura de la norma para una mejor comprensión

Tabla 2

Estructura de la norma ISO 27799:2008

ISO 27799:2008	
1.- Alcance	
2.- Referencias normativas	
3.- Términos y definiciones	
4.- Términos abreviados	
5.- Seguridad de la información sanitaria	• Objetivos de seguridad de la información en salud

	• Seguridad de la información dentro de la gobernanza de la información • Gobernanza de la información dentro del gobierno corporativo y clínico • Información de salud a proteger • Amenazas y vulnerabilidades en la seguridad de la información de salud
6.- Plan de acción práctico para la aplicación de la norma ISO/IEC 27002	• Taxonomía de las normas ISO/IEC 27002 e ISO/IEC 27001 • Compromiso de la administración con la implementación de ISO/IEC 27002 • Establecer, operar, mantener y mejorar el SGSI • Planificar: establecimiento del SGSI • Hacer: implementar y operar el SGSI • Comprobar: monitoreo y revisión del SGSI • Actuar: mantener y mejorar el SGSI
7.- Implicaciones para la salud de ISO/IEC 27002.	• General • Política de seguridad de la información • Organización de la seguridad de la información • Gestión de activos • Seguridad de los recursos humanos • Seguridad física y medio ambiental • Comunicaciones y gestión de operaciones • Control de acceso • Adquisición, desarrollo y mantenimiento de sistemas de información • Gestión de incidentes de seguridad de la información • Aspectos de la seguridad de la información en la gestión de la continuidad del negocio (BCM) • Conformidad

Fuente: (Enríquez, 2018)

En resumen en el presente capítulo se abordó conceptos y principios de seguridad de la información, así mismo se analizó las normas ISO 27799:2008 y otros estándares relacionados, además de explorar la legislación nacional en Ecuador sobre confidencialidad de la información en la salud, con estos antecedentes en el siguiente apartado se define la metodología y las diferentes acciones a seguir (identificación de activos, identificación de riesgos, tratamiento de riesgos) que servirán para el desarrollo de la propuesta de modelo de SGSI para el área de TI del HGMYM.

4.4. Medición y priorización de los riesgos

En la norma ISO 27799:2008, la medición y priorización de los riesgos es un proceso fundamental dentro del marco de gestión de seguridad de la información. Este proceso tiene como objetivo identificar, evaluar y clasificar los riesgos asociados a la seguridad de la información en una organización.

La medición de riesgos implica la identificación de los activos de información y sus valores, así como la determinación de las amenazas potenciales que podrían afectar la confidencialidad, integridad y disponibilidad de esos activos. Además, se analizan las vulnerabilidades existentes, es decir, las debilidades en los controles de seguridad que podrían ser explotadas por las amenazas.

A partir de la correcta identificación de los riesgos y su respectiva consecuencia se evalúan las prioridades, donde se establecen los siguientes criterios y notaciones:

4.4.1. Probabilidad de ocurrencia

- Muy alta (MA)
- Alta (A)
- Media (M)
- Baja (B)
- Muy Baja (MB)

4.4.2. Nivel de impacto

- Alto (A): Cuando se requieren gran cantidad de medidas para mitigar el impacto, viéndose afectada la continuación del proyecto sino se toman las medidas adecuadas.
- Medio (M): Afectación en la calidad del proyecto sino se toman las medidas de mitigación adecuadas.
- Bajo (B): El impacto puede mitigarse a través de medidas sencillas y existe poca afectación en la calidad del proyecto y entrega a tiempo del mismo.

Para representar los resultados se creó una matriz de impacto por probabilidad de ocurrencia tal y como muestra la Tabla 3

Tabla 3

Matriz de probabilidad e impacto.

Probabilidad	Impacto		
	Alto	Medio	Bajo
Muy alta (MA)	MAP	MAP	AP
Alta (A)	MAP	AP	PM
Media (M)	AP	PM	PB
Baja (B)	PM	PB	MBP
Muy baja (MB)	PB	MBP	MBP

Fuente: El Autor

De aquí que se defina el nivel de riesgo a través de las categorías:

- Muy alta prioridad (MAP)
- Alta prioridad (AP)
- Prioridad media (PM)
- Prioridad baja (PB)
- Muy baja prioridad (MBP)

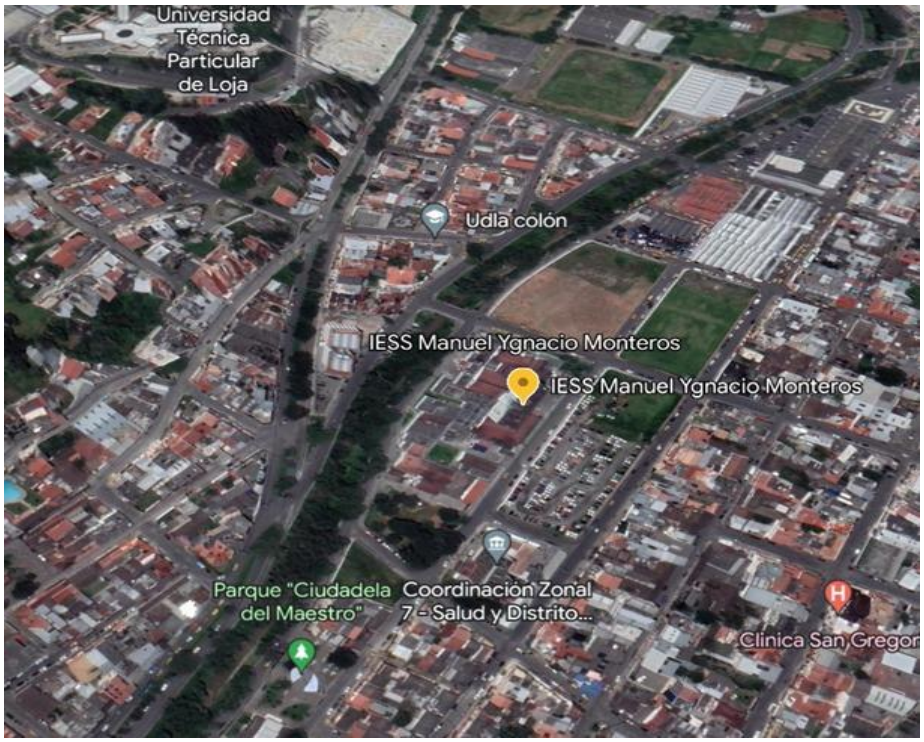
5. Metodología

5.1. Área de Estudio

El Hospital General Manuel Ygnacio Monteros se encuentra ubicado al Nororiente de la ciudad de Loja, en la parroquia El Valle del Cantón Loja, Provincia de Loja, que por su desarrollo y ubicación geográfica fue nombrada sede administrativa de la zona 7 conformada por las provincias de El Oro, Loja y Zamora Chinchipe. Se encuentra a 3°59'3" latitud Sur y 79°12'11" longitud Oeste.

Figura 4

Localización del Área de Estudio



5.2. Procedimiento

La presente investigación se la realizó utilizando los lineamientos definidos en la Norma ISO 27799:2008, tomando como referencia para el análisis los riesgos identificados, partiendo del análisis de la situación actual del área de Tecnologías de la Información del Hospital General Manuel Ygnacio Monteros en cuanto a seguridad de la información se refiere. Además, se utilizó técnicas de investigación cualitativa como: observación participativa, investigación documental, análisis de datos y reporte de resultados. De esta forma se definieron las fases con sus respectivas tareas que permitieron cumplir con los objetivos planteados en la presente investigación, detalladas a continuación:

- Fase Uno: Identificación del ámbito de aplicación y los objetivos de seguridad de la información

- Identificación del ámbito de aplicación
- Objetivos de seguridad de la información
- Determinar el Alcance
- Identificación del procedimiento

- Fase Dos: Gestión de activos de información del área de Tecnologías del Hospital Manuel Ygnacio Monteros.
  - Identificación de activos de información.
  - Inventario de activos información
  - Propiedad de los Activos
- Fase Tres: Identificar las amenazas y vulnerabilidades asociadas a la Seguridad de Información del Hospital General Manuel Ygnacio Monteros.
  - Medición y priorización de los riesgos.
  - Mitigación de riesgos.
  - Monitoreo de los riesgos
  - Comunicación del riesgo.
- Fase Cuatro: Diseño y propuesta del modelo de gestión de seguridad de la información.
  - Definir las políticas de seguridad de uso de seguridad informática y de la información.
  - Determinar las disposiciones generales para la administración el sistema MIS AS400.
  - Establecer los lineamientos de seguridad informática.
  - Establecer los lineamientos generales para la administración y gestión del Sistema MIS AS400
  - Establecer las restricciones y prohibiciones.
- Fase Cinco: Documentación anexa para su aplicabilidad en la administración del sistema MIS AS400.
  - Definir los formatos de administración de usuarios.
  - Compromiso de confidencialidad de la información.

6. Resultados

6.1. Análisis Situacional

Es importante comprender el contexto en el que opera el Hospital, tomando en cuenta el estado actual de la Institución y en la organización del área de TI y sus competencias con respecto al manejo de información del HGMYM.

6.1.1. La Institución

Figura 5

Hospital General Manuel Ygnacio Montero

El HGMYM (Figura 5) pertenece a una tipología de nivel II, cuenta con una capacidad instalada de 129 camas censables y 51 camas no censables, cuya zona de influencia son las provincias de Loja, Zamora Chinchipe y El Oro, teniendo como unidades de las que recibe referencias a dos Hospitales del Día, 11 Unidades de Atención Ambulatoria tipo B, 1 Unidad de Atención ambulatoria tipo A, 56 Unidades Médicas del SSC de las provincias de Loja y de Zamora Chinchipe y 35 Unidades del SSC de El Oro, sin olvidar las referencias recibidas de la Red Pública de Salud, que a partir del año 2011 la cobertura de servicios de salud también beneficias a los hijos/as menores de 18 años de afiliados/as, Cobertura de Conyugue, ISFA, ISPOL y Red Pública de Salud.

El HGMYM, brinda servicios de salud a pacientes hospitalizados como ambulatorios con una cobertura a nivel de la Zona 7. Es una unidad de referencia subregional o provincial

que atiende a usuarios con equipos de trabajo multidisciplinario, formada científica, ética y humanísticamente en cirugía clínica, cuidado materno infantil, medicina crítica y Auxiliares.

6.1.2. Área de Tecnologías de Información

La Unidad de TI, está posicionada dentro de la estructura organizacional de la entidad en un nivel que le permite efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además, debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.

La misión del área de TI es generar y administrar servicios de tecnología de la información, que permitan garantizar el control y seguridad informática en la gestión de la institución, de una manera eficiente, alineados a la misión institucional y al marco regulatorio vigente.

6.1.3. Administración de la Información médica en el área de tecnologías

El área de TI del HGMYM es la responsable de llevar a cabo la Administración y control técnico del Sistema MIS-AS400 del HGMYM, en la configuración y parametrización de sus módulos complementarios, sus procesos deben ser informados, coordinados, supervisados y aprobados previamente por la Dirección Nacional de Tecnologías de la Información (DNTI), con la finalidad de dirigir los proyectos tecnológicos relativos a este sistema y el logro de una adecuada administración del sistema, en cumplimiento de objetivos y responsabilidades institucionales, con resultados de eficiencia y eficacia.

La DNTI es quien realiza la coordinación y supervisión de las actividades tecnológicas, con los técnicos informáticos desconcentrados y/o técnicos de las dependencias del IESS, incluidos técnicos informáticos de las Unidades Médicas del Seguro General de Salud Individual y Familiar a Nivel Nacional, Coordinaciones Generales de TIC de los Hospitales de Especialidades.

En el ámbito de la competencia el área de TI del HGMYM es la encargada de administrar todo lo referente a las parametrizaciones en el sistema MIS AS400 (creación/inactivación de usuarios, dependencias, bodegas, kárdex y otros parámetros) y a su vez del control técnico, brindando soporte en los diferentes requerimientos de los usuarios que hacen uso del sistema.

6.2. Identificación del ámbito de aplicación y los objetivos de seguridad de la información.

6.2.1. Ámbito de aplicación

Área de Tecnologías de la Información del Hospital General Manuel Ygnacio Monteros que maneja el Sistema de gestión médica MIS-AS400.

6.2.2. Objetivo

Generar un flujo de atención de los requerimientos, solicitudes de información, mantenimientos y desarrollos para el Sistema MIS-AS400 a nivel del área de TI.

6.2.3. Alcance

Normar de forma estandarizada el flujo de atención de requerimientos técnicos, solicitudes de entregas de información y/o mejoras en el Sistema MIS-AS400, desde la generación del requerimiento, hasta el cierre del requerimiento.

6.2.4. Identificación del procedimiento

Procedimiento de Administración y Control Técnico del Sistema MIS-AS400.

6.3. Situación Tecnológica del Hospital

El HGMYM establece directrices para el tratamiento y administración de las tecnologías de la información internas, mismas que deben ser aplicadas para garantizar el funcionamiento de las áreas administrativas y de salud, pero no dirigidas a la Seguridad de la Información y específicamente para el área de TI en el manejo del sistema MIS-AS400. Cuenta con un documento de políticas para el uso adecuado de las tecnologías de la información y comunicación, políticas de contraseñas, políticas de uso de correo electrónico, política de uso de software, política de desarrollo de software, política de uso de internet e intranet y política de arquitectura de software.

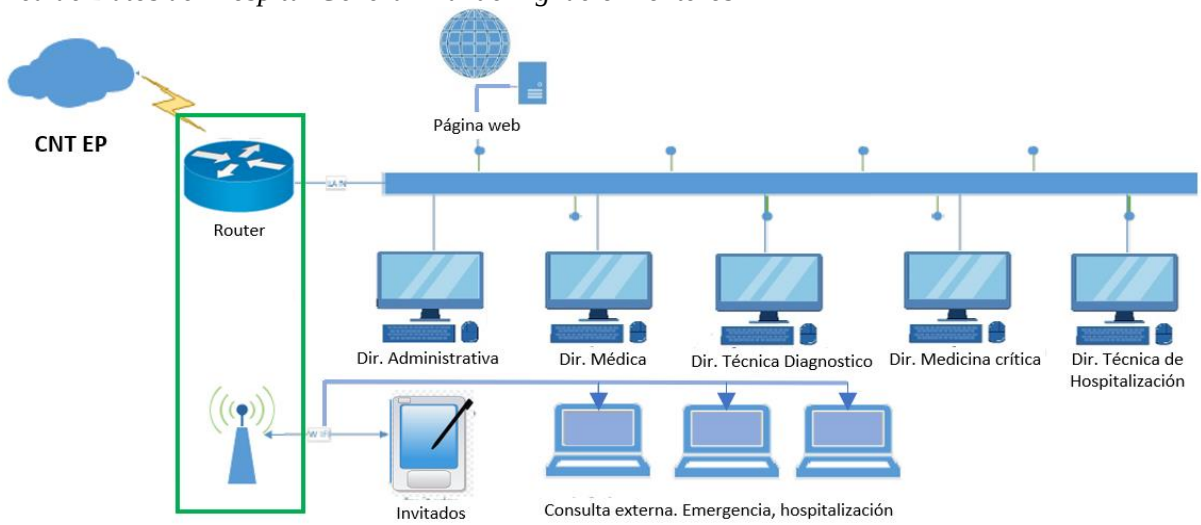
En la actualidad el HGMYM carece de políticas o guías para cumplir con la seguridad de la información del paciente en el sistema MIS-AS400, basado en el cumplimiento del marco normativo y regulatorio aplicable a la gestión de la seguridad de la información en el sector de la salud.

6.3.1. Red de Datos

El proveedor de servicios de comunicaciones Corporación Nacional de Telecomunicaciones CNT EP controla la red de datos del HGMYM, que tiene una velocidad de 40 Mbps. La infraestructura incluye un router, un conversor de fibra óptica proporcionado por el proveedor, un switch, servidores, un firewall y computadoras. El diagrama actual de la red de datos del Hospital se presenta en la Figura 6.

Figura 6

Red de Datos del Hospital General Manuel Ygnacio Monteros



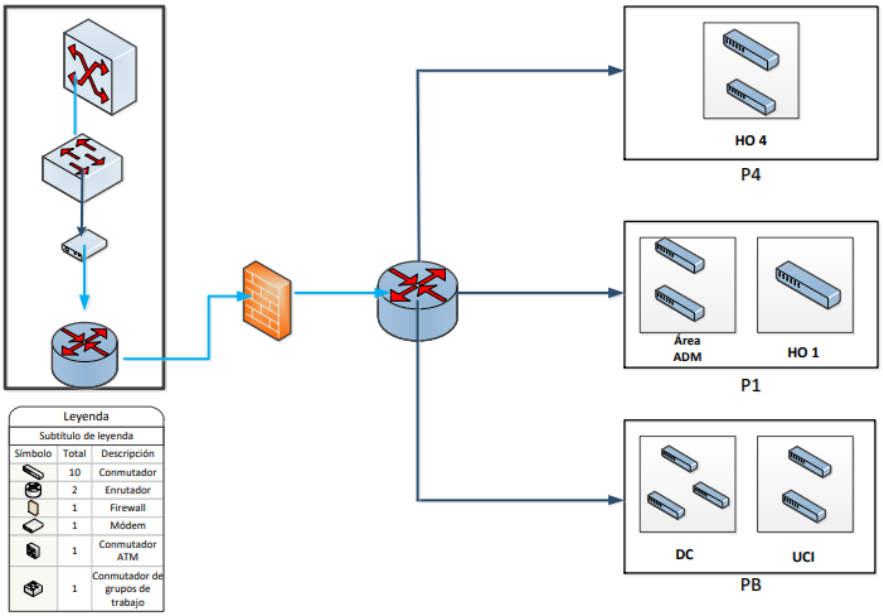
Fuente: El Autor

6.3.2. Topología de la red

El HGMYM cuenta con una estructura de red lineal, que abarca desde la conexión a un servicio de datos, un firewall, un equipo de enrutamiento, un controlador de redes inalámbricas, servidores de correo, sistemas médicos entre otros. Además, posee una topología de red jerárquica, tal como se muestra en la figura 7 un bosquejo de la red en general y del área de Tecnologías en la figura 8.

Figura 7

Bosquejo de la red del Hospital General Manuel Ygnacio Monteros

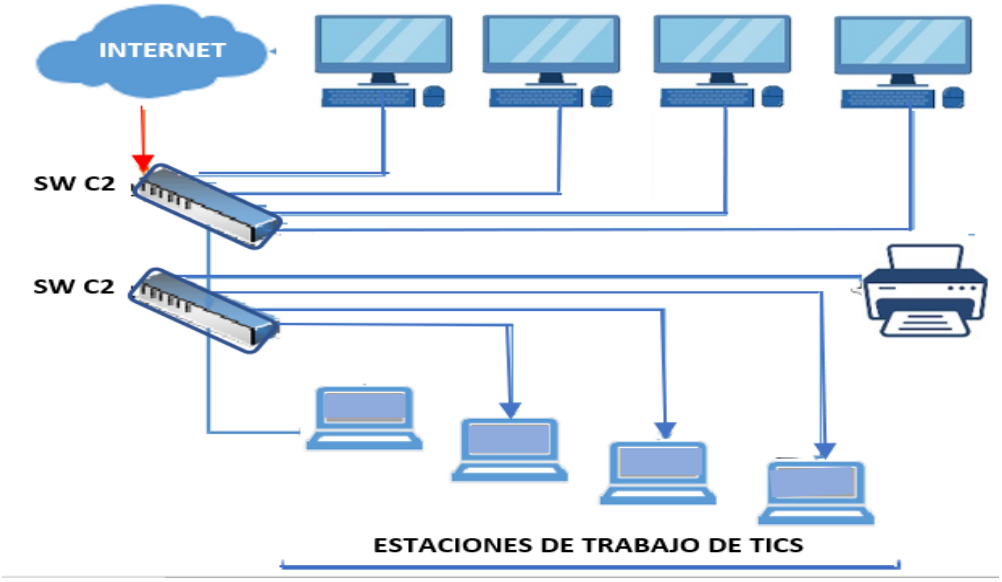


Fuente: El Autor

El área de estudio se encuentra en la primera planta y posee la siguiente topología de infraestructura:

Figura **8**

Topología de red del Área de Tecnología



Fuente: El Autor

6.3.3. Personal del Área

El área de Tecnologías de la Información se encuentra conformada por cuatro personas que desempeñan las diferentes actividades del área las mismas que se detallan en la Tabla 4

Tabla 4

Actividades Personal Área de Tecnologías

DENOMINACIÓN	ACTIVIDADES
Tecnólogo Informático 1	Brindar Soporte Técnico (hardware, software) a plataformas gubernamentales, Sistema MIS AS400, e infraestructura tecnológica (computadores, impresoras, equipos networking)
Tecnólogo Informático 2	Desinstalación, Instalación y configuración de equipos informáticos (PC)
Tecnólogo Informático 3	Parametrizaciones en el sistema MIS AS400 (creación/inactivación de usuarios, dependencias, bodegas, kárdex y otros parámetros).
Tecnólogo Informático 4	Depuración, regularización y ajuste de las bodegas, usuarios; Parametrización de dependencias, procedimientos en base al Tarifario de Prestaciones para el Sistema Nacional de Salud y cartera de servicios de nuestra unidad médica

Fuente: El Autor

6.3.4. Equipos de Computación

A nivel de equipos el Hospital General Manuel Ygnacio Monteros cuenta con el siguiente número de estaciones de trabajo en cada una de las áreas de la unidad médica, conforme se muestra en la Tabla 5

Tabla 5

Estaciones de trabajo de las Áreas del Hospital General Manuel Ygnacio Monteros

Tabla Estaciones de Trabajo				
Nro.	**Nombre del área**	**Computadores**	**Portátil**	**Total**
1	Dirección Administrativa	3	1	4
2	Jefatura Financiera	10	1	11
3	Talento Humano	6	1	7
4	Planificación y Estadística	4	1	5
5	Bodega General	6		6
6	Jurídico	2	1	3
7	Adquisiciones	6	1	7
8	Servicios Generales	6		6
9	Lavandería	2		2
10	Dietética	4		4
11	Transporte	4		4
12	Limpieza	2		2
13	Mantenimiento	10		10
14	Unidad de Comunicación	1		1
15	Unidad de Activos Fijos	2	1	3
16	Unidad de TICS	4	3	7
17	Unidad de Calidad	2		2
18	Dispositivos Médicos	6		6
19	Auditoría Médica	8		8
20	Epidemiología	5		5
21	Gestión de Riesgos	6	2	8
22	Unidad de Servicio al Asegurado	8		8
23	Dirección Médica	2	1	3
24	Farmacia	12	1	13
25	Dirección Técnica de Diagnóstico	2		2
26	Departamento de Imagen	13		13
27	Departamento de Laboratorio Clínico	7		7
28	Patología	6		6
29	Banco de Sangre	3		3
30	Dirección Técnica de Hospitalización	2		2
31	Consulta Externa	46		46
32	Hospitalización	28	5	33
33	Endoscopia	5		5
34	Biológicos	7	1	8
35	Fisiatría y Rehabilitación	4		4
36	Hospitalización Covid	12		12
37	Dirección Técnica de Medicina Crítica.	1		1
38	Emergencia Alterna y Emergencia	30	2	32
39	Servicio de Terapia Intensiva	19		19
40	Centro Quirúrgico	11	8	19
41	Jefatura de Enfermería	20		20
	TOTAL DE EQUIPOS		**337**	**30**

En la Figura 9 se muestra los equipos de computación Todo en Uno con los que cuenta el área de TI deL HGMYM

Figura 9

Computadoras Todo en Uno del HGMYM

Fuente: El Autor

En la Tabla 6 se detallan las características de los equipos de computación todo en uno.

Tabla 6

Características Computadoras Todo en Uno

Computador Todo en Uno Gama Media	
Marca	LENOVO
Modelo	400G6PO AiO NT i5-10500 8GB/512GB PC
Formato	Todo en Uno
Procesador	i5-10500T Décima Generación, Frecuencia base: 2.30GHz, Frecuenciaturbo máxima: 3.80GHz, 6 núcleos, 12 MB
Chipset	B460
Seguridad - Protección de Datos	TPM 2.0
Memoria RAM	16GB (1x16GB) DDR4 2666MHz.
Slot de memoria	2 slots que soportan como mínimo 32GB cada uno.
Disco duro interno	1TB o superior
Interfaz del dico duro	SATA
Velocidad rotacional disco duro	7200 rpm
Soporte para 64 bits	Soporta 64 bits
Tarjeta gráfica	Integrada
Inalámbrico	Wireless Dual-band 2x2 802.11ac Wi-Fi con Bluetooth 5.0 o superior

Puertos	3 USB 3.2 o de velocidad superior.1 USB 3.2 Tipo-C. 2 USB 2.0.1 RJ-45. 1 Display Port. 1 Conector de audio universal. 1 SD Slot.
Audio	Si, integrado
Cámara	Webcam, integrada
Puertos de Expansión	2 conectores M.2 (1 para disco sólido y 1 Wi-Fi)
Tarjeta de red	Gigabit Ethernet 10/100/1000, integrada

Fuente: El Autor

En la Figura 10 se muestra los equipos de computación portátil con los que cuenta el área de TI del HGMYM

Figura 10

Computadoras Portátiles del área de TI del HGMYM

Fuente: El Autor

En la Tabla 7 se detallan las especificaciones técnicas de los equipos de computación portátiles.

Tabla 7

Características Computadoras Portátiles

	Computador Portátil Gama Media
Marca	DELL
Modelo	PB440G8 i5-1135G7 14 8GB/512 PC
Formato	Portátil
Chasis	certificación MIL-STD-810G
Procesador	i5-10210U Décima generación, Frecuencia base: 1.60 GHz, Frecuencia turbo máxima: 4.20 GHz, 4 núcleos, 6 MB

Chipset	Integrado al procesador
Chip de seguridad	TPM 2.0
Disco Duro Interno	512 GB
Tipo de Disco Duro	SSD (Solid State) PCIe NVMe
Memoria RAM	8GB (1x8GB) 2666MHz
Slot de memoria	2 slots que soporten como mínimo 16GB cada uno.
Tipo de memoria	DDR4
Tarjeta de video	Integrada
Pantalla	Antirreflejo Led HD
Tamaño de pantalla	Mínima 14" pulgadas
Peso	Máximo hasta 1.7 Kg.
Conectividad	Wireless Dual Band 802.11ac (2x2) o superior. Bluetooth 5.0 incorporado o superior. Gigabit Ethernet 10/100/1000 Mbps o superior
Audio	Integrado
Puertos	2 USB 3.1 o de velocidad superior. 1 USB Tipo-C. 1 USB 2.0 o de velocidad superior. 1 RJ-45. 1 HDMI. 1 conector de audio universal.
Soporte 64 bits	Soporta 64 bits
Teclado	Español, sin teclado numérico
Unidad Óptica	Si, Lector/Quemador de DVD's y CD's integrada
Cargador	Si
Batería	Si, 40Whr
Mouse Óptico	Si, mouse USB
Adicionales	Mchila y candado de seguridad
Sistema Operativo	Windows 10 Profesional de 64 bits respectivamente licenciado y en idioma español o superior
Controlador de hardware	Si, Compatible con Windows 10 o superior; y, GNU\Linux compatible con todos los componentes de hardware.

Fuente: El Autor

6.3.5. Servidor

En la Figura 11 se observa el Rack principal donde se aloja el servidor, el mismo que permite almacenamiento y gestión de datos, aplicaciones, servicios y recursos en el HGMYM

- Equipo marca DELL Intel® Xeon® ampliables de 2.ª generación
- Memoria Velocidad DIMM Hasta 2933 MT/s
- 48 ranuras para DIMM DDR4 (12 ranuras para NVDIMM o 24 ranuras solo para DCPMM)

Figura 11
Servidor de red del HGMYM

Fuente: Referencia del equipo del HGMYM tomada de DELL Technologies

6.3.6. Switch

El HGMYM cuenta con 2 Switch principal 48 POE+, 4 fibras 10 Gbps, 8 Switch acceso 48 POE+ 740W y 23 Acces Point marca Aruba, modelo 535. La figura 12 muestra el modelo de switch con los que cuenta el HGMYM.

Figura 12
Modelo de switch del HGMYM

Fuente: El Autor

La Figura 13 muestra el modelo de Acces Point ubicados en diferentes sitios de la Unidad Médica.

Figura 13
Acces Point Aruba

Fuente: El Autor

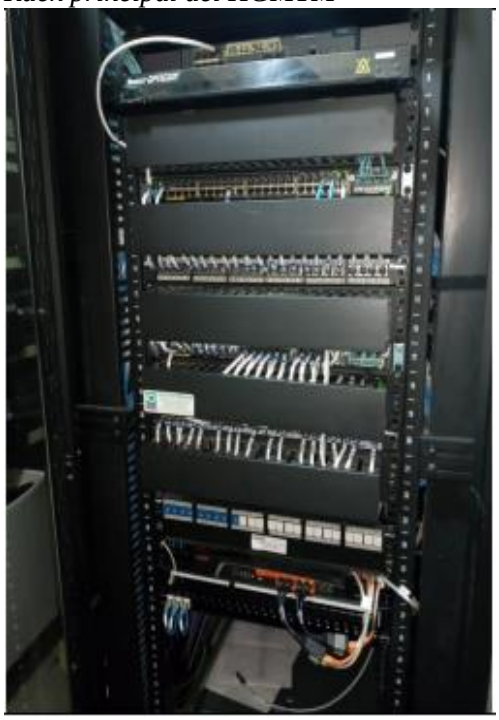
6.3.7. Seguridad Física

El centro de datos del HGMYM es de fácil acceso debido a que la seguridad únicamente depende de una llave de la puerta de ingreso. La figura 14 muestra el acceso al centro de datos y en la Figura 15 el rack principal.

Figura 14
Entrada al Centro de Datos

Fuente: El Autor

Figura 15
Rack principal del HGMYM



Fuente: El Autor

6.3.8. Aplicaciones

El HGMYM emplea diversas aplicaciones para llevar a cabo la gestión de sus operaciones relacionadas con los servicios médicos. En la Tabla 8 se detallan las diferentes aplicaciones utilizadas para facilitar la prestación de dichos servicios.

Tabla 8
Aplicaciones utilizadas en el Hospital

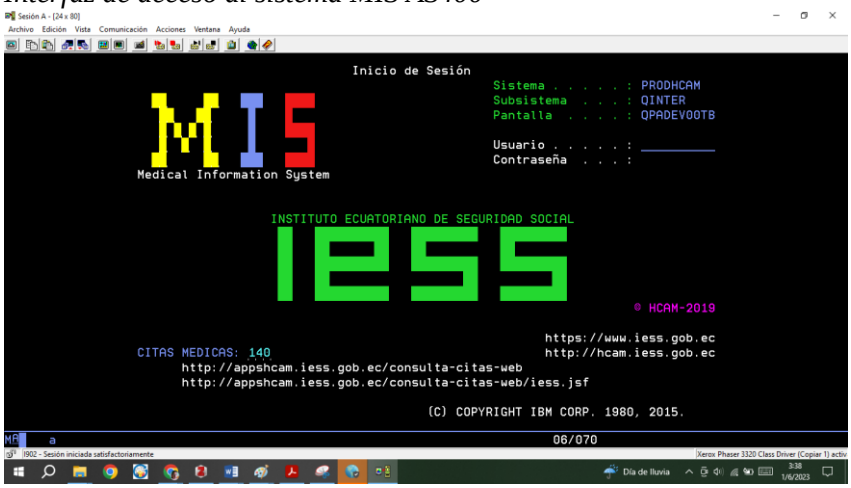
Aplicación	Tipo de aplicación	Comentarios
Paquete de Office	Paquete de office herramienta de ofimática	
Microsoft Windows	Sistema Operativo	
Microsoft Windows server	Sistema Operativo	Servidor
Firefox (Mozilla), Google Chrome, Internet Explorer	Navegador web	
Eset nod32	Programa antivirus	
MIS AS400	Sistema de gestión médica	
Sistema de Gestión Documental	Plataformas Gubernamentales	
Correo Institucional		

Fuente: El Autor

6.3.9. Acceso al sistema MIS AS400

El sistema MIS AS400 del IESS está sujeto a las políticas y configuraciones implementadas por la institución, en el HGMYM el acceso a este sistema se lo realiza a través de un usuario y contraseña proporcionado por el área de TI de acuerdo al rol del usuario. La figura 16 muestra la interfaz de acceso al sistema MIS AS400.

Figura 16
Interfaz de acceso al sistema MIS AS400



Fuente: El Autor

6.4. Identificación de activos

Para la identificación de los activos de información en el área de Tecnologías del HGMYM se consideró tanto los activos primarios como los activos de soporte. A continuación, se presenta la clasificación de los diferentes tipos de activos:

- Activos Primarios
    - Servicios Médicos
    - Información / Datos
- Activos de Soporte
    - Redes de Comunicaciones
    - Hardware
    - Software
    - Personas
    - Sitio/Instalaciones

6.5. Identificación de Riesgos

En este apartado se presenta los riesgos que pueden surgir en la seguridad de la información en el área de TI del HGMYM.

Como primer paso se realizó la identificación de los riesgos a partir del análisis de aquellas tareas que pueden resultar vulnerables y las consecuencias de los mismos. A continuación, la Tabla 9 describe los riesgos identificados.

Tabla 9

Riesgos identificados del Sistema de gestión Médica

Riesgo	Amenaza	Consecuencia	Principio de Seguridad Afectado
R01	Falta de personal cualificado para la administración del sistema MIS AS400	Se retrasan las actividades, no se da atención a los requerimientos de usuarios por desconocimiento del sistema. O se realiza mal las parametrizaciones de los servicios generando pérdida económica y afectación en la facturación del hospital.	Integridad Confidencialidad Disponibilidad
R02	Se pierde información por daños en el hardware o software.	Hay un retraso en el cumplimiento de los diferentes requerimientos, no se tiene acceso a la información de registros médicos y demás opciones del sistema.	Disponibilidad Integridad
R03	Poco o ningún conocimiento acerca del sistema de gestión médica MIS AS400.	Los requerimientos pueden ser mal interpretados lo que traería un mal diseño de la solución.	Integridad Confidencialidad

			Disponibilidad
Riesgo	**Amenaza**	**Consecuencia**	**Principio de Seguridad Afectado**
R04	Ataques de malware, virus y phishing	Afectan el funcionamiento del computador y del sistema de gestión médica.	Integridad Confidencialidad Disponibilidad
R05	Interrupción o degradación de los sistemas de información críticos para la atención médica	Indisponibilidad del sistema MIS AS400 para realizar la atención médica de manera oportuna y la atención a los requerimientos de los diferentes usuarios.	Disponibilidad
R06	Problemas de enfermedad de un integrante que forma parte del área de tecnologías.	Traería cambios en la planificación de las actividades, asignación de funciones al personal, reorganizar tareas dentro del área, esto conlleva tiempo.	Disponibilidad
R07	Errores humanos y fallas en la gestión de datos médicos.	La información no es real, datos no coinciden con el registro médico del paciente. No existe coherencia.	Integridad Confidencialidad Disponibilidad
R08	Pérdida o robo de dispositivos de almacenamiento de datos que contienen información médica	Divulgación de información reservada, uso mal intencionado de la información.	Integridad Confidencialidad Disponibilidad
R09	Acceso no autorizado a información médica confidencial	Accesos indebidos al sistema de gestión médica.	Integridad Confidencialidad

Fuente: El Autor

6.6. Mitigación de riesgos

La Tabla 10 muestra el plan de mitigación para cada riesgo identificado, así como el nivel de prioridad basado en el análisis conjunto de probabilidad e impacto.

Tabla 10

Plan de Mitigación de riesgos

Riesgo	Amenaza	Mitigación	Probabilidad	Impacto	Prioridad
R01	Falta de personal cualificado para la administración del sistema MIS AS400	Tener una definición clara de los perfiles solicitados y realizar tareas de divulgación y capacitación del manejo del sistema MIS AS400.	Baja (B)	Media (M)	Baja (B)
R02	Se pierde información por daños en el hardware o software.	Se deben efectuar respaldos de forma periódica y se deben	Muy Baja (MB)	Alto (A)	Baja (B)

		tener en cuenta los aspectos definidos en los planes de seguridad de la información.			
R03	Poco o ningún conocimiento acerca del sistema de gestión médica MIS AS400.	Realizar capacitaciones y facilitar información, manuales del sistema MIS AS400. Se realizarán reuniones de aclaración de dudas y se les asignará un personal con conocimientos en el tema.	Media (M)	Alto (A)	Alta (AP)
R04	Ataques de malware, virus y phishing	Se debe contar con antivirus, herramientas de protección que buscan y detectan virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir los ataques.	Media (M)	Alto (A)	Alta (AP)
R05	Interrupción o degradación de los sistemas de información críticos para la atención médica	Contar con un plan de contingencia, dar previo aviso a las interrupciones planificadas por los mantenimientos preventivos y correctivos.	Media (M)	Alto (A)	Alta (AP)
R06	Problemas de enfermedad de un integrante que forma parte del área de tecnologías.	Mantener toda la información que realicen los miembros del equipo en el repositorio, actualizada y debidamente comentada; de forma tal que se pueda acceder a ella. Trabajo en equipo que permita la transferencia de conocimiento.	Media (M)	Alto (A)	Alta (AP)
R07	Errores humanos y fallas en la gestión de datos médicos.	Realizar constantemente capacitaciones a los integrantes del área de tecnologías.	Media (M)	Alto (A)	Alta (AP)
R08	Pérdida o robo de dispositivos de almacenamiento de datos que contienen información médica	El departamento de tecnologías será responsable de custodiar los dispositivos de almacenamiento que contienen información médica.	Baja (B)	Alto (A)	Media (PM)
R09	Acceso no autorizado a información médica confidencial	Asegurar acciones encaminadas a proteger la información de los pacientes y el personal frente a cualquier tipo de amenaza, manteniendo intacta la confidencialidad,	Alta (A)	Alto (A)	Muy alta (MAP)

	integridad y disponibilidad de los datos.	

Fuente: El Autor

6.7. Medidas a tomar

En este apartado se citan los diferentes tipos de protocolos que se pueden usar dentro del HGMYM, tomando en consideración sus activos y la eficacia del protocolo. Por lo tanto, una vez identificados los riesgos a los que se encuentra expuesto la información en el área de TI del HGMYM se ha hecho uso de controles de la información basados en la norma ISO 27799:2008 y sus características, los mismos que se detallan en la tabla 11

Tabla 11

Resumen de la aplicación del control de Seguridad de Información

Sección y medidas de control	Características	
	Responsable	**Fecha de implantación**
5. Políticas de seguridad de la información	Directivos del hospital	Implementada
	Directivos del hospital	Mayo-2023
6. Organización de la seguridad de la información	Departamento de talento humano	Implementada
	Departamento de talento humano	Junio-2023
	Departamento de TI	Junio-2023
7. Seguridad de los recursos humanos	Departamento de talento humano	Mayo-2023
	Departamento de talento humano	Mayo-2023
	Departamento de talento humano	Junio-2023
	Departamento de TI	Junio-2023
	Departamento de talento humano	Junio-2023
	Departamento de TI	Mayo-2023
8 Gestión de activos	Departamento de TI	Implementada
	Departamento de TI	Implementada
	Departamento de TI	Mayo-2023
	Departamento de TI	Junio-2023
	Departamento de TI	Junio-2023
	Departamento de TI	Mayo 2023
	Departamento de TI	Julio 2023
	Departamento de TI	Julio 2023
9 Control de acceso	Departamento de TI	Agosto-2023
	Departamento de TI	Agosto-2023
	Departamento de TI	Agosto-2023
	Departamento de TI	Agosto-2023
	Departamento de TI	Agosto-2023
	Departamento de TI	Agosto-2023
	Departamento de TI	Agosto-2023
	Departamento de TI	Agosto-2023

	Departamento de TI	Agosto-2023
10 Criptografía	Departamento de TI	Septiembre-2023
	Departamento de TI	Octubre-2023
11 Seguridad física y del entorno	Departamento de TI	Mayo-2023
	Departamento de TI	Octubre-2023
	Departamento de TI	Octubre-2023
	Departamento de TI	Implementada
	Departamento de TI	Implementada
	Departamento de TI	Mayo-2023
	Departamento de TI	Mayo-2023
	Departamento de TI	Octubre -2023
	Departamento de TI	Junio-2023
12 Seguridad de las operaciones	Departamento de TI	Septiembre-2023
	Departamento de TI	Septiembre-2023
	Departamento de TI	Septiembre-2023
	Departamento de TI	Septiembre-2023
13 Seguridad de las comunicaciones	Departamento de TI	Septiembre-2023
	Departamento de TI	Septiembre-2023
	Departamento de TI	Septiembre-2023
	Departamento de TI	Septiembre-2023
	Departamento de TI	Septiembre-2023
	Departamento de TI	Septiembre-2023
14 Adquisición, desarrollo y mantenimiento de los sistemas de información	Departamento de TI	Septiembre-2023
	Departamento de TI	Septiembre-2023
	Departamento de TI	Septiembre-2023
16 Gestión de incidentes de seguridad de la información	Departamento de TI	Agosto-2023
18 Cumplimiento	Departamento de talento humano	Mayo-2023

Fuente: El Autor

En la tabla 11 se muestra el resumen de la situación actual y la aplicación del control de seguridad de la información, se la puede visualizar completa en el Anexo 1

A continuación, en la Tabla de 12 se describen las políticas de seguridad de la información adoptadas para la presente propuesta de investigación.

Tabla 12
Medidas a tomar de las políticas de seguridad de la información

CONTROL ISO 27799:2008	Control
5. Políticas de seguridad de la información	
5.1. Directrices de gestión para la seguridad de la información	
5.1.1 Políticas de seguridad de la información	Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
5.1.2 Revisión de las políticas de seguridad de la información	Las políticas de seguridad de la información deberían revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
6. Organización de la seguridad de la información	
6.1 Organización interna	
6.1.1 Roles y responsabilidades de seguridad de la información	Todas las responsabilidades en seguridad de la información deberían definirse y asignarse.
6.1.2 Segregación de funciones	Las funciones y áreas de responsabilidad deberían segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.
6.1.3 Contacto con las autoridades	Deberían mantenerse los contactos apropiados con las autoridades relevantes.
7. Seguridad de los recursos humanos	
7.1 Antes del empleo	
7.1.1 Investigación de antecedentes	La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debería llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debería ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.
7.1.2 Términos y condiciones de empleo	Cómo parte de sus obligaciones contractuales, los empleados y contratistas deberían establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.
7.2 Durante el empleo	

7.2.1 Responsabilidades de la dirección	La dirección debería exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.
7.2.2 Concientización, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deberían recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
7.2.3 Proceso disciplinario	Debería existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.

7.3 Terminación y cambio de empleo

7.3.1 Responsabilidades ante la finalización o cambio	Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deberían definir, comunicar al empleado o contratista y se deberían cumplir

8 Gestión de activos

8.1 Responsabilidad por los bienes

8.1.1 Inventario de activos	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deberían estar claramente identificados y debería elaborarse y mantenerse un inventario.
8.1.2 Propiedad de los activos	Todos los activos que figuran en el inventario deberían tener un propietario.
8.1.3 Uso aceptable de los activos	Se deberían identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.
8.1.4 Devolución de activos	Todos los empleados y terceras partes deberían devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

8.2 Clasificación de la información

8.2.1 Clasificación de la información	La información debería ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.
8.2.2 Etiquetado de la información	Debería desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

8.3 Manipulación de los soportes

8.3.1 Gestión de soportes extraíbles	Se deberían implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
8.3.3 Soportes físicos en tránsito	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro.

9 Control de acceso

9.1 Requisitos de negocio para el control de acceso

9.1.1 Política de control de acceso	Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
9.1.2 Acceso a las redes y a los servicios de red	Únicamente se debería proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.

9.2 Gestión de acceso de usuario

9.2.1 Registro y baja de usuario	Debería implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
9.2.2 Provisión de acceso de usuario	Debería implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
9.2.3 Gestión de privilegios de acceso	La asignación y el uso de privilegios de acceso debería estar restringida y controlada.
9.2.6 Retirada o reasignación de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deberían ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.

9.3 Responsabilidades del usuario

9.3.1 Uso de la información secreta de autenticación	Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación

9.4 Control de acceso a sistemas y aplicaciones

9.4.1 Restricción del acceso a la información	Se debería restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
9.4.3 Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deberían ser interactivos y establecer contraseñas seguras y robustas.

10 Criptografía

10.1 Controles criptográficos

10.1.2 Gestión de claves	Se debería desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

11 Seguridad física y del entorno

11.1 Áreas seguras

11.1.1 Perímetro de seguridad física	Se deberían utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.
11.1.2 Controles físicos de entrada	Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
11.1.6 Áreas de carga y descarga	Deberían controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.

11.2 Seguridad de los equipos

11.2.1 Emplazamiento y protección de equipos	Los equipos deberían situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.
11.2.3 Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debería estar protegido frente a interceptaciones, interferencias o daños.
11.2.4 Mantenimiento de los equipos	Los equipos deberían recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas
11.2.5 Retirada de materiales propiedad de la empresa	Sin autorización previa, los equipos, la información o el software no deberían sacarse de las instalaciones.
11.2.6 Seguridad de los equipos fuera de las instalaciones	Deberían aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.

11.2.7 Reutilización o eliminación segura de equipos	Todos los soportes de almacenamiento deberían ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Los usuarios deberían asegurarse que el equipo desatendido tiene la protección adecuada.

12 Seguridad de las operaciones

12.1 Procedimientos y responsabilidades operacionales

12.1.2 Gestión de cambios	Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deberían ser controlados.

12.2 Protección contra el software malicioso (malware)

12.2.1 Controles contra el código malicioso	Se deberían implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.

12.3 Copias de seguridad

12.3.1 Copias de seguridad de la información	Se deberían realizar copias de seguridad de la información, del software y del sistema y se deberían verificar periódicamente de acuerdo a la política de copias de seguridad acordada.

12.5 Control del software en explotación

12.5.1 Instalación del software en explotación	Se deberían implementar procedimientos para controlar la instalación del software en explotación.

13 Seguridad de las comunicaciones

13.1 Gestión de la seguridad de redes

13.1.1 Controles de red	Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
13.1.2 Seguridad de los servicios de red	Se deberían identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deberían incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
13.1.3 Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deberían estar segregados en redes distintas

13.2 Intercambio de información

13.2.1 Políticas y procedimientos de intercambio de información	Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.
13.2.3 Mensajería electrónica	La información que sea objeto de mensajería electrónica debería estar adecuadamente protegida.
13.2.4 Acuerdos de confidencialidad o no revelación	Deberían identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.
14 Adquisición, desarrollo y mantenimiento de los sistemas de información	
14.1 Requisitos de seguridad en los sistemas de información	
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Los requisitos relacionados con la seguridad de la información deberían incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes
14.2 Seguridad en el desarrollo y en los procesos de soporte	
14.2.1 Política de desarrollo seguro	Se deberían establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.
14.2.2 Procedimiento de control de cambios en sistemas	La implantación de cambios a lo largo del ciclo de vida del desarrollo debería controlarse mediante el uso de procedimientos formales de control de cambios.
16 Gestión de incidentes de seguridad de la información	
16.1 Gestión de incidentes de seguridad de la información y mejoras	
16.1.1 Responsabilidades y procedimientos	Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
18 Cumplimiento	
18.1 Cumplimiento de los requisitos legales y contractuales	
18.1.4 Protección y privacidad de la información de carácter personal	Debería garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.

Fuente: (UNE-EN ISO/IEC 27002:2017, 2017)

6.8. Diseño y propuesta del modelo de gestión de seguridad de la información

Para asegurar la protección de la información y la confianza de los pacientes y otros actores del sistema de salud se propone un modelo de gestión de seguridad de la información, donde se establecen políticas, lineamientos, reglas y directrices que deben seguirse para garantizar el uso adecuado de información que se maneja en el área de TI del HGMYM.

6.8.1. Gestión de activos del HGMYM

6.8.1.1. Inventario de activos de información Una vez identificados los activos de información, ubicación, características y su importancia en términos de confidencialidad, integridad y disponibilidad dentro del Hospital, se procedió a levantar un inventario de los activos más relevantes con el propósito de gestionar adecuadamente su seguridad y protección.

6.8.1.2. Propiedad de los Activos Los custodios de la información son aquellos que por la naturaleza de su cargo en la organización deben custodiar, respaldar o almacenar la información. Se convierten en custodios el personal que tenga acceso a bases de información. Entre sus responsabilidades constan:

- El manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso
- Mantener la disponibilidad e integridad de la información custodiada
- Mantener el acceso y permisos de acceso a la información custodiada
- Brindar soporte para evaluar e identificar la información para su clasificación.

El área de Tecnologías de la Información de la unidad médica serán los responsables de los activos tecnológicos bajo su custodia, y los responsables de la seguridad de la información serán cada una de las dependencias de la unidad médica.

Los responsables de la información son definidos para asegurar adecuadamente la pertenencia, custodia y salvaguarda de los activos de la información, teniendo en cuenta una correcta separación de funciones que se diferencia entre:

Responsables Directos: Los responsables directos de la información son aquellos que por naturaleza de su posición en la Institución conocen el tipo de información que se genera o comunica o ingresen en los diversos sistemas o aplicativos, los mismos que son responsables de:

- La clasificación de la información, de la organización y autorización del acceso a la información.
- Manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.
- Monitoreo del uso de la información por parte de personal a su cargo
- Asignar a los responsables del uso y manejo de la información.

Responsables Secundarios: Los responsables secundarios de la información son aquellos que por la naturaleza de su cargo en la organización deben acceder, modificar o almacenar información. Son responsables de:

- Manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.

6.8.2. Políticas de seguridad de uso de seguridad informática y de la información

6.8.2.1. Lineamientos Generales Las y los usuarios internos cumplirán las siguientes recomendaciones:

- El equipo informático debe estar configurado para que se bloquee automáticamente, cuando se detecte inactividad a un tiempo determinado, es responsabilidad del usuario interno el bloquear su equipo de trabajo cuando este abandone su lugar de trabajo.
- No modificar las configuraciones de direcciones IP, DNS, hora, nombre de equipos y demás. En caso de requerir un cambio deberá notificar a los técnicos informáticos de la institución.
- Todo el personal de la Unidad Médica, de acuerdo a su competencia deberá cumplir los lineamientos y directrices de seguridad informática emitidos por la DNTI y bajo el amparo de seguridad de la información de la Dirección Nacional de Riesgos Institucionales.

6.8.2.2. Compromiso de Confidencialidad Las y los servidores de la institución deberán firmar compromisos de confidencialidad y de no divulgación de información. El personal de Talento Humano será el encargado de controlar que los permisos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción, gestionar la custodia de los compromisos firmados, en los expedientes , físicos o electrónicos, de cada funcionario y/o servidor, y controlar que la firma de los compromisos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios y/o servidores a la institución, sin excepción.

6.8.2.3. Clasificación de la información Los responsables directos de la información deberán clasificar adecuadamente la información que manejan y deben asegurarse de que se respete el acceso a la misma por parte del personal a su cargo.

6.8.2.4. Almacenamiento La información obtenida de cualquiera de los servicios y que sea almacenada localmente en el equipo de cómputo del usuario y de propiedad institucional no podrá ser distribuida o transmitida por la red institucional o por otros medios de comunicación sin la autorización del inmediato superior.

6.8.2.5. Transmisión de datos Al fin de garantizar la integridad y confidencialidad de la información obtenida de los sistemas y aplicativos informáticos de la institución y en razón de que los dispositivos móviles, magnéticos y los soportes extraíbles generan vulnerabilidades como divulgación no autorizada de datos, robo de datos, datos dañados o comprometidos por la facilidad de uso, alta movilidad y capacidad de almacenamiento.

6.8.3. Disposiciones generales para la administración del sistema MIS AS400 para el HGMYM

- Los Servidores que dan atención y soporte dentro del Sistema MIS-AS400 del IESS relacionados con la ejecución de este procedimiento, deberán aplicarlo y cumplirlo de manera obligatoria.
- Las solicitudes de requerimientos deberán apegarse a los formatos establecidos por el área de TI para la aplicación del presente procedimiento.
- El equipo de trabajo técnico que brinda atención y soporte dentro del Sistema MIS-AS400, una vez atendida la solicitud deberá notificar a la unidad requirente y dar por cerrado el requerimiento.
- Toda actividad relacionada a la administración del Sistema MIS-AS400 deberá estar enmarcado a los roles y responsabilidades dentro del ámbito de competencias del equipo de trabajo tecnológico.
- Conforme el tipo de necesidad registrada, se debe validar que la documentación habilitante se encuentre completa y debidamente formalizada previo a su atención. En caso de que la documentación habilitante no se encuentre completa y/o debidamente formalizada se devolverá a la unidad requirente para la debida corrección.

6.8.3.1. Lineamientos de seguridad informática La tabla 13 se detalla cada uno de los lineamientos de seguridad informática con su respectiva descripción.

Tabla 13
Lineamientos de Seguridad Informática

Lineamiento	Descripción
Lineamiento de Seguridad Informática Control de Accesos Lógicos, al Software Base, de las Plataformas Administradas por el área de Tecnologías de la Información	Apoya en el manejo de controles de acceso dentro del Sistema MIS AS400, considerando tipo de cuentas de los usuarios y contraseñas.
Lineamiento de Seguridad Informática «Para la Evaluación de Controles de Seguridad Informática»	Verifica el nivel de seguridad en base a un Check List de información, el no cumplir con este listado al 100 % no es un limitante de uso del sistema, sin embargo es un detonante para la implementación de un plan de mejora y generación de lineamiento alternos al AS400, protegiendo así el acceso a la aplicación.
Lineamiento de Seguridad Informática «Para respaldo y/o restauración de la Información digital»	Generación de respaldos de acuerdo con las necesidades que maneja el negocio de salud en la plataforma de información médica MIS AS400, la cual ejecuta acciones de mantenimiento y almacenamiento de información
Lineamiento de Seguridad Para Bloqueo de Usuarios de Aplicativos Informáticos.	Generación de bloqueos por intento de ingresos, dentro de la AS400 por tres intentos de acceso se bloquea el usuario, así como por el no uso consecutivo del mismo.
Lineamiento de seguridad informática «Para gestión de pistas de auditoría»	Dentro del sistema de gestión médica MIS-AS400, se generan pista de auditoria del ingreso de los usuarios a los distintos servicios, lo que proporciona la trazabilidad de accesos y manejo de información.

Fuente: El Autor

6.8.3.2. Lineamientos generales para la administración y gestión del Sistema MIS AS400

- La administración y control técnico de la plataforma del Sistema MIS-AS400, se encuentran bajo responsabilidad de la unidad de tecnologías de la información y comunicación del HGMYM y en caso de necesitar apoyo se escala el requerimiento a la Dirección Nacional de Tecnologías de la Información.
- Para la gestión de requerimientos a nivel de atención técnica, se deberá contar con segregaciones de funciones a nivel de administración del Sistema MIS-AS400 y contar con los siguientes perfiles tal como se muestra en la Tabla 14

Tabla 14

Lineamientos para administración y control del sistema MIS AS400

ACTOR	PERFIL MIS-AS400	DETALLE
Técnico de soporte – Nivel I	Administrador Local UM – AS400	Persona encargada de atender/solventar requerimientos a nivel únicamente de Establecimientos de Salud.
Técnico de soporte –	Administrador Nacional – AS400	Persona encargada de atender requerimientos provenientes de Establecimientos de Salud, Coordinaciones
Técnico de soporte – Nivel III	Técnico Nacional – AS400	Persona especializada encargada de atender requerimientos de mejoras en aplicativo y actualización de información, definición de lineamientos, definición de mecanismos.

Fuente: El Autor

- Cada año durante el mes de enero expirarán las claves de los administradores del MIS-AS400 a nivel nacional, y se entregarán las nuevas claves durante febrero del año en curso, para lo cual se deberá entregar previamente el «Compromiso de confidencialidad de la información» debidamente formalizados en el área de tecnologías del hospital y enviados a la Subdirección Nacional de Seguridad Informática.
- La creación de perfiles y permisos de usuarios para el MIS-AS400, solicitados por las unidades requirentes, serán creados previa firma del «Compromiso de confidencialidad de la información» y el formulario de administración de usuarios, además estará supervisado por el área de tecnologías del hospital y enviados a la Subdirección Nacional de Seguridad Informática.
- No deberá existir más de 2 usuarios (principal y backup) con perfil de Administrador del Sistema MIS-AS400 en el HGMYM, a menos que sea autorizado por la máxima autoridad del HGMYM.
- Los roles del Sistema MIS-AS400 del personal administrativo y médico del HGMYM, (Bodega, Farmacia, Admisión, Médico, Enfermera, Facturación, Imagen, etc.), serán entregados y actualizados bajo un lineamiento definido por la Dirección del Seguro General de Salud Individual y Familiar, el mismo que deberá formalizarlo en un plazo no mayor a 10 días una vez emitido el presente documento.
- La segregación de funciones del personal técnico que labora en el área de tecnologías de la información del HGMYM que brinda soporte al Sistema de Gestión Médica MIS AS400, deben ir conforme al ámbito de sus competencias.

- La creación de bodegas virtuales en el MIS-AS400 deberá ser bajo la autorización de la máxima autoridad del HGMYM, mismo que deberá estar bajo supervisión periódica de la Dirección del Seguro General de Salud Individual y Familiar.
- El área de TI solicitará apoyo a la DNTI, para que puedan verificar periódicamente las pistas de auditoria del Sistema MIS-AS400 el ingreso y buen uso de la información por parte de los usuarios técnicos.
- Es potestad del área de tecnologías del HGMYM, elaborar documentos «Formatos» de este procedimiento cuando lo considere necesario; previo a la comunicación formal del documento a los grupos de interés y para su implementación con el fin de llevar a cabo y documentar los diferentes requerimientos solicitados por los usuarios.
- El área de TI, debe establecer y socializar los procedimientos, lineamientos, documentos técnicos, para la gestión de la atención de solicitudes de información, mantenimientos relacionados al Sistema MIS AS400 a todos los usuarios internos del hospital.
- Los servidores del HGMYM, deben utilizar los formularios, formatos y/o documentación establecida en el procedimiento para la gestión de la atención de solicitudes de información, mantenimientos relacionados al Sistema MIS AS400.
- El Administrador del Sistema MIS AS400 del área de tecnologías, deberá realizar al menos 2 capacitaciones anuales internas a su personal, con la finalidad de evitar la centralización del conocimiento en un solo servidor del HGMYM.
- El coordinador/técnico local del HGMYM, deberá realizar respaldos periódicamente de la información registrada en el Sistema MIS AS400.

6.8.3.3. Establecer las restricciones y prohibiciones.

- Bajo ningún concepto se realizará respaldos de información personales no planificadas y no autorizadas por la el área de TI.
- Bajo ningún concepto se debe utilizar la información del MIS AS400 para beneficio o conocimiento propio de los usuarios de la plataforma.
- Los usuarios técnicos responsables de la administración del Sistema MIS-AS400, no deberán tener roles que no correspondan al ámbito tecnológico.

6.9. Monitoreo de los riesgos

Los procesos y las actividades de mitigación de riesgos asociados a la administración y control técnico de los activos dentro del área de TI del HGMYM, serán monitoreados de forma

periódica para prevenir problemas graves que puedan afectar la culminación del mismo. Las revisiones se establecen en actas para su constancia y tendrán una frecuencia cada 15 días.

6.10. Comunicación del riesgo

Una de las acciones principales y primordiales es la comunicación y socialización de los riesgos al personal del área de TI y comunicación del HGMYM, ya que se convierten en el primer punto de origen de la inseguridad por acciones voluntarias como involuntarias, para garantizar la seguridad de los pacientes y la protección de la información confidencial de la salud del sistema MIS AS400, esta comunicación se la realiza de manera clara y detallada, asegurando que el área de tecnologías entienda los riesgos y esté dispuesta a tomar las medidas plasmadas para mitigarlos. La comunicación del riesgo se realiza por escrito y mediante reuniones periódicas con el personal del área de tecnologías, donde efectúan el seguimiento para garantizar que las medidas de mitigación se implementen de manera efectiva y se monitoreen continuamente.

7. Discusión

La gestión de riesgos en la infraestructura de TI es un aspecto fundamental en la actualidad. Con el avance de la tecnología, esta se ha convertido en una herramienta esencial para las operaciones organizacionales. En este contexto, el HGMYM se enfrenta al desafío de implementar medidas de gestión de riesgos que aseguren la protección y el correcto funcionamiento de su infraestructura tecnológica.

Durante el desarrollo de la propuesta de modelo de gestión de seguridad de la información, se ha considerado la legislación nacional relacionada con la confidencialidad de la información en salud en Ecuador. Esto ha permitido adaptar el modelo a los requisitos legales específicos y garantizar el cumplimiento normativo en la Unidad Médica.

El HGMYM reconoce la importancia de salvaguardar la integridad de su información y la confiabilidad de sus sistemas. Para lograrlo, es necesario contar con un enfoque proactivo en la gestión de riesgos, identificando los posibles peligros y vulnerabilidades que podrían afectar a la infraestructura tecnológica. Para ello se realiza una revisión bibliográfica del concepto de gestión de riesgos en TI y se aplica una metodología de evaluación de riesgos adecuada a las necesidades del hospital.

La propuesta de medidas de gestión de riesgos permitirá al hospital anticiparse a posibles incidentes y minimizar su impacto. Entre las acciones necesarias se encuentran la evaluación regular de la seguridad de los sistemas, la implementación de políticas y procedimientos robustos, el establecimiento de controles de acceso adecuados, privilegios, copia de respaldo, monitoreo del sistema y la capacitación constante del personal en materia de seguridad informática.

La gestión de riesgos en la infraestructura de TI no solo es una responsabilidad del departamento de tecnología, sino que requiere el compromiso y la participación de todos los miembros del hospital. Es importante fomentar una cultura de seguridad informática, promoviendo buenas prácticas entre el personal y concientizando sobre los riesgos asociados al uso inadecuado de la tecnología.

Así mismo, en otras investigaciones se muestra un comportamiento similar: por ejemplo Puga-Jácome (2019), diseñó un modelo de gestión de seguridad de la información para el área de imagenología del Hospital General Docente de Calderon, Reinoso-Quijo (2019) implementó políticas de seguridad para las aplicaciones médicas del laboratorio clínico del centro de salud tipo B «Fray Bartolomé de las Casas» del Ministerio de Salud Pública del Ecuador, comparado con la propuesta de modelo de gestión de seguridad de la información del

HGMYM, se afirma que la norma ISO 27799:2008 proporciona una guía para la gestión de la seguridad de la información en el sector de la salud y es aplicable a cualquier organización que maneje información de salud.

En comparación con estudios previos, tomando como referencia el trabajo de investigación de (Cárdenas, 2018; Puga-Jacome, 2019; Reinoso-Quijo, 2019), los resultados son consistentes con los del HGMYM, se considera las leyes y regulaciones sobre confidencialidad de la información que posee el Ecuador, aplican la norma ISO 27799 y obtienen beneficios similares que incluyen la mejora de la confidencialidad, integridad y disponibilidad de la información, la reducción de los riesgos y amenazas de seguridad, y la mejora de la imagen y reputación de la organización.

La propuesta de Modelo de gestión de seguridad de la información para el HGMYM, basado en la norma ISO 27799:2008, se presenta como una solución integral y adecuada para garantizar la seguridad de la información, la protección de los sistemas y registros médicos en el ámbito hospitalario. Esto requiere un enfoque integral que involucre evaluaciones regulares, políticas sólidas, controles adecuados y una cultura de seguridad informática arraigada en todos los miembros de la unidad médica.

8. Conclusiones

En relación a los objetivos específicos planteados en la investigación sobre la propuesta de Modelo de gestión de seguridad de la información para el Hospital General Manuel Ygnacio Monteros IESS-LOJA, basado en la norma ISO 27799:2008 se concluye:

- Se realizó una evaluación exhaustiva de los riesgos asociados a la infraestructura de tecnología de la información (TI) del Hospital General Manuel Ygnacio Monteros IESS-LOJA.
- La propuesta de un modelo de gestión de seguridad de la información basado en la norma ISO 27799:2008 es de gran beneficio para el Hospital General Manuel Ygnacio Monteros IESS-LOJA, ya que a través de esta propuesta se busca mejorar la seguridad y protección de la información en el hospital.
- El modelo propuesto se basa en los principios de la norma ISO 27799:2008 y se adapta a las necesidades específicas del hospital, tomando en cuenta los recursos disponibles y los riesgos a los que se encuentra expuesta la información en el entorno actual.
- La propuesta del modelo de gestión de la información no solo contribuirá a mejorar la seguridad de la información, sino que también fomentará una cultura de seguridad en la organización y sensibilizará al personal sobre la importancia de proteger la información en su día a día. Esto puede tener un impacto positivo en la calidad del servicio y la confianza de los pacientes en la institución.
- La norma ISO 27799:2008 es una herramienta útil para el desarrollo de un modelo de gestión de seguridad de la información en el ámbito de la salud, ya que tiene en cuenta las particularidades de este sector y proporciona un marco de referencia completo y estructurado.
- La propuesta de este modelo no solo mejorará la protección de los datos sensibles, sino que también permitirá al hospital cumplir con las normativas y regulaciones vigentes en materia de seguridad de la información en el ámbito de la salud. Además, se fomentará una cultura de seguridad de la información entre los trabajadores, lo que se traducirá en una mayor conciencia y responsabilidad en el manejo de los datos sensibles.

9. Recomendaciones

En relación a los objetivos específicos planteados en la investigación sobre la propuesta de Modelo de gestión de seguridad de la información para el Hospital General Manuel Ygnacio Monteros IESS-LOJA, basado en la norma ISO 27799:2008 se recomienda:

- Se recomienda adoptar formalmente la norma ISO 27799:2008 como marco de referencia para la gestión de la seguridad de la información en el HGMYM. Esto incluye la identificación de los requisitos y lineamientos establecidos en la norma y su adecuada implementación en todas las áreas y procesos relevantes.
- Se recomienda implementar medidas técnicas adecuadas para garantizar la seguridad de la información. Esto incluye el uso de firewalls, sistemas de detección de intrusiones, encriptación de datos, copias de seguridad regulares y actualizaciones de software y sistemas operativos.
- Se sugiere brindar capacitación y concientización regular a todo el personal del hospital sobre la importancia de la seguridad de la información y la correcta implementación de las políticas y procedimientos establecidos. Esto garantizará que todos los miembros del personal estén alineados y comprometidos con las prácticas de seguridad.
- Se recomienda establecer un programa de auditoría y monitoreo continuo de los sistemas de información del hospital. Esto permitirá detectar posibles vulnerabilidades o incidentes de seguridad, así como evaluar la eficacia de las medidas implementadas.
- Se recomienda establecer un proceso de mejora continua en la gestión de seguridad de la información, realizando revisiones periódicas y actualizando las políticas y procedimientos de acuerdo con los cambios tecnológicos y las nuevas amenazas identificadas.
- Se recomienda fomentar la colaboración con otras instituciones de salud para intercambiar buenas prácticas y experiencias en la implementación de SGSI basados en la norma ISO 27799:2008.

10. Bibliografía

Ley de Derechos y Amparo del paciente, Pub. L. No. 77 (2006). https://www.salud.gob.ec/wp-content/uploads/downloads/2014/09/Normativa-Ley-de-Derechos-y-Amparo-del-Paciente.pdf

Reglamento de Información confidencial en el Sistema Nacional de Salud, (2015). http://instituciones.msp.gob.ec/cz6/images/lotaip/Enero2015/Acuerdo%20Ministerial%205216.pdf

Baena, R. G., Mendoza Mendez, R. V., & Coronado, E. (2019). Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestión de la seguridad de la información. contribuciones a la Economía, junio. https://www.eumed.net/rev/ce/2019/2/norma-iso-eic.html

Cárdenas, I. G. (2018). Diseño de una política de seguridad de la información basada en la norma ISO 27799 para el control de accesos a las aplicaciones médicas de la red en el hospital AXXIS.

Cayambe Villa, O. P. (2020). Plan de seguridad informática aplicando la norma ISO 27001, para la protección de activos en la asociación Conferib [BachelorThesis]. https://dspace.uniandes.edu.ec/handle/123456789/13305

Código Orgánico Integral Penal, (2014). https://oig.cepal.org/sites/default/files/2014_ecu_codpenal.pdf

Constitución de la República de Ecuador, (2008). https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Contardi, S. (2005). Gestión de información: Dimensiones e implementación para el éxito organizacional / Gloria Ponjuán Dante. Rosario: Nuevo Parhadigma, 2004. 214 p.

ISBN:987-96536-6-1. Información, cultura y sociedad, 12, Article 12. https://doi.org/10.34096/ics.i12.908

Contero, W. M. C. (2019). Diseño de una política de seguridad de la información basada en la norma iso 27002:2013, para el sistema de botones de seguridad del ministerio del interior. https://repositorio.uisek.edu.ec/bitstream/123456789/3345/1/TESIS%20MC%2026_03_2019.pdf

Córdoba, P. (2022). Sistema de Gestión de la Seguridad de la Información [Universidad Siglo 21]. https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/24916/TFG%20-%20C%c3%b3rdoba%2c%20Pablo.pdf?sequence=1&isAllowed=y

Durand-More, A. (2019). Evaluación de técnicas de ethical hacking para el diagnóstico de vulnerabilidades de la seguridad informatica en una empresa prestadora de servicios [Universidad Señor de Sipan]. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/7359/Durand%20More%2c%20Andr%c3%a9s%20David.pdf?sequence=1&isAllowed=y

Enríquez, A. (2018). Modelo de gestión de seguridad de la información para instituciones de salud, basado en las normas iso 27799:2008, iso/iec 27005:2008 e iso/iec 27002:2013 aplicada a la clínica médica fértil. http://repositorio.utn.edu.ec/bitstream/123456789/8572/1/04%20RED%20201%20TRABAJO%20DE%20GRADO.pdf

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. Polo del Conocimiento, 2(12), Article 12. https://doi.org/10.23857/pc.v2i12.420

Flores, Ma. G., & Castillo, A. (2012, mayo 8). Una mirada desde la sociedad civil a la Gobernanza del Sistema Nacional de Salud by Grupo FARO - Issuu. https://issuu.com/grupofaroecuador/docs/gobernanza-salud-ecuador

Garcia Cruz, R. A. (2021). Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de Tecnologías de Información del gobierno regional Piura; 2020. Universidad Católica Los Ángeles de Chimbote. https://repositorio.uladech.edu.pe/handle/20.500.13032/20296

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informática organizacional: Un modelo de simulación basado en dinámica de sistemas. Scientia et technica, 22(2), 196. https://doi.org/10.22517/23447214.11371

Gutiérrez-Martínez, J., Núñez-Gaona, M. A., Aguirre-Meneses, H., & Delgado-Esquerra, R. E. (2014). Implementación de la seguridad en el manejo de las imágenes médicas. https://www.medigraphic.com/pdfs/invdis/ir-2014/ir144d.pdf

Lachapelle, E., & Bislimi, M. (2015). ISO 27001 Information Technology – Security Techniques Information Security – Management Systems—Requirements. https://pecb.com/whitepaper/iso-27001-information-technology--security-techniques-information-security--management-systems---requirements

Ley Orgánica de la Salud, Pub. L. No. 67 (2006). https://www.salud.gob.ec/wp-content/uploads/2017/03/LEY-ORG%C3%81NICA-DE-SALUD4.pdf

Ley Orgánica de Transparencia y acceso a la Información Pública, (2004). https://www.educacionsuperior.gob.ec/wp-content/uploads/downloads/2014/09/LOTAIP.pdf

Ley Orgánica del Sistema Nacional de Salud. (2002). LEY ORGANICA DEL SISTEMA NACIONAL DE SALUD. https://cpl.thalesgroup.com/es/compliance/iso-277992016-compliance

Lucio, R., Villacrés, N., & Henríquez, R. (2011). Sistema de salud de Ecuador. salud pública de méxico, 53. https://www.scielosp.org/article/ssm/content/raw/?resource_ssm_path=/media/assets/spm/v53s2/13.pdf

Nieves, A. C. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001:2013. https://alejandria.poligran.edu.co/handle/10823/994

Puga-Jacome, C. E. P. (2019). Diseño de una política de gestión de seguridad de la información para el área de imagenología del hospital general docente de calderón utilizando los estandares ISO 27001 e ISO 27799. https://repositorio.uisek.edu.ec/bitstream/123456789/3343/1/TESIS%20MTI%20EDUARDO%20PUGA.pdf

Reglamento orgánico funcional IESS. (2016). Resolución del IESS 535. https://spryn2.finanzas.gob.ec/esipren-web/archivos_html/file/Reglamento%20Org%C3%A1nico%20Funcional%20del%20IESS.pdf

Reinoso-Quijo, A. (2019). Política de seguridad de la información basada en la norma iso 27799—2008 para las aplicaciones médicas del laboratorio clínico del centro de salud tipo b fray bartolomé de las casas del ministerio de salud pública del ecuador.

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. Polo del Conocimiento, 3(4), Article 4. https://doi.org/10.23857/pc.v3i4.809

Téllez Carvajal, E. (2018). TECNOLOGÍAS, SEGURIDAD INFORMÁTICA Y DERECHOS HUMANOS. IUS ET SCIENTIA, 1(4), 19-39. https://doi.org/10.12795/IETSCIENTIA.2018.i01.03

Torres Fernández, J. P., Gallo Mendoza, J. G., Hallo Alvear, R. F., Abcarius, J. J., Muriel Páez, M. H., & Fernández Lorenzo, A. (2017). Gestión de la información como herramienta para la toma de decisiones en salud: Escenarios más probables. Revista Cubana de Investigaciones Biomédicas, 36(3), 0-0.

Torres León, M. R. (2018). Diseño de un sistema de gestión de la seguridad de la información (SGSI), basada en la norma ISO/IEC 27001:2013, para el proceso de servicio post-venta de un integrador de soluciones en Telecomunicaciones [Licenciatura, Universidad Peruana de Ciencias Aplicadas]. https://doi.org/10.19083/tesis/624142

UNE-EN ISO/IEC 27002:2017. (2017). Tecnología de la Información Técnicas de seguridad Código de prácticas para los controles de seguridad de la información. ASOCIACION INSTITUTO DE NORMAS TECNICAS DE COSTA RICA. https://static.eoi.es/inline/une-en_iso-iec_27002_norma_mincotur.pdf

Valencia-Duque, F. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 22, 73-88. https://doi.org/10.17013/risti.22.73-88

Vega Briceño, E. (2021). Seguridad de la información (1.ª ed.). Editorial Científica 3Ciencias. https://doi.org/10.17993/tics.2021.4

11. Anexos

Anexo 1 . ***Situación actual y aplicación del control de seguridad de la información***

Medidas de control		**Nivel de Alerta**						**Característica**	
Sección	Control	Cantidad de medidas	N_I	N_II	N_III	N_IV	N_V	Responsable	Fecha de implantación
5. Políticas de seguridad de la información	Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a todos los servidores públicos del hospital, así como a las partes externas relevantes.	2	1	2	3	4	5	Directivos del hospital	Implementada
	La política de seguridad de información se revisa a intervalos planificados, y si ocurren cambios significativos se asegura su conveniencia, adecuación y eficacia continua		1	2	3	4	5	Directivos del hospital	Mayo-2023

6. Organización de la seguridad de la información	Todas las organizaciones cuyo personal esté implicado en el tratamiento de datos personales sanitarios deberían documentar tales implicaciones en las descripciones de los puestos de trabajo Las organizaciones que traten datos personales sanitarios deberían, cuando sea viable, segregar las tareas y áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o de uso indebido de los datos personales sanitarios. La alta dirección apoya (dirige, se compromete, demuestra y reconoce responsabilidades) activamente la SI en el hospital, asimismo el personal de la alta gerencia del HGMYM deberá inmiscuirse en el conocimiento de la política y gestionarla de tal forma que se cumpla dentro del área de tecnología.	3	1	2	3	4	5	Departamento de talento humano Departamento de talento humano Departamento de TI	Implementada Junio-2023 Junio-2023

	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos y necesidades, la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.		4	5	Departamento de talento humano	Mayo-2023
7. Seguridad de los recursos humanos	Todas las organizaciones que traten datos personales sanitarios deberían incluir en los términos y condiciones de contratación de los empleados que procesan, o procesarán, datos personales sanitarios una declaración sobre las responsabilidades del empleado en seguridad de la información	6	4	5	Departamento de talento humano	Mayo-2023
	Es importante destacar el énfasis especial que es necesario poner sobre las preocupaciones de los sujetos de la asistencia que no desean que accedan a sus datos personales sanitarios aquellos trabajadores sanitarios que sean vecinos, compañeros o familiares. Tales inquietudes a menudo esconden un alto porcentaje de		4	5	Departamento de talento humano	Junio-2023

	reclamaciones de aquellos con temor sobre la confidencialidad de sus datos personales sanitarios. Del mismo modo, los miembros del personal a menudo no desean estar innecesariamente en la posición de tener que revisar información sobre amigos, familiares o vecinos. Una gestión efectiva de los sistemas de información sanitarios necesita tratar estas inquietudes					
	Todas las organizaciones que traten datos personales sanitarios deberán asegurar que se proporciona formación y capacitación en seguridad de la información, y que se proporciona a todos los empleados actualizaciones regulares en políticas y procedimientos de seguridad de la organización, y cuando sea relevante, a los contratistas terceros, los investigadores, los estudiantes y los voluntarios que tratan datos personales sanitarios		4	5	Departamento de TI	Junio-2023
	Los procesos disciplinarios en las organizaciones sanitarias con respecto a las brechas de seguridad de la información deberían seguir		4	5	Departamento de talento humano	Junio-2023

	procedimientos que estén reflejados en las políticas y sean por tanto conocidos por los sujetos objeto del proceso disciplinario Es importante resaltar que, en sanidad, muchos tipos de personal, por ejemplo, los médicos y las enfermeras, habitualmente progresan a través de programas de formación y otras «rotaciones» en los que sus derechos de acceso pueden cambiar sustancialmente. Para asegurar la finalización de los derechos anteriores que ya no son necesarios para su rol, tales cambios de empleo deberían ser inicialmente tratados de la misma forma que en aquellos individuos que abandonan el empleo en la organización.					4	5	Departamento de TI	Mayo-2023
8 Gestión de activos	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deberían estar claramente identificados y debería	8	1	2	3	4	5	Departamento de TI	Implementada

	elaborarse y mantenerse un inventario.							
	Todos los activos que figuran en el inventario deberían tener un propietario.	1	2	3	4	5	Departamento de TI	Implementada
	Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	1	2	3	4	5	Departamento de TI	Mayo-2023
	Todos los empleados y usuarios de partes externas deberían devolver todos los activos del hospital que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	1	2	3	4	5	Departamento de TI	Junio-2023
	Las organizaciones que traten datos personales sanitarios deberían clasificar uniformemente tales datos como confidenciales.	1	2	3	4	5	Departamento de TI	Junio-2023

	Todos los sistemas de información sanitarios que traten datos personales sanitarios deberían informar a los usuarios de la confidencialidad de los datos personales sanitarios accesibles desde el sistema	1	2	3	4	5	Departamento de TI	Mayo 2023
	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por el hospital. El uso de laptop para la realización de los servicios fuera del hospital requiere que estos tipos de activos sean protegidos y asegurados.	1	2	3	4	5	Departamento de TI	Julio 2023
	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. En el hospital todas las laptops son entregadas al personal, pero no se ha tenido un control correcto. Es por eso que es necesario un control de registro de materiales que se haya entregado a cada colaborador y que se comprometa a	1	2	3	4	5	Departamento de TI	Julio 2023

	cuidar y regresarlos cuando no esté en uso.								
9 Control de acceso	La política de la organización sobre el control de accesos debería establecerse sobre la base de roles predefinidos con autoridades asociadas que sean adecuadas, pero limitadas a, las necesidades de ese rol.	8	1	2	3	4	5	Departamento de TI	Agosto-2023
	Únicamente se debería proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados		1	2	3	4	5	Departamento de TI	Agosto-2023
	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.		1	2	3	4	5	Departamento de TI	Agosto-2023
	Se debería implementar un proceso de provisión de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios médicos del hospital.		1	2	3	4	5	Departamento de TI	Agosto-2023

Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	1	2	3	4	5	Departamento de TI	Agosto-2023
Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deberían ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	1	2	3	4	5	Departamento de TI	Agosto-2023
Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	1	2	3	4	5	Departamento de TI	Agosto-2023
El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	1	2	3	4	5	Departamento de TI	Agosto-2023
Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas	1	2	3	4	5	Departamento de TI	Agosto-2023

10 Criptografía	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las claves criptográficas durante todo su ciclo de vida. Muchas organizaciones sanitarias han considerado la adopción de tecnologías de autenticación alternativas para tratar este problema.	1	1	2	3	4	5	Departamento de TI	Septiembre-2023
11 Seguridad física y del entorno	Las organizaciones que realizan tratamiento de datos personales sanitarios deberían utilizar perímetros de seguridad para proteger las áreas que contienen recursos para el tratamiento de la información para esas aplicaciones sanitarias	10	1	2	3	4	5	Departamento de TI	Octubre-2023
	Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado		1	2	3	4	5	Departamento de TI	Mayo-2023

	Es importante destacar que la provisión de asistencia sanitaria incluye distintas circunstancias en las que el público es físicamente ingresado en áreas con grandes cantidades de información sensible. Aquellas áreas físicas en la asistencia sanitaria que recogen información sanitaria mediante entrevistas y que contienen sistemas en los que se ven datos en una pantalla deberían, por tanto, estar sujetas a un escrutinio adicional. Los dispositivos médicos que registran o informan de datos también pueden requerir consideraciones especiales de seguridad en relación al entorno en el que operan y a las emisiones electromagnéticas que se producen durante su funcionamiento. Las organizaciones sanitarias, especialmente los hospitales, deberían asegurar que las directrices de emplazamiento y protección de TI minimizan la exposición a esas emisiones	1 1	2 2	3 3	4 4	5 5	Departamento de TI Departamento de TI	Octubre-2023 Octubre-2023

	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debería estar protegido frente a interceptaciones, interferencias o daños.	1	2	3	4	5	Departamento de TI	Implementada
	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas	1	2	3	4	5	Departamento de TI	Implementada
	Las organizaciones que proporcionen o utilicen equipos, datos o software para dar soporte a una aplicación sanitaria que contenga datos personales sanitarios no deberá permitir quo esos equipos, datos o software salgan de las instalaciones o sean reubicados dentro de ellas sin autorización de la organización.	1	2	3	4	5	Departamento de TI	Mayo-2023
	Las organizaciones que traten datos personales sanitarios deberían asegurar que ha sido autorizado todo uso, fuera de las instalaciones, de dispositivos médicos que registran o informan datos. Esto debería incluir los equipos utilizados por los	1	2	3	4	5	Departamento de TI	Mayo-2023

	teletrabajadores, incluso cuando esa utilización sea permanente									
	Las organizaciones que traten aplicaciones de informática sanitaria deberán sobrescribir de forma segura o incluso destruir todos los medios que contengan software de sistemas informáticos sanitarios o datos personales sanitarios cuando ya no sean necesarios.		1	2	3	4	5	Departamento de TI	Octubre -2023
	Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.		1	2	3	4	5	Departamento de TI	Junio-2023
12 Seguridad de las operaciones	Se debería controlar los cambios en la organización, en los procesos del hospital, en las instalaciones y en los sistemas de procesamiento de	4				4	5	Departamento de TI	Septiembre-2023

información que afectan la seguridad de información					
Las organizaciones que traten datos personales sanitarios deberán implantar controles adecuados de prevención, detección y respuesta para proteger contra el software malicioso y deberán implantar la formación adecuada para la concienciación del usuario.		4	5	Departamento de TI	Septiembre-2023
Las organizaciones que traten datos personales sanitarios deberán realizar copias de seguridad de todos los datos personales sanitarios y almacenarlas en un entorno físicamente seguro que garantice su futura disponibilidad.		4	5	Departamento de TI	Septiembre-2023
Se deberían implementar procedimientos para controlar la instalación del software en explotación.		4	5	Departamento de TI	Septiembre-2023
Las redes se deberían gestionar y controlar para proteger la	6	4	5	Departamento de TI	Septiembre-2023

	información en sistemas y aplicaciones.					
	Las organizaciones que traten datos personales sanitarios deberían considerar cuidadosamente qué impacto tendría la pérdida de disponibilidad de servicios de red sobre la práctica clínica.		4	5	Departamento de TI	Septiembre-2023
	Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.		4	5	Departamento de TI	Septiembre-2023
13 Seguridad de las comunicaciones	Las organizaciones deberán asegurarse de que la seguridad de esos intercambios de información está sujeta a la política de desarrollo y auditorías de conformidad.		4	5	Departamento de TI	Septiembre-2023
	Las organizaciones que transmitan datos personales sanitarios mediante mensajería electrónica deberían realizar acciones para asegurar su confidencialidad e integridad. Es importante destacar que la seguridad de un correo electrónico y de los mensajes instantáneos que contengan datos personales sanitarios puede implicar procedimientos para el personal		4	5	Departamento de TI	Septiembre-2023

	sanitario que no pueden ser impuestos ni a los sujetos de la asistencia ni al público.								
	Las organizaciones que traten datos personales sanitarios deberán tener un acuerdo de confidencialidad en vigor que especifique la naturaleza confidencial de esta información. El acuerdo deberá ser aplicable a todo el personal que accede a la información sanitaria.					4	5	Departamento de TI	Septiembre-2023
14 Adquisición, desarrollo y mantenimiento de los sistemas de información	Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	3	1	2	3	4	5	Departamento de TI	Septiembre-2023
	Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los		1	2	3	4	5	Departamento de TI	Septiembre-2023

	desarrollos que se dan dentro del hospital. Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.		1	2	3	4	5	Departamento de TI	Septiembre-2023
16 Gestión de incidentes de seguridad de la información	Se requiere identificar responsabilidades y un procedimiento para la gestión de incidentes.	1			3	4	5	Departamento de TI	Agosto-2023
18 Cumplimiento	Es necesario establecer un acuerdo de confidencialidad sobre la privacidad de las personas y la protección de datos de carácter personal de la organización.	1	1	2	3	4	5	Departamento de talento humano	Mayo-2023
	Total	**53**							

Anexo 2. Certificación de traducción del resumen

Loja, 14 de junio de 2023

Yo, Paulina Elizabeth Leon Pucha, Magister en Pedagogía de los Idiomas Nacionales y Extranjeros mención en Enseñanza de Inglés, registrada en Senescyt con el número 1049-2020-2190675.

CERTIFICO:

Que he prestado mis servicios profesionales para la traducción del resumen de la tesis titulada Propuesta de Modelo de Gestión de Seguridad de la Información para el Hospital General Manuel Ygnacio Monteros IESS-LOJA, basado en la norma ISO 27799:2008, mismo que pertenece al señor Cristian Vinicio Palacios Andrade, estudiante de la maestría en Telecomunicaciones de la Universidad Nacional de Loja.

Esta certificación se expide a solicitud del interesado, pudiendo hacer uso de la misma según ella convenga.

_____

Paulina Elizabeth Leon Pucha

Senescyt No. 1049-2020-2190675.