DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DEL HOSPITAL SAN VICENTE DE PAÚL DE FRESNO.

GERMAN ALEXIS PRADA OSPINA
ROGER MARINO ORTIZ MERCHAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2022

DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DEL HOSPITAL SAN VICENTE DE PAÚL DE FRESNO.

GERMAN ALEXIS PRADA OSPINA
ROGER MARINO ORTIZ MERCHAN

PROYECTO APLICADO PARA OPTAR POR EL TÍTULO DE ESPECIALISTAS EN SEGURIDAD INFORMÁTICA

JOEL CARROLL VARGAS
Asesor Trabajo de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2022

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedicamos este trabajo primero que todo a Dios, por sus grandes bendiciones, a nuestros padres por su apoyo incondicional, por las fuerzas y energías que nos transmiten cada día para superar los obstáculos de la vida, a nuestros familiares y amigos por las palabras de aliento para no desfallecer en esta nueva etapa que decidimos emprender como profesionales.

AGRADECIMIENTOS

Agradecemos a la gerente del Hospital San Vicente de Paúl del municipio de Fresno Tolima, por permitirnos utilizar la empresa para el desarrollo de este proyecto.

A los funcionarios del Hospital San Vicente de Paúl del municipio de Fresno Tolima, por el tiempo dedicado para poder obtener la información plasmada en el proyecto.

A los tutores Katerine Marceles y Joel Carroll Vargas, directores y tutores del curso, por su entrega y dedicación a su trabajo, por el gran apoyo brindado en el desarrollo de todas las actividades propuestas.

Agradecemos a la Universidad Nacional Abierta y a Distancia UNAD, quienes nos ofrecen la oportunidad de continuar nuestros estudios de postgrado con una oferta académica de calidad y tratando de llegar a todas las personas que quieren obtener su título, ya que nos brindan diferentes opciones de estudio y nos ofrecen la oportunidad de estudiar y laborar, de igual manera, agradecer a los tutores y directores que nos dedicaron su compañía y aportaron su conocimiento para alcanzar este logro.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

El diseño de este proyecto se basará en el estudio y análisis del estado actual, respecto al ámbito de seguridad informática y de la información del área de las tecnologías de la información y comunicación del Hospital San Vicente de Paúl del municipio de Fresno Tolima. Teniendo en cuenta que la información es uno de los activos de mayor valor en una organización, y más para una entidad del área de la salud que maneja información clasificada y privada de gran importancia para sus usuarios; se plantea este proyecto para identificar los riesgos y vulnerabilidades existentes en la infraestructura tecnológica de la entidad y en los procesos que manipulen información, con el fin de clasificar y calificar dichas amenazas y sus posibles consecuencias, se seleccionara una metodología de evaluación del riesgo para poder definir estrategias y así evitar la pérdida irremediable de información valiosa para la institución de salud.

De esta manera, este documento pretende demostrar la importancia de diseñar un sistema de gestión de seguridad de la información en el hospital para mejorar procesos y administrar los activos de información de la entidad de una manera más segura y concreta.

Palabras clave: Control, Información, Riesgos, Seguridad, Vulnerabilidad.

ABSTRACT

The design of this project will be based on the study and analysis of the current state, regarding the area of computer security and information in the area of information and communication technologies of the San Vicente de Paul Hospital in the municipality of Fresno Tolima. Taking into account that information is one of the most valuable assets in an organization, and more so for an entity in the health area that handles classified and private information of great importance for its users; This project is proposed to identify the existing risks and vulnerabilities in the entity's technological infrastructure and in the processes that manipulate information, in order to classify and qualify said threats and their possible consequences, a risk assessment methodology will be selected to be able to define strategies and thus avoid the irremediable loss of valuable information for the health institution.

In this way, this document aims to demonstrate the importance of designing an information security management system in the hospital to improve processes and manage the entity's information assets in a more secure and specific way.

Keywords: Control, Information, Risks, Security, Vulnerability.

INTRODUCCIÓN

Después de vivir una pandemia en carne propia, la sociedad dio mayor importancia al sector salud y principalmente a las entidades prestadoras de servicios de salud. Dichas entidades tuvieron que trabajar el doble, esforzándose así por continuar con la prestación de sus servicios y recolectar la información personal de cada uno de sus usuarios en la historia clínica, con el fin de resguardar la información presente y generar antecedentes que puedan ayudar a futuros diagnósticos.

El Hospital San Vicente de Paúl no fue ajeno a ello, y como entidad de salud, tuvo que fortalecer sus procesos y su equipo de trabajo con el fin de preservar la vida y salud de la población fresnense resguardando la información de consultas por servicios como urgencias, consulta general, promoción y prevención, toma de exámenes y demás servicios en su único sistema de información denominado SIHOS, el cual funciona como ERP y HIS permitiendo así tener un sistema universal en donde se maneje información asistencial y administrativa a la vez.

Dadas estas circunstancias, se recomienda elaborar un análisis del nivel de implementación de estrategias y controles definidos por el Ministerio de las TIC y su política de Gobierno Digital, con el fin de estipular el nivel de madurez que maneja el Hospital San Vicente de Paúl de Fresno en la aplicación de controles con el fin de incrementar la seguridad y privacidad de la información resguardada por la entidad.

Una vez se defina el nivel de madurez en la que se encuentra el hospital, se realizará el inventario de activos de información del área de tecnologías y sistemas de información para calificar dichos activos en términos de integridad, disponibilidad y confidencialidad y así poder realizar un estudio de riesgos y definir una matriz con los riesgos más críticos que se puedan llegar a materializar y el respectivo manejo que se le puede dar con el fin mitigar dichas condiciones graves.

Al realizar estos procesos, lo que se busca es diseñar nuevas políticas de seguridad y privacidad de información que fortalezcan todos los procesos que manejen información dentro del hospital. Dichas políticas deben ir alineadas con la normativa y estándares, en materia de tecnologías, implementados por el gobierno y así prevenir y mitigar el impacto de la materialización de un riesgo en dichos activos.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La seguridad informática es uno de los componentes más vulnerables a cualquier tipo de amenazas tanto físicas como lógicas en una organización. En nuestra sociedad las entidades públicas o privadas en especial las entidades de salud luchan constantemente en crear nuevas estrategias que eviten la materialización de riesgos a las que se ven expuestas, debido al gran volumen de información que procesan diariamente, de acuerdo a esto, los expertos en ciberseguridad en Colombia indican que el 90% de los incidentes informáticos suceden por el poco conocimiento y aplicabilidad de políticas de seguridad en las empresas[1].

Es importante tener claro que este tipo de amenazas vuelven vulnerable a cualquier infraestructura tecnológica de índole pública o privada, atacando así desde grandes entidades estatales como el Senado de Colombia[2] que sufrió de una infiltración en la información de sus correos por parte de la organización Anonymous e hizo públicos algunos datos privados de índole secreto, hasta pequeñas empresas en donde su información es resguardada en un equipo conectado a una red simple de hogar; en resumen, todas las entidades y organizaciones deben dar importancia al tema de ciberseguridad. El Hospital San Vicente de Paúl de Fresno Tolima no ha sido ajeno a este tipo de amenazas, presentado así perdida de información, daños en equipos informáticos, infección masiva de equipos en red por troyanos y malwares, entre otros, vulnerabilidades que han sido materializadas por el poco conocimiento en ciberseguridad del personal, falta de implementación de herramientas de seguridad y la falta de una estricta implementación de políticas que ayuden a incrementar la seguridad en los activos de información de la entidad.

1.2 FORMULACIÓN DEL PROBLEMA

[1] RAMIREZ, Carlos. ¡pilas! El 90 % De Incidentes Informáticos Ocurren Al Hacer Clic En Mensajes Sospechosos. [EN LÍNEA]. 2021. [Citado en 4 de octubre de 2021]. Disponible en internet: <https://www.semana.com/finanzas/guias-basicas/articulo/pilas-el-90-de-incidentes-informaticos-ocurren- al-hacer-clic-en-mensajes-sospechosos/202113/>

[2] PORTAFOLIO, ¿qué Tipos De Ciberataques Realizó Anonymous En Colombia? [EN LÍNEA]. Economía. 2021. [Citado en 4 de octubre de 2021]. Disponible en internet: <https://www.portafolio.co/economia/que-tipos-de-ciberataques-realizo-anonymous-en-colombia-551839>

En la actualidad todas las empresas u organizaciones sin importar su índole trabajan de la mano con las nuevas tecnologías de la información y comunicaciones buscando siempre salvaguardar sus activos de información, esto con el fin de ayudar a cumplir sus procesos misionales, es por eso que el Hospital San Vicente de Paúl del municipio de Fresno Tolima, en sus procesos de mejora y pensando a futuro, requiere mejorar la seguridad de sus activos de información y demás que se desprendan de ella.

Por lo anterior, teniendo en cuenta los riesgos y amenazas que se presentan en el área de Tecnología del Hospital San Vicente de Paúl del municipio de Fresno Tolima y con base a los eventos ya presentados se ha generado el siguiente interrogante ¿Qué características o tipo de impacto traerá para el Hospital San Vicente de Paúl el diseño de un sistema de gestión de seguridad de la información para el área de la tecnología?

2 JUSTIFICACIÓN

El desarrollo de nuevas tecnologías de información y comunicación resultan cada vez más atractivas para las empresas las cuales las involucran a través de su aplicación en cada uno de sus procesos, esto se debe a las ventajas y beneficios que proporciona al mejorar la calidad y eficiencia en ellos.

Hoy en día, la información ha obtenido un gran valor para todas las entidades, Ricardo Semler, empresario, expresa “Si miras cualquier tipo de organización moderna y piensas ¿Cuál es el instrumento de poder más potente?, verás que es la información.”[3], en otras palabras, sin la información una organización literalmente no sería nada, no existiría.

Al ser un activo tan valioso, es vulnerable a riesgos y amenazas debido al gran volumen de datos que a diario procesa y resguarda. Es por esto que la seguridad y privacidad de la información se ha convertido en un factor prioritario en las entidades, el cual debe garantizar: la protección, confidencialidad, el blindaje de los datos, eficiencia en la ejecución de sus procesos, mitigación de riesgos, amenazas entre otros.

El Hospital San Vicente de Paúl del municipio de Fresno Tolima, es una entidad que presta servicios de salud de baja complejidad con enfoque preventivo, calidad, seguridad y calidez, dirigido a la población fresnense y área de influencia, que contribuye al mejoramiento de las condiciones de salud mediante la atención oportuna, enfocada en dar cumplimiento a los estándares de habilitación y fortaleciendo la incursión de nuevas tecnologías que contribuirán al bienestar de la comunidad en el cual se manejará su historia clínica tomada como información confidencial y privada para cada uno de sus usuarios.

Por ende, se hace necesario el estudio y análisis del estado actual, respecto al ámbito de seguridad informática y de la información, del área de las tecnologías de la información y comunicación del Hospital San Vicente de Paúl del municipio de Fresno Tolima para así identificar los riesgos y vulnerabilidades existentes en la infraestructura tecnología de la entidad y en los procesos que manipulen información, con el fin de clasificar y calificar dichas amenazas y sus posibles consecuencias y por ende determinar si estas directrices son importantes a través de una política de seguridad de la información.

[3] SEMLER, Ricardo. Soberanía De Nuestros Datos. [EN LÍNEA]. 2021. [Citado en 4 de octubre de 2021]. Disponible en internet: <https://elartedemedir.com/blog/soberania-de-nuestros-datos/>

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001/2013 que permita gestionar la integridad, confidencialidad y disponibilidad de la información del área de Tecnologías de la información y las comunicaciones (TIC) en el Hospital San Vicente de Paúl de Fresno.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar el estado actual del área de las TICS del hospital San Vicente de Paúl mediante un instrumento propuesto por el ministerio de las TIC, con el fin de conocer si cuentan con controles de seguridad implementados.

- Determinar la vulnerabilidades, amenazas y riesgos de seguridad informáticos a los activos de información existentes en el área de TIC del Hospital San Vicente de Paúl, basados en una metodología de gestión de riesgos, con el fin de minimizar los riesgos.

- Desarrollar el documento de aplicabilidad basado en los resultados del análisis y evaluación del riesgo en el área de TIC, con el fin de determinar los controles requeridos para el endurecimiento de la seguridad.

- Proponer políticas de seguridad alineadas al proceso, basada en la evaluación de gestión de riesgo realizada, con el fin de gestionar y brindar seguridad al área TIC del Hospital San Vicente de Paúl.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1. La importancia de salvaguardar la información en las organizaciones. Hoy en día el tratamiento de la información en las organizaciones se ha convertido en un desafío constante para la creación, implementación y aplicación de acciones y técnicas que eviten que este activo tan valioso se vea expuesto a riesgos, amenazas, perdida de información o, peor aún, que llegue a manos equivocadas. Se entiende como activo de información todo lo relacionado a soportes físicos como infraestructura o equipamiento, soportes intelectuales como proyectos, documentos, planillas, reportes etc, la cual puede estar de manera física o digital), así como también su reconocimiento, credibilidad y confianza para sus beneficiarios. Cada activo de la organización se ve expuesto a riesgos, amenazas y vulnerabilidades que lo hacen susceptible a sufrir daños inesperados, tales como ataques informáticos, espionajes, robo de información, etc y otros riesgos o amenazas naturales como por ejemplo incendios, desastres naturales, descargas eléctricas entre otros. La seguridad de estos activos de información depende de la adecuada gestión de una serie de factores, tales como: políticas integradas, planes de contingencia, análisis de riesgos, habilidades y capacidades del personal, compromiso con las directivas, inversión en tecnología y el grado de control que se ejerce[4].

Bajo esta conjetura, es necesario identificar y conocer algunos conceptos y aspectos normativos que se implementan para la creación de un Sistema de Gestión de Seguridad de la Información SGSI que permitan garantizar la confianza, flexibilidad y adaptación del sistema en el área de las Tic y así minimizar los riesgos y amenazas a los que se ve expuesto, tanto a los factores internos o externos de su entorno.

4.1.2. Estándares internacionales para la protección de datos. Dentro de las múltiples definiciones que existen sobre el Sistema de Gestión y Seguridad de la Información, es importante mencionar a que se hace referencia en la norma ISO/IEC 27001 la cual se centra en la preservación de la información en las organizaciones. No obstante, se dará a conocer la definición de la Norma antes mencionada.

[4] SGSI, ISO 27001. Aspectos Claves Y Relación Con Las Normas Iso 22301 E Iso/iec 20000. [EN LINEA]. 2019. [Citado en 10 de diciembre de 2021]. Disponible en internet: <https://www.pmg-ssi.com/2019/08/iso-27001-aspectos-claves-y-relacion-con-las-normas-iso-22301-e-iso-iec-20000/>

La Norma ISO 27001[5] es un estándar internacional que permite mejorar continuamente los procesos, mediante la cual se dan las pautas para la creación de un Sistema de Gestión de Seguridad de la Información (SGSI) con el fin de detectar posibles amenazas y definir maneras para solucionarlas, las cuales pueden amenazar la información privada de la organización, como los datos de terceros. También permite establecer políticas y reglamentos de acceso de control ideales para eliminar o reducir los riesgos.

De acuerdo con la norma ISO 27001, el SGSI incluye acciones basadas en el ciclo PHVA (Planear–hacer–verificar-actuar) para proteger la información (independientemente de su formato) contra todas las amenazas, asegurando así la continuidad del negocio en todo momento. Su propósito es resguardar e incrementar la confidencialidad, integridad y disponibilidad de la información.

4.1.3. Las fases del ciclo Deming. Estas se conocen con el famoso ciclo PHVA y están alineadas a un sistema de seguridad de la información, a continuación, se desglosan cada una de ellas:

- **Planificación (Plan) [establecer el SGSI]:** Definir políticas, normas, procesos y lineamientos con el fin de administrar el riesgo y aumentar la seguridad en la información dentro de la entidad con el fin de garantizar que los análisis sean consistentes con los planes de acción generales de la entidad.

- Definir los procesos a mejorar.
- Recolectar información del proceso a mejorar.
- Realizar análisis de la información recolectada.
- Definir objetivos que lleven a mejorar los procesos.
- Analizar los resultados obtenidos.
- Establecer las acciones para cumplir los objetivos propuestos.

- **Ejecución (Do) [implementar y gestionar el SGSI]:** Instalar y gestionare el Sistema de Gestión de acuerdo con las políticas y lineamiento del SGSI. Si es posible, se deben realizar pruebas en un ambiente controlado para analizar sus resultados antes de implementarlo en el sistema de producción.

[5] ICONTEC, Certificación ISO 27001, Sistemas De Gestión De Seguridad De La Información. [EN LÍNEA]. 2018. [Citado en 16 de octubre de 2021]. Disponible en internet: <https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de- la-informacion-2/>

- **Seguimiento (Check) [monitorizar y revisar el SGSI]: Verificar**. Calcular y analizar los beneficios de las operaciones de SGSI. Verificar que las acciones aplicadas estén vigentes, por lo que se deben recolectar nuevamente los datos y monitorear el funcionamiento del sistema.

- **Mejora (Act) [mantener y mejorar el SGSI]:** Implementar y gestionar acciones de mejora basadas en la valoración y evaluación interna para mejorar el SGSI. Se trata de actitudes adoptadas después de los primeros tres pasos y dependerá de lo que suceda. Si ocurre algún error, repita el ciclo. Si se hace correctamente, la última modificación se instalará en el sistema [6].

Teniendo en cuenta los estándares anteriormente descritos y buscando la manera de identificar y analizar cada uno de los riesgos y amenazas que puedan alterar o estropear la información de la entidad se pretende hacer uso e implementación de una metodología con el fin de definir las vulnerabilidades a las que el Sistema de Información principal del Hospital San Vicente de Paul del municipio de Fresno – Tolima, se ve expuesto.

La gestión de riesgos es la selección de medidas de seguridad adecuadas después de realizar una ardua revisión a todos los resultados obtenidos durante el estudio que hemos realizado anteriormente para poder entender, prevenir, prevenir, limitar o controlar todos los riesgos identificados para que puedan ser reducidos y minimizados[7].

4.1.4. Modelo de Seguridad y Privacidad de la Información (MSPI). este instrumento nace de la importancia de identificar los niveles de madurez al momento de implementar el modelo de seguridad y privacidad de la información adoptando controles técnico y administrativos en las entidades estatales, ayudando a impartir lineamientos de implementación y adopción a las buenas prácticas, con referencia a los estándares internaciones, orientando así la gestión e implementación de ciclo de vida de la seguridad de la información.[8]

[6] GOBIERNO DE ESPAÑA, ISO/IEC 27001. [EN LINEA]. [Citado en 10 de diciembre de 2021]. Disponible en internet: <http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/isoirc_27001_pdca.html>

[7] SGSI, ISO 27001: El Método Magerit. [EN LINEA]. 2015. [Citado en 10 de diciembre de 2021]. Disponible en internet: <https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/>

[8] GOBIERNO DIGITAL, ¿qué Es El MSPI?. [EN LINEA]. [Citado en 28 de agosto de 2022]. Disponible en internet: <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>

Para llevar a cabo la implementación del MSPI se deben ejecutar 3 fases[9]:

- **Levantamiento de información**
  - Reunión de inicio
  - Solicitud de información
  - Consolidación de información

- **Pruebas y análisis**
  - Pruebas administrativas
  - Pruebas técnicas
  - Análisis avance en ciclo PHVA
  - Análisis frente a mejores practicas

- **Informes y recomendaciones**
  - Madurez de la entidad frente al MSPI
  - Identificación de brecha
  - Recomendaciones para remediar los hallazgos
  - Elaboración del plan de seguridad

4.2 MARCO CONCEPTUAL

4.2.1 Activos de la información. Son los medios utilizados por los Sistemas de Gestión de Seguridad de la Información con el propósito de que la organizaciones o empresas logren conseguir los objetivos propuestos por sus directivos[10]. Para la Norma ISO/IEC 27001, los activos de información, tienen gran valor en las organizaciones y por ende deben ser protegidas e igualmente se cuenta con la gestión de activos de información la cual diseña e implementa procesos que conlleven a la caracterización, puntuación, clasificación y tratamiento de los mismos, dentro de los activos de información encontramos[11]:

[9] MINTIC, Instructivo Para El Diligenciamiento De La Herramienta De Diagnostico De Seguridad Y Privacidad De La Información. [EN LINEA]. 2017. [Citado en 28 de agosto de 2022]. Disponible en internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf>

[10] SGSI, ¿Cómo Realizar Un Inventario De Activos De Información? [EN LÍNEA]. 2017. [Citado en 9 de noviembre de 2021]. Disponible en internet: <https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/>

[11] NOVASEC, ¿Qué Es La Gestión De Activos De Información? [EN LÍNEA]. [Citado en 9 de noviembre de 2021]. Disponible en internet: <https://www.novasec.co/blog/67-gestion-de-activos-de-informacion>

- Inventario de activos
- Propiedad de activos
- Directrices de clasificación de activos
- Tratamiento de activos

4.2.2 Amenazas. Cualquier comportamiento que explote una vulnerabilidad de seguridad de un sistema de información. En otras palabras, puede afectar negativamente a algunos elementos de nuestro sistema. Las amenazas pueden provenir de ataques (fraude, robo, virus), eventos físicos (incendios, inundaciones) o negligencia y decisiones organizacionales (uso indebido de secretos) contraseña, no se usa cifrado). Desde una perspectiva organizacional, pueden ser tanto internas como externas. Para reducir el riesgo, la implementación es necesaria[12]:

- analices de vulnerabilidades
- capacitación a todo el personal de la organización sobre tendencias de ciberseguridad
- Mantener los Firewall y antivirus activos, entre otros

4.2.3 Estándares de seguridad: Estas técnicas a menudo están integradas en el material publicado y están diseñadas para proteger el entorno en línea del usuario o de la organización. Dentro de estos estándares se encuentra la norma ISO promoviendo normas internacionales como la ISO 27001 y la IEC, estas normas van encaminadas a realizar estandarización de las acciones importantes a realizar, generando los respectivos análisis de riesgos, con la ejecución de planes de acción para mitigar o eliminar los riesgos[13].

4.2.4 Gestión del riesgo: Es el proceso de identificar, comprender, evaluar y mitigar las amenazas y sus posibles vulnerabilidades y su impacto en la información y los sistemas

[12] HOSTDIMEBLOG, ¿Qué Es Una Amenaza Informática? ¿cómo Contenerla? [EN LÍNEA]. 2020. [Citado en 9 de noviembre de 2021]. Disponible en internet: <https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/>

[13] WEBINARS KAWAK, Estándares Seguridad De La Información ISO 27001. [EN LÍNEA]. 2020. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://www.kawak.net/project/webinar-estandares-iso-27001-seguridad-de-la-informacion-mantenga-la-confidencialidad/>

de información en las organizaciones basadas en información para actuar Estos riesgos se dividen en cuatro etapas[14]:

- Análisis
- Clasificación
- Reducción
- Control

Estas fases se implementan bajo las políticas de seguridad, normas y reglas institucionales, formando un marco operativo para garantizar la disminución de vulnerabilidades.

4.2.5 ISO 27001. Este es un estándar internacional definido por la Organización Internacional para la Estandarización (ISO), que estipula como gestionar la seguridad de la información en una empresa. Este estándar o norma se emplea principalmente en los sistemas de gestión de la seguridad de la información[15] con el fin de realizar evaluación del riesgo, aplicando los respectivos controles para disminuirlo o eliminarlos. La versión de la norma que actualmente se implementa se publicó en 2013 y se define como ISO/IEC 27001: 2013. Su primera versión se dio a conocer en el año 2005 y se basa en la norma británica BS 7799-2.[16]. Actualmente la ISO trabaja en la aprobación de actualización para dicho estándar.

4.2.6 Seguridad informática. También conocido como Seguridad de la red, este es un proceso para proteger la infraestructura tecnológica (hardware y software) como base para los sistemas de TI. Para hacer esto, es importante identificar activos importantes que forman parte de esta infraestructura para identificar amenazas, vulnerables y lidiar con este riesgo. La seguridad informática cuenta con una tipología cuya función es proteger al software, la red y el hardware[17].

[14] GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA, Gestión De Riesgo En La Seguridad Informática. [EN LÍNEA]. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/>

[15] ISOTOOLS, Software ISO Riesgos Y Seguridad. [EN LÍNEA]. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>

[16] ACADEMY, ¿Qué Es Norma ISO 27001? [EN LÍNEA]. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://advisera.com/27001academy/es/que-es-iso-27001/>

[17] UNIR, ¿Qué Es La Seguridad Informática Y Cuáles Son Sus Tipos? [EN LÍNEA]. 2021. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/>

4.2.7 Sistema de gestión de seguridad de la información. Incluye un conjunto de políticas, procedimientos, directrices, recursos y actividades relacionados conjuntamente por organizaciones, diseñados para proteger sus activos de información esenciales, tal como se define en la norma internacional ISO/IEC 27000.[18] Para poder implementar un SGSI es importante diseñar, implementar y mantener un grupo de lineamientos y actividades que gestionen efectivamente el acceso seguro a la información, siempre buscando la protección de la confidencialidad, integridad y disponibilidad de todos los activos de información[19].

4.2.8 Vulnerabilidad. Las debilidades o fallas de los sistemas de TI amenazan la seguridad de la información, evitando que los atacantes comprometan su integridad, disponibilidad o seguridad, por lo cual es importante hallarlas, analizarlas y suprimirlas lo antes posible. Estos "errores" pueden tener su inicio desde varias fuentes de ingreso al sistema, tales como: fallas de diseño, malas configuraciones o falta de software. Para realizar frente a las vulnerabilidades se hace necesario que todas las organizaciones cuenten con un departamento de seguridad o un especialista en la misma[20].

4.3 ANTECEDENTES O ESTADO ACTUAL

Con el fin de generar un buen proyecto, se hizo factible buscar algunas fuentes investigación o proyectos relacionados con el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basándose en la implementación del estándar ISO 27001:2013 y que tuviera afinidad con cada uno de los objetivos del plan a implementar en el Hospital San Vicente de Paúl de Fresno.

En las referencias halladas y mencionadas a continuación, se destaca que en todas se plantea la necesidad de implementar un Sistema de Gestión de Seguridad de la

[18] PENSEMOS, Claudia Victoria Alvarado. Sistema De Gestión De Seguridad De La Información: Qué Es Y Sus Etapas. [EN LÍNEA]. 2021. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas>

[19] FIRMA-E, ¿Qué Es Un SGSI – Sistema De Gestión De Seguridad De La Información? [EN LÍNEA]. 2013. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/>

[20] VIU, Vulnerabilidad Informática, Tipos Y Debilidades Principales. [EN LÍNEA]. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://www.universidadviu.com/es/actualidad/nuestros-expertos/vulnerabilidad-informatica-tipos-y-debilidades-principales>

Información y que dicha creación permitirá fortalecer las estrategias de ciberseguridad con el fin salvaguardar los activos de información de las entidades, permitiendo así cumplir con los tres pilares como lo son la integridad, confidencialidad y disponibilidad de la información, como lo afirma Juan Carlos de León en su proyecto investigativo:

"Con un sistema de gestión de seguridad de la Información y utilizando como marco de referencia el código de buenas prácticas de la norma ISO/IEC 27001, las entidades conocen los riesgos y las amenazas a los que está sometida la información y sus activos, de esta manera los asume, minimiza, protege y controla mediante unos procedimientos sistémicos, documentados y conocido por todos".

Este trabajo denominado "Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001 para Entidades del Estado", busca crear políticas y estrategias de forma general sobre cómo iniciar con el diseño y definir el alcance y límites para la implementación de un SGSI en una organización del estado colombiano. [21]

En el trabajo anteriormente mencionado, se hace énfasis en la importancia que se le deben dar a los activos de información y a las estrategias de seguridad que se pueden implementar con el fin de evitar la pérdida, daño o corrupción de información importante en las entidades del sector público. También se hace claridad de las normas y leyes que rigen y apoyan este tipo de seguridad en las empresas y que se apoya principalmente en las directrices emitidas por el Ministerio de las Tecnologías de la Información y la Comunicación en el territorio colombiano.

Otro referente que se tomó como base para iniciar esta investigación, es el proyecto de grado denominado "Diseño de un Sistema de Gestión de la Seguridad de la Información en la IPS ASSALUD de Corozal Sucre, mediante la implementación de la metodología MAGERIT y la Norma ISO 27001:2013" realizado por LUIS CARLOS DIAZ, en el cual se plasma el valor de la seguridad en la información en una entidad prestadora de servicios de salud[22]: "Para poder llevar a cabo el diseño de un SGSI, es necesario tener pleno conocimiento de los bienes que posee la entidad prestadora de servicios de salud y los riesgos a los cuales están expuestos, para llevar a cabo este proceso es necesario la

[21] DE LEÓN, Juan Carlos. Diseño De Un Sistema De Gestión De Seguridad De La Información (SGSI) Basado En La Norma ISO/IEC 27001 Para Entidades Del Estado. Trabajo De Grado Especialista En Seguridad Informática. La Guajira.: Universidad Nacional Abierta Y A Distancia - Unad. 2019. 118p.
[22] DIAZ, Luis Carlos. Diseño De Un Sistema De Gestión De La Seguridad De La Información En La Ips Assalud De Corozal Sucre, Mediante La Implementación De La Metodología Magerit Y La Norma Iso 27001:2013. Trabajo De Grado Especialista En Seguridad Informática. Sucre.: Universidad Nacional Abierta Y A Distancia - Unad. 2017. 205p.

implementación de una metodología que establezca las pautas para tal fin, en este caso será utilizada MAGERIT, la cual se centra en tres fases, la planeación, el análisis de riesgo y el tratamiento del riesgo; con ello se logra obtener una idea clara de los riesgos y además se definen salvaguardas para ser utilizados en caso de presentarse uno de ellos y evitar la pérdida de información de usuarios."

En este aporte destacamos la importancia y profundización que se realiza a la metodología MAGERIT como herramienta para definir un inventario de activos de información y realizar el debido análisis de riesgos y amenazas de los mismos, con el fin de generar políticas de protección y seguridad de la información en las empresas.

Otro referente tomado como guía para desarrollar el presente proyecto, es el trabajo de grado titulado "Diseño de Políticas de Seguridad de la Información para la Unidad De Tecnología De La Cámara De Comercio De Cúcuta" presentado por MARIA CAROLINA DUARTE MARTINEZ, en donde se realiza un análisis a fondo de la situación actual en la implementación de Estrategias y políticas de Seguridad en una empresa del sector privado, y en donde se describe el proceso de cómo realizar el inventario de activos de información, con el fin de obtener una base y trabajar sobre ella en los riesgos y amenazas que se pueden presentar en una arquitectura informática empresarial.

4.4 MARCO LEGAL

A continuación, se exponen algunas de las principales leyes y reglamentos relacionados con la creación y puesta en marcha de sistemas de gestión de seguridad de la información en entidades públicas y privadas en Colombia:

- **Ley 1266 de 2008.** "Por la cual se dictan las disposiciones generales del hábeas data que se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"[23] la ley significa que cualquier persona puede conocer, actualizar y corregir toda la información sobre sí misma almacenada las centrales de información.

[23] COLOMBIA. SENADO DE LA REPUBLICA. Ley 1266 De 2008. (31, diciembre, 2008). Por La Cual Se Dictan Las Disposiciones Generales Del Hábeas Data. Bogotá, 2009.

- **Ley 1273 de 2009.** "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".[24]
  Esta ley denomina a la Información como activo importante en todo proceso y establece la información y protección de datos e información en sistemas o tecnologías que hagan uso de ellos. Entre sus principales artículos se destacan el Articulo 269 enciso A en donde hablan del Acceso Abusivo a un sistema informático, el articulo 269 enciso D en donde se habla del daño informático en general, enciso E en donde prohíbe el uso de software malicioso y en el enciso F describe la importancia del buen tratamiento y uso de datos personales en bases de datos.

- **Ley Estatutaria 1581 De octubre Del 2012.** "La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."[25]
  Este derecho otorga a las personas y usuarios derechos sobre los datos que se encuentren registrados en bases de datos o archivos de una organización y puedan ser tratados por personas jurídicas de carácter público o privado, utilizados por las empresas en procesos internos.

- **Ley 1712 de 2014.** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."[26]
  En ella, la función pública establece lineamientos especiales para las entidades públicas con el fin de permitir y dar acceso a la información pública de las empresas del estado, cumpliendo ciertos criterios dados por el MinTIC y supervisado por contralorías y procuradurías.

[24] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 De 2009. (5, enero, 2009). Por El Cual Se Crea El Bien Jurídico Denominado La Protección De La Información Y De Los Datos. Bogotá, 2009.
[25] CONGRESO DE COLOMBIA. Ley estatutaria 1581 del 17 de octubre de 2012. [online]. 17 de octubre de 2012. [citado abril 2021]. Disponible en internet: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf
[26] COLOMBIA. FUNCIÓN PÚBLICA. Ley 1712 De 2014. (6, marzo, 2014). Or Medio Del Cual Se Crea La Ley De Transparencia Y Del Derecho De Acceso A La Información Pública Nacional. Bogotá, 2014.

- **Decreto 1151 de 2008.** “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la república de Colombia, se reglamenta parcialmente la ley 962 de 2005, y se dictan otras disposiciones”
  Este decreto establece la implementación de la estrategia Gobierno en Línea, hoy en día denominado Gobierno Digital, en todas las empresas del sector público del territorio colombiano.

- **Decreto 2573 de 2014.** “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”.
  Se establecen los lineamientos y directrices a cumplir en la estrategia Gobierno en Línea.

5 DISEÑO METODOLÓGICO

5.1 METODOLOGÍA DE LA INVESTIGACIÓN

Para determinar las amenazas y vulnerabilidades existentes y realizar un debido procedimiento de tratamiento de riesgos, se realizarán entrevistas y cuestionarios con el líder de las áreas presentes en el proceso de recolección y resguardo de información del Hospital San Vicente de Paúl de Fresno, en donde se definirá el inventario de los activos de información usados en la institución y se generará un análisis descriptivo de las actividades con enfoque al uso y activación de seguridad informática y de la información en cada uno de sus procesos.

Una vez identificadas las principales vulnerabilidades, amenazas y riesgos existentes en los procesos que involucren información y tecnología en el Hospital, se realizará el análisis detallado de cada una de ellas aplicando una metodología de evaluación del riesgo que permitirá realizar el análisis de la gestión de riesgos derivados del uso de tecnologías de la información y la comunicación, por medio de un método sistemático. Con la metodología de evaluación del riesgo se analizará y verificará el impacto que puedan generar los ciberataques a la seguridad informática y de la información en el Hospital.

Este proyecto estará alineado a la norma ISO 27001/2013 con el propósito de diseñar y acoger el Sistema de Gestión de Seguridad de la Información SGSI con la implementación de buenas prácticas, desarrollado bajo la metodología de investigación aplicada contando con un enfoque cualitativo y una práctica enfocada al diagnóstico para poder argumentar la necesidades o problemas que afecten a la entidad[27], entendiendo la metodología aplicada como un proceso experimental ayudando a mejorar los interrogantes o problemas que se puedan encontrar en el desarrollo del mismo, lo cual va a permitir poder realizar y alcanzar de manera adecuada el desarrollo de cada uno de los objetivos, en este mismo sentido y basados en este análisis, se documentarán los métodos de control, técnicas y políticas más adecuadas a implementar en la entidad para mitigar los riesgos y evitar su materialización.

[27] IBERO TIJUANA, ¿Qué es La investigación aplicada y cuáles son sus principales características? [EN LINEA]. 2020. [Citado en 07 de noviembre de 2021]. Disponible en internet: <https://blogposgrados.tijuana.ibero.mx/investigacion-aplicada/>

6 DESARROLLO DE LOS OBJETIVOS

6.1 ANALIZAR EL ESTADO ACTUAL DEL ÁREA DE LAS TICS DEL HOSPITAL SAN VICENTE DE PAÚL MEDIANTE UN INSTRUMENTO PROPUESTO POR EL MINISTERIO DE LAS TIC, CON EL FIN DE CONOCER SI CUENTAN CON CONTROLES DE SEGURIDAD IMPLEMENTADOS.

6.1.1 Actividad 1: Realizar evaluación del estado actual en seguridad informática y de la información haciendo uso del Instrumento de identificación y evaluación del Modelo de Seguridad y Privacidad de la Información del MinTIC.

Teniendo en cuenta que el Hospital San Vicente de Paúl es una institución pública que presta el servicio de atención primaria en salud, se toman como ejemplo algunas de las guías que el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC ha implementado con el fin de fortalecer la Gestión TI en las entidades.

Con el fin de evaluar el estado en el proceso de Gestión de la Seguridad de la Información en el hospital, se hizo uso del “Instrumento de Evaluación MSPI” creado por el MinTIC y cuyo objetivo principal es el de realizar el diagnóstico del nivel de madurez en la implementación del Modelo de Seguridad y Privacidad de la información[28] en las entidades estatales. Para este caso, se realizó el diagnostico teniendo en cuenta los ítems administrativos y técnicos del instrumento, los cuales son basados en los controles implementados por el estándar ISO 27001:2013, lo que permitiría realizar una medición más exacta en la evaluación inicial.

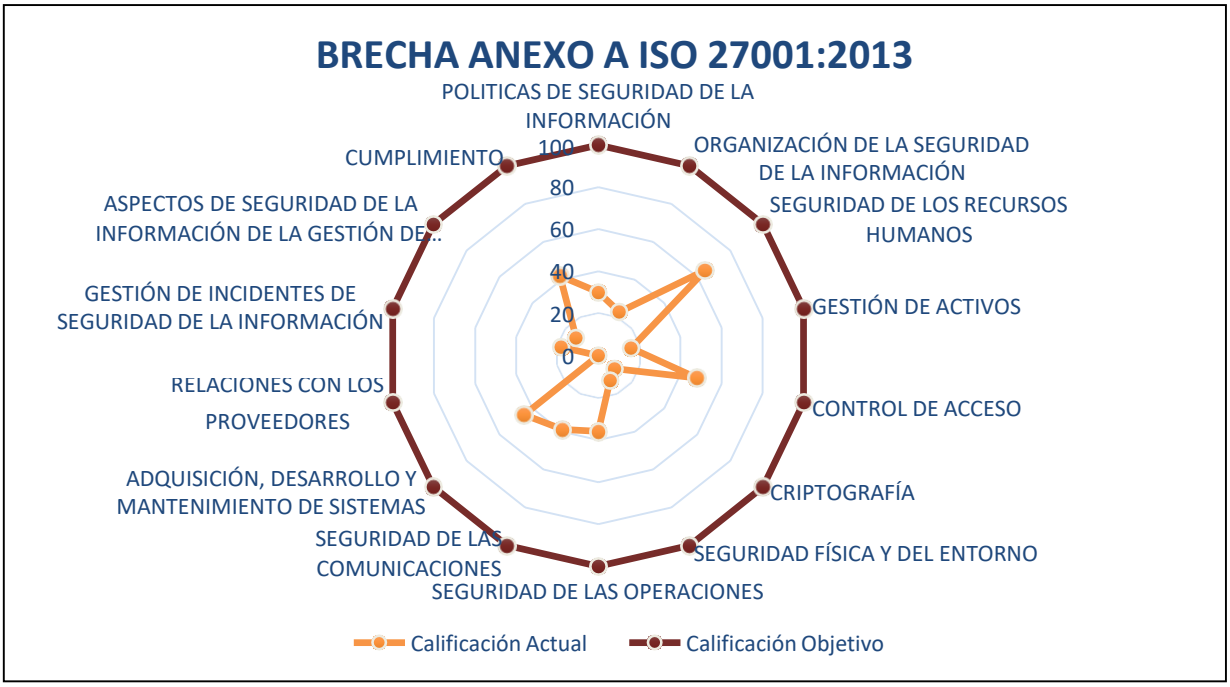
Después de haber realizado la evaluación, calificando de 0 a 100 cada de los ítems técnicos y administrativos reflejados en el instrumento de evolución del MSPI, dicha matriz arroja los resultados en una tabla y son reflejados en un gráfico, en donde se puede observar el nivel logrado en la efectividad de implementación de los dominios de control definidos dentro del modelo.

[28] GOBIERNO DIGITAL, ¿qué Es El MSPI?. [EN LINEA]. [Citado en 28 de agosto de 2022]. Disponible en internet: <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>

Tabla 1 Resultados Instrumento de Evaluación MSPI
Fuente: Elaboración propia

N°	EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - MSPI			
	DOMINIO	Puntuación Actual	Puntuación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	30	100	**REPETIBLE**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	23	100	**REPETIBLE**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	65	100	**GESTIONADO**
A.8	GESTIÓN DE ACTIVOS	16	100	**INICIAL**
A.9	CONTROL DE ACCESO	48	100	**EFECTIVO**
A.10	CRIPTOGRAFÍA	10	100	**INICIAL**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	13	100	**INICIAL**
A.12	SEGURIDAD DE LAS OPERACIONES	36	100	**REPETIBLE**
A.13	SEGURIDAD DE LAS COMUNICACIONES	39	100	**REPETIBLE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	45	100	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	0	100	**INEXISTENTE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	18	100	**INICIAL**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	14	100	**INICIAL**
A.18	CUMPLIMIENTO	42	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**28**	**100**	**REPETIBLE**

Figura 1 Gráfica resultados de avances en controles de seguridad.



Fuente: Elaboración propia

6.1.2 Actividad 2: Análisis de resultados de instrumento de medición.

Después de aplicar el instrumento de medición de implementación del MSPI y revisar sus resultados, se realiza el respectivo análisis en donde se identifica que el Hospital San Vicente de Paúl se encuentra en una fase “repetible”, denominada así dentro de este instrumento, ya que en este nivel se ubican las organizaciones, en las que están definidos procesos primarios de gestión de la seguridad y privacidad de la información y en donde se encuentran políticas y procesos con los que se detectarían posibles riesgos de seguridad, los cuales no están administrados dentro del componente principal de planificación del MSPI.

A continuación, se describen algunos de los principales ítems en donde el hospital tiene mayor puntuación y en donde se ha visto mayor gestión; estos corresponden al modelo de Seguridad de los recursos humanos, Control de acceso y Adquisición, desarrollo y mantenimiento de sistemas:

- El Hospital se asegura de contratar personal idóneo al cargo disponible, realizando un estudio previo por cada vinculación de funcionarios que se realiza.

- Los funcionarios comprenden sus responsabilidades y deberes respecto a su cargo.

- Se realiza respectiva verificación de antecedentes y validación de títulos presentados por el personal.

- Al realizar vínculo con el personal, el hospital solicita autorización de verificación de datos e información personal por medio de formato codificado e implementado por el área de Talento Humano y contratación a todo el personal.

- Acuerdo de contrato con funcionarios y contratistas definiendo claramente responsabilidades y organización de la seguridad de la información.

- En el proceso de inducción, se expone la responsabilidad que cada funcionario tiene con la información compartida y recolectada de los usuarios que asisten al hospital, explicando así la importancia de la privacidad y clasificación de la información conservada en Historias clínicas, ordenes médicas y demás datos.

- Por parte del área de sistemas, se realizan capacitaciones y socializaciones de los planes y políticas implementados a la actualidad con el fin de generar conciencia y fortalecer el conocimiento respecto a la seguridad y privacidad de la información.

- Se cuenta con un protocolo de asignación de roles y permisos en el sistema de información principal del hospital, con el fin de determinar el acceso limitado a la información a los funcionarios según sus cargos.

- Se realiza auditoria constantemente a los usuarios activos en el sistema de información.

- El proceso de asignación de contraseñas cuenta con fuertes validaciones, con el fin de generar contraseñas seguras.

- Las contraseñas son encriptadas al momento de guardar los datos en la base de datos principal del sistema de información, con el fin de no permitir el acceso a terceros a la información privilegiada del hospital.

- En el comité de Historias Clínicas, se realiza verificación de la buena recolección de información en las Historias Clínicas por consulta, por parte del personal

asistencial, con el fin de verificar que todos los datos requeridos dentro de la consulta sean acordes a los solicitados por la ley.

- El acceso al código fuente del sistema de información institucional es restringido al personal, usando validación de acceso al momento de ingresar al servidor principal y por medio de la IP pública.

- Se cuenta con un plan de mantenimiento institucional en donde se describen instrucciones específicas para el mantenimiento y buen uso de los dispositivos informáticos existentes en el inventario del hospital.

- Se tiene establecido un formato específico para la recolección de los datos principales del equipo en una hoja de vida por cada dispositivo y las acciones de mantenimiento realizadas en el formato de mantenimiento.

También se describen los ítems más importantes dentro de cada uno de los modelos que obtuvieron menor puntaje según los resultados del instrumento de medición. Entre dichos modelos encontramos las relaciones con los proveedores, uso de criptografía y seguridad física del entorno:

- El Hospital no cuenta con un plan o política en donde se evidencien los requisitos de S.I. para prevenir amenazas referentes al acceso de tercero y proveedores a algunos de los activos de información de la organización.

- No se evidencian acuerdos que traten el tema de seguridad de la información pertinente que debe tener cada proveedor.

- No se cuenta desarrollada e implementada una política de protección de la información con controles criptográficos.

- En el centro de datos o datacenter principal del hospital, la seguridad perimetral es muy poca, ya que no cuenta con las medidas de seguridad físicas necesarias como puertas metálicas, techo reforzado, chapa de puertas poco seguras, etc.

- El centro de datos no cuenta con sensores de ambiente con el fin de controlar la temperatura ambiente del lugar.

- No se tiene instalado un sistema de aire acondicionado con el fin de controlar la temperatura del cuarto y los dispositivos allí resguardados.

- Algunas oficinas y consultorios en donde reposan dispositivos que resguardan información privilegiada, no cuentan con la seguridad física necesarias.

- No se cuenta con dispositivos especiales como firewall, IDS, IPS, entre otros, que sirven para la protección de la información ante ataques maliciosos o ciberataques.

- No todos los equipos informáticos de la institución cuentan con sistemas de protección contra fallas eléctricas.

- La ubicación de algunas canaletas de la red principal no es la apropiada, permitiendo así el acceso de terceros al cableado de la red.

- No se tiene adoptada una política de escritorio de pantalla limpio para los archivos e información que cada equipo resguarda, con el fin de impartir orden y dar seguridad a los documentos y carpetas.

Finalmente se cierra este primer objetivo, con el cual se puede evidenciar todos los aspectos positivos y debilidades que se encontraron en el área de Tecnologías de la Información y la Comunicación según los controles indicados por el Ministerio de TICs y la cual se puedo obtener a partir de la aplicación del Instrumento de identificación y evaluación del MSPI. Gracias a dicho instrumento, se pudo evidenciar el porcentaje y estado de efectividad de los controles implementados que tienen frente al desarrollo del estándar ISO 27001:2013.

6.2 DETERMINAR LA VULNERABILIDADES, AMENAZAS Y RIESGOS DE SEGURIDAD INFORMÁTICOS A LOS ACTIVOS DE INFORMACIÓN EXISTENTES EN EL ÁREA DE TIC DEL HOSPITAL SAN VICENTE DE PAÚL, BASADOS EN UNA METODOLOGÍA DE GESTIÓN DE RIEGOS, CON EL FIN DE MINIMIZAR LOS RIESGOS.

6.2.1. Actividad 1: Determinar la metodología de gestión de riesgos. La metodología de gestión de riesgos se encarga de asignar la escala en que las amenazas se pueden

materializar sobre los activos causando daños o perdidas en la empresa u organización[29], para poder seleccionar la metodología a implementar describiremos cada una de ellas con sus ventajas y desventajas:

6.2.1.1. CRAMM. (Risk Analysis and Management Method) Es una metodología basada en el análisis de riesgos que fue creada por el gobierno británico y su agencia central de Comunicación y Telecomunicación CCTA, en el año de 1987 se lanza su versión inicial y actualmente está en su versión la 5.2, esta metodología es de gran importancia en la administración pública británica, y de igual manera, en las empresas e instituciones de gran tamaño[30].

CRAMM cuenta con tres fases para realizar el análisis del riesgo:

- Define los objetivos globales de la seguridad
- Se analiza el riesgo identificando la amenazas y vulnerabilidades
- Identificación y selección de las politicas de seguridad, implementando una librería con 3000 medidas de seguridad.

6.2.1.2. CORAS. (Construct a platform for Risk Analysis of Security critical system) Su creación se dio desde el año 2021 por los investigadores noruegos SINTEF que a su vez estaban financiados por las organizaciones del sector público y privado, esta metodología proporciona[31]:

- Análisis de riesgos, presentados en siete pasos los cuales son fundamentales para la entrevista con los expertos y son:
  - ✓ Presentación
  - ✓ Estudio de alto nivel
  - ✓ Aceptación
  - ✓ Identificación
  - ✓ Estimación de riesgos

[29] ISOTOOLS, ¿Cuáles Son Las Metodologías Para La Gestión De Riesgo? [EN LÍNEA]. 2017. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://www.isotools.com.mx/cuales-las-metodologias-la-gestion-riesgo/>

[30] SECURITYARTWORK, Antonio Huerta. Introducción Al Análisis De Riesgos – Metodologías (i). [EN LÍNEA]. 2012. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/>

[31] SEGURIDAD7A, Metodología Coras (construct A Platform For Risk Analysis Of Security Critical System). [Citado en 11 de noviembre de 2021]. Disponible en internet: <http://seguridades7a.blogspot.com/p/coras.html>

- ✓ Evaluación de riesgos
- ✓ Tratamiento de riesgos

- Un lenguaje UML para definir los modelos de activos, amenazas y riesgos.
- Editor grafico que soporta la elaboración de los modelos
- Biblioteca de casos reutilizables
- Herramienta que gestiona los casos
- Representación textual XML

6.2.1.3. MAGERIT. El antiguo Consejo Superior de Administración electrónica de España que en la actualidad es la comisión estratégica TIC fue el encargado de elaborar la metodología Magerit la cual es de índole público, buscando dar cumplimiento a la misión de la creciente utilización de las tecnologías de la información por parte de la sociedad[32]. La versión 3 de la metodología esta estructura en 3 libros: Método, Catálogo de Elementos y guías de técnicas.

Los principales objetivos de la metodología MAGERIT son:

- Sensibilizar a la organización sobre la existencia de amenazas y la importancia de abordarlas.
- Proporcionar un sistema de análisis de riesgos procedentes del uso habitual de las tecnologías de la información y la comunicación.
- Identificar y planificar para abordar los peligros indirectos y controlables de manera oportuna.
- Preparar a las organizaciones para cuando llegue el momento de la auditoría, evaluación, certificación o acreditación.

6.2.1.4. OCTAVE. Esta metodología fue creada en el año 2001 por la universidad Carnegie Mellon de Pensilvania, con el propósito de analizar los riesgos de los principios de confidencialidad, integridad y disponibilidad, el significado de su acrónimo es "Operationally Critical Threat, Asset and Vulnerability Evaluation"[33], esta metodología cuenta con 3 versiones:

[32] PAEPORTALADMINISTRACIONELECTRONICA, Magerit V.3: Metodología De Análisis Y Gestión De Riesgos De Los Sistemas De Información. [EN LÍNEA]. [Citado en 11 de noviembre de 2021]. Disponible en internet: <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html>

[33] SECURITYARTWORK, Antonio Huerta. Introducción Al Análisis De Riesgos – Metodologías (ii). [EN LÍNEA]. 2012. [Citado en 11 de noviembre de 2021]. Disponible en internet:

- La versión OCTAVE original.
- La versión OCTAVE-S para PYMES.
- La versión OCTAVE-ALLEGRO simplificada.

La Metodología cuenta con tres fases de desarrollo[34]:

- Fase 1: es la fase encargada de los activos, las amenazas, vulnerabilidades que lleguen a tener las empresas u organizaciones, exigiendo seguridad y normas.
- Fase 2: Esta fase es la continuación de los procesos de la anterior, realizando un correcto análisis y gestionando los riesgos en el interior de las empresas u organizaciones.
- Fase 3: Se encarga de evaluar los riesgos, realiza la estrategia de protección con el fin de crear los planos de reducción de los riesgos.

Tabla 2 Ventajas y Desventajas de las metodologías

NOMBRE METODOLOGÍA	VENTAJA Y DESVENTAJAS
CRAMM Aplica a: Organizaciones públicas y privadas	**Ventajas:** Es aplicable a los sistemas y redes de información con el propósito de completar, desarrollar e implementar el ciclo de vida dentro de un S.I., y proporcionar políticas de seguridad y todos los demás recursos de políticas de manera formal, estructurada y reglamentaria. **Desventajas:** Esta metodología no implementa elementos de procesos y recursos.
CORAS	**Ventajas:** Es una metodología que brinda herramientas para el desarrollo y mantenimiento a aplicarse en los nuevos sistemas. Se encargar de mostrar las vulnerabilidades que pueda encontrar en sus procesos. **Desventajas:** No se encarga de examinar los riesgos cuantitativos, ni utiliza elementos de procesos y dependencias.
MAGERIT	**Ventajas:** Cuenta con bastantes recursos informáticos, amenazas y todo tipo de activos, es de uso libre y no es necesario adquirir

<https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/>

[34] SGSI, Metodología Octave Para El Análisis De Riesgos En SGSI. [EN LINEA]. 2021. [Citado en 11 de noviembre de 2021]. Disponible en internet: <https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-analisis-de-riesgos-en-sgsi/>

Aplica a: El Estado, empresas grandes, pymes y pequeñas empresas.	autorización para su uso. Unos de sus principales complementos es el análisis y la gestión del riesgo, implementando herramientas para el análisis de riesgo como PILAR. Implementa análisis de riesgo de manera cuantitativa y cualitativa para ir preparando a las empresas u organizaciones para presentar los procesos de evaluación, auditoria y acreditación. **Desventajas:** Esta metodología no implementa procesos, recursos, ni vulnerabilidades, es catalogada costosa para implementar su aplicación.
OCTAVE Aplica a: Pymes, pequeñas empresas y empresas del sector público y privado.	**Ventajas:** Es una metodología de fácil desarrollo, permitiendo a las organizaciones utilizar a sus funcionarios para el desarrollo de la misma, creando así equipos multidisciplinarios. **Desventajas:** Este es un método que no tiene una definición clara de los activos de información, además implementa una literatura muy rica para el análisis de riesgos.

Fuente: ALEMÁN NOVOA, Helena. y RODRIGUEZ BARRERA, Claudia. Metodologías Para El Análisis De Riesgos En Los SGSI. Boyacá.: Fundación Universitaria Juan De Castellanos. 2014. 7-10p.

Después de revisadas las ventajas y desventajas, se toman características descriptivas comunes de cada una de ellas, permitiendo realizar un análisis y la comparación de cada metodología:

- Ámbito de aplicación: Es el tipo de entidad u organización la cual tendrá el respaldo de la metodología.
- Costo de implementación: Es el valor económico con el cual debe contar la empresa u organización para implementar la tecnología.
- Disponibilidad de profesionales: Es la facilidad de poder encontrar información, personal idóneo y proyectos ya aplicados en Colombia.
- Licenciamiento: Es la que indica si es necesaria la adquisición de una licencia para poder utilizar la metodología.
- Incluye estándares de seguridad: Esta metodología aplica estrategias sobre el control o protección de las fuentes de información.

Con el fin de realizar la evaluación para escoger la metodología a aplicar en el proyecto, se le asignó un valor por cada una de las características, donde 3 es la mayor puntuación y 1 la más baja, un desglose de dichos ítems del método elegido se presenta en la siguiente tabla:

Tabla 3 evaluación de metodologías

METODOLOGÍAS					
CARACTERÍSTICAS	**Importancia (1 a 3 donde 3 es mayor puntaje)**	**Cramm**	**Coras**	**Magerit**	**Octave**
Ámbito de aplicación	3	3	3	3	3
Costo de implementación	3	1	2	3	2
Disponibilidad	3	2	1	3	1
Licenciamiento	3	2	1	3	1
Controles de seguridad	2	3	1	3	3
TOTAL:		33	24	42	27

Fuente: Elaboración Propia

Al realizar la sumatoria de cada puntuación de las características de las metodologías, multiplicado por la importancia de la misma, se obtuvo el mayor puntaje para la metodología MAGERIT, siendo esta la metodología escogida para realizar el análisis de riesgos del Hospital San Vicente de Paúl del municipio de Fresno Tolima.

6.2.2. Actividad 2: Realizar inventario de los activos de información. La búsqueda de cada uno de los activos de información se llevó a cabo bajo los parámetros propuestos por la metodología MAGERIT y gracias al acompañamiento del Ingeniero de Sistemas de la oficina de tecnologías de la información del Hospital, que por medio de entrevistas y reuniones pudo obtener la siguiente tabla:

Tabla 4 Inventario de Activos

Nombre del Activo	Cantidad	Responsable
Tipo: [D] Datos		
Base de Datos MySQL	1	Administrador del sistema
Tipo: [K] Claves criptográficas		
Firma electrónica Gerencia	1	Gerente
Firma electrónica Contador	1	Contador
Tipo: [SW] Servicios		
Página web	1	MinTIC y Profesional área TICs
Intranet	1	Profesional área TICs
Correo electrónico	55	MinTIC y líderes de procesos

Almacenamiento en la nube - Google Drive	1	MinTIC y líderes de procesos
Tipo: [SW] Software		
Sistemas operativos	1	Profesional área TICs
Antivirus	1	Profesional área TICs
Software Microsoft	1	Profesional área TICs
Tipo: [HW] Hardware		
Servidor	1	Profesional área TICs
Computadores	78	Profesional área TICs
portátiles	4	Profesional área TICs
Impresoras	32	Profesional área TICs
Escáner	4	Profesional área TICs
Switches	9	Profesional área TICs
Access Point	8	Profesional área TICs
Tipo: [COM] Redes de comunicación		
Red LAN	1	Profesional área TICs
Red WIFI	1	Profesional área TICs
Internet	1	Profesional área TICs
Tipo: [Media] Soportes de información		
Discos duros Externos	3	Líderes de procesos
Memorias USB	8	Líderes de procesos
Tipo: [AUX] Elementos auxiliares		
UPS	47	Profesional área TICs
Reguladores	75	Profesional área TICs
Cableado estructurado	1	Profesional área TICs
Tipo: [L] Instalaciones físicas		
Data Center	1	Profesional área TICs
Oficinas	1	Líderes de procesos
Tipo: [P] Personal		
Ingeniero de sistemas	1	Jefe de personal

Fuente: elaboración propia

6.2.3 Actividad 3: valoración de cada una de los tres pilares de seguridad para los activos de información. Para los activos de información de la oficina de TICs del Hospital San Vicente de Paúl de Fresno Tolima, se definió como factores de evaluación la disponibilidad, la confidencialidad y la integridad. Estas tres dimensiones representan

propiedades de la información que se pueden amortizar en una amenaza. Las tres dimensiones de seguridad serán definidas en las siguientes tablas de valoración:

6.2.3.1 Disponibilidad: es uno de los aspectos fundamentales de la seguridad de la información, basándose en facilitar el acceso a los datos de personas y organizaciones con el fin de poder realizar un trabajado ya definido.

Tabla 5 Valoración de la Disponibilidad

Valor Cuantitativo	Valor Cualitativo	Descripción
1	Bajo	Es posible que el activo no encuentre disponible por un día.
2	Medio	El activo al no encontrarse disponible por 8 horas, presentará inconvenientes al momento de cumplir con actividades propuestas.
3	Alto	seria crítico para la entidad, la no reparación del activo en menos de una hora.

Fuente: Elaboración propia

6.2.3.2 Confidencialidad: es la garantía que se ofrece a la información, con el fin de que sea manipulada solo por las personas autorizadas para acceder a ella, esta dimensión fue definida por la norma internacional ISO/IEC 27002.

Tabla 6 Valoración de la Confidencialidad

Valor Cuantitativo	Valor Cualitativo	Descripción
1	Bajo	Información pública / al ser divulgada sin autorización, no genera inconvenientes a la entidad.
2	Medio	Información clasificada / esta publicación sin autorización, incumplen las políticas de privacidad y seguridad de la información.
3	Alto	La información confidencial / publicación no autorizada de activos puede afectar la imagen de la entidad o conducir a un comportamiento ilegal.

Fuente: Elaboración propia

6.2.3.3 Integridad: Es la encargada de mantener la información tal y como se creó, previniendo modificaciones mal intencionadas de la misma.

Tabla 7 Valoración de la Integridad

Valor Cuantitativo	Valor Cualitativo	Descripción
1	Bajo	La modificación del activo no tendría mucha relevancia para la entidad.
2	Medio	La modificación del activo presenta un impacto medio para la entidad.
3	Alto	La modificación del activo presenta un impacto crítico para la entidad.

Fuente: Elaboración propia

6.2.3.4 Activo: es un cálculo realizado con cada evaluación de la dimensión de seguridad para determinar la severidad del contenido encontrado en la oficina de sistemas del Hospital San Vicente de Paúl de Fresno Tolima, expresado en Niveles Bajo, Medio y Alto. Los activos de medianos y altos serán seleccionados como activos para la valoración de riesgos.

Tabla 8 Criticidad de los Activos

Valor Cuantitativo	Valor Cualitativo	Descripción
1	Bajo	Representa un impacto bajo o no significativo para la institución.
2	Medio	Representa un impacto medio o medianamente crítico para la entidad.
3	Alto	Representa un impacto fuerte para la institución.

Fuente: Elaboración propia

El enfoque de esta metodología, propone una selección de activos, cuyo propósito es identificar los riesgos más representativos para cada una de ellas, estableciendo así una relación.

Las categorías propuestas por Magerit son:

- Datos [D]
- Claves criptografías [k]
- Servicios [S]
- Software [S]
- Hardware [H]
- Redes de comunicación [COM]
- Soporte de información [Media]
- Elementos auxiliares [AUX]
- Instalaciones físicas [L]
- Personal [P]

Tabla 9 Dimensiones activos de información

Nombre del Activo	Valoración de Dimensiones			Valor Cuantitativo (Criticidad)	Valor Cuantitativo (Criticidad)
	D	C	I		
Tipo: [D] Datos					
Base de Datos MySQL	3	3	3	3	Alto
Tipo: [K] Claves criptográficas					
Firma electrónica Gerencia	2	3	3	3	Alto
Firma electrónica Contador	2	3	3	3	Alto
Tipo: [SW] Servicios					
Página web	3	2	2	2	Medio
Intranet	2	2	2	2	Medio
Correo electrónico	2	2	3	2	Medio
Almacenamiento en la nube - Google Drive	2	3	3	3	Alto
Tipo: [SW] Software					
Sistemas operativos	3	2	1	2	Medio
Antivirus	2	1	2	2	Medio
Software Microsoft	1	2	2	2	Medio
Tipo: [HW] Hardware					
Servidor	3	3	3	3	Alto
Computadores	1	2	1	1	Bajo

portátiles	1	2	1	1	Bajo
Impresoras	1	1	1	1	Bajo
Escáner	1	1	1	1	Bajo
Switches	3	1	3	2	Medio
Access Point	1	1	1	1	Bajo
Tipo: [COM] Redes de comunicación					
Red LAN	3	2	3	3	Alto
Red WIFI	2	3	1	3	Alto
Internet	3	1	1	2	Medio
Tipo: [Media] Soportes de información					
Discos duros Externos	1	3	3	2	Medio
Memorias USB	1	3	3	2	Medio
Tipo: [AUX] Elementos auxiliares					
UPS	3	1	1	2	Medio
Reguladores	3	1	1	2	Medio
Cableado estructurado	3	1	1	2	Medio
Tipo: [L] Instalaciones físicas					
Data Center	3	3	3	3	Alto
Oficinas	1	1	1	1	Bajo
Tipo: [P] Personal					
Ingeniero de sistemas	1	3	1	2	Medio

Fuente: Elaboración propia

6.2.4 Actividad 4: Identificar las amenazas a las que se encuentran expuestos los activos. Son los comportamientos que se utilizan para amenazar la seguridad de los sistemas de información. El método Magerit proporciona una lista de amenazas clasificadas por su origen, las cuales son:

Tabla 10 Lista de amenazas

Ítem	Amenaza
[N] Desastres Naturales	
1	[N.1] Fuego
2	[N.2] Daños por agua
3	[N.*] Desastres Naturales

[I] De origen industrial	
5	[I.1] Fuego
6	[I.2] Daños por agua
7	[I.*] Desastres industriales
8	[I.3] Contaminación mecánica
9	[I.4] Contaminación electromagnética
10	[I.5] Avería de origen físico o lógico
11	[I.6] Corte del suministro eléctrico
12	[I.7] Condiciones inadecuadas de temperatura o humedad
13	[I.8] Fallo de servicios de comunicaciones
14	[I.9] Interrupción de otros servicios y suministros esenciales
15	[I.10] Degradación de los soportes de almacenamiento de la información
16	[I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	
17	[E.1] Errores de los usuarios
18	[E.2] Errores del administrador
19	[E.3] Errores de monitorización (log)
20	[E.4] Errores de configuración
21	[E.7] Deficiencias en la organización
22	[E.8] Difusión de software dañino
23	[E.9] Errores de [re-]encaminamiento
24	[E.10] Errores de secuencia
25	[E.14] Escapes de información
26	[E.15] Alteración accidental de la información
27	[E.18] Destrucción de información
28	[E.19] Fugas de información
29	[E.20] Vulnerabilidades de los programas (software
30	[E.21] Errores de mantenimiento / actualización de programas (software)
31	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
32	[E.24] Caída del sistema por agotamiento de recursos
33	[E.25] Pérdida de equipos
34	[E.28] Indisponibilidad del personal
[A] Ataques intencionados	
35	[A.3] Manipulación de los registros de actividad (log)
36	[A.4] Manipulación de la configuración
37	[A.5] Suplantación de la identidad del usuario

38	[A.6] Abuso de privilegios de acceso
39	[A.7] Uso no previsto
40	[A.8] Difusión de software dañino
41	[A.9] [Re-]encaminamiento de mensajes
42	[A.10] Alteración de secuencia
43	[A.11] Acceso no autorizado
44	[A.12] Análisis de tráfico
45	[A.13] Repudio
46	[A.14] Interceptación de información (escucha)
47	[A.15] Modificación deliberada de la información
48	[A.18] Destrucción de información
49	[A.19] Divulgación de información
50	[A.22] Manipulación de programas
51	[A.23] Manipulación de los equipos
52	[A.24] Denegación de servicio
53	[A.25] Robo
54	[A.26] Ataque destructivo
55	[A.27] Ocupación enemiga
56	[A.28] Indisponibilidad del personal
57	[A.29] Extorsión
58	[A.30] Ingeniería social (picaresca)

Fuente: GOBIERNO DE ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Catálogo de Elementos. 2012.

6.2.5 Actividad 5: Valoración de las amenazas. Las amenazas no generan daño a todos los activos, de igual manera sus dimensiones de seguridad tampoco son afectadas con la misma medida, por lo cual se establece cuales amenazas llegan a perjudicar al activo para valorar su nivel de afectación, para realizar la valoración se utilizarán las dimensiones de impacto y probabilidad.

6.2.5.1 Probabilidad: es el análisis que se le realiza a la amenaza con el fin de poderla materializar, teniendo en cuenta la siguiente tabla, el análisis se realiza de acuerdo a la categorización.

Tabla 11 Nivel de Probabilidad

	Nomenclatura	Categoría	Frecuencia	Valoración
Probabilidad	MA	Prácticamente seguro	A diario	5
	A	Probable	Mensual	4
	M	Posible	Anual	3
	B	Poco probable	Cada varios años	2
	MB	Muy raro	Siglos	1

Fuente: Elaboración propia

6.2.5.2 Impacto: Se estudia cuál sería el impacto o daño generado por el activo ante dicho riesgo, como se indica en la siguiente tabla:

Tabla 12 Nivel de Impacto

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy bajo	1

Fuente: Elaboración propia

6.2.6 Actividad 6: valoración del riesgo. Un riesgo es el posible daño a un sistema, y cuando se conoce el impacto de una amenaza en los activos, el riesgo puede determinarse por la frecuencia con la que ocurre. El riesgo aumenta con el impacto y la frecuencia.

El cálculo del riesgo se puede realizar a partir de un análisis cuantitativo, multiplicando los factores probabilidad e impacto.

$$\text{Riesgo} = \text{Impacto x Probabilidad}$$

Tabla 13 Valoración del riesgo

	Nomenclatura	Categoría	Valoración
Valoración del Riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Medio	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Elaboración propia

Después de definir como se realizará dicha calificación, se establece la matriz de valoración de riesgos evaluando los activos de información con mayor importancia en el Hospital San Vicente de Paúl:

Tabla 14 Matriz de valoración de riesgos

Activo	Amenazas	Impacto en cada dimensión			Impacto	Probabilidad	Nivel de riesgo
		D	C	I			
Base de Datos MySQL	[I.9] Interrupción de otros servicios y suministros esenciales	5	2	2	M	B	BAJO
	[I.10] Degradación de los soportes de almacenamiento de la información	5	1	1	B	M	BAJO
	[E.2] Errores del administrador	3	4	4	A	B	BAJO
	[E.3] Errores de monitorización (log)	3	4	2	M	B	BAJO
	[E.4] Errores de configuración	4	5	2	A	M	MEDIO
	[E.14] Escapes de información	2	5	2	M	M	BAJO
	[E.15] Alteración accidental de la información	2	5	5	A	B	BAJO
	[E.18] Destrucción de información	5	5	5	MA	B	MEDIO
	[E.19] Fugas de información	2	5	3	M	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	2	2	M	M	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	4	2	2	M	M	BAJO
	[A.3] Manipulación de los registros de actividad (log)	2	4	5	A	B	BAJO

	[A.4] Manipulación de la configuración	4	5	5	MA	B	MEDIO
	[A.5] Suplantación de la identidad del usuario	2	5	5	A	M	BAJO
	[A.11] Acceso no autorizado	2	5	3	M	B	BAJO
Claves criptográficas	[E.1] Errores de los usuarios	-	-	2	B	A	BAJO
	[E.2] Errores del administrador	4	4	3	A	A	IMPORTANTE
	[E.14] Escapes de información	-	-	4	A	M	MEDIO
	[E.15] Alteración accidental de la información	-	2	-	B	M	BAJO
	[E.18] Destrucción de información	3	-	-	M	M	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	A	A	IMPORTANTE
Intranet	[E.2] Errores del administrador	3	-	3	M	M	BAJO
	[E.4] Errores de configuración	3	-	3	M	M	BAJO
	[E.15] Alteración accidental de la información	3	-	5	A	B	BAJO
	[E.18] Destrucción de información	5	-	3	A	B	BAJO
	[E.19] Fugas de información	-	4	-	A	B	BAJO
	[E.20] Vulnerabilidades de los programas (software)	4	-	-	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	A	M	MEDIO
	[A.4] Manipulación de la configuración	-	-	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	3	5	5	A	B	BAJO
	[A18] Destrucción de información	4	-	4	A	B	BAJO
	[A19] Divulgación de información	-	4	-	A	B	BAJO
Página web	[E.2] Errores del administrador	3	-	3	M	M	BAJO
	[E.4] Errores de configuración	3	-	3	M	M	BAJO
	[E.15] Alteración accidental de la información	3	-	5	A	B	BAJO
	[E.18] Destrucción de información	5	-	3	A	B	BAJO
	[E.19] Fugas de información	-	4	-	A	B	BAJO

	[E.20] Vulnerabilidades de los programas (software)	5	-	-	MA	A	IMPORTANTE
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	-	-	MA	A	IMPORTANTE
	[E.28] Indisponibilidad del personal	5	-	-	MA	M	MEDIO
	[A.4] Manipulación de la configuración	-	-	5	MA	B	MEDIO
	[A.6] Abuso de privilegios de acceso	-	4	4	A	B	BAJO
	[A.15] Modificación deliberada de la información	3	3	3	M	B	BAJO
	[A18] Destrucción de información	4	-	4	A	B	BAJO
	[A19] Divulgación de información	-	4	-	A	B	BAJO
	[A.24] Denegación de servicio	5	-	-	MA	B	MEDIO
Correo electrónico	[E.8] Difusión de software dañino	3	3	3	M	M	BAJO
	[E.19] Fugas de información	-	-	5	MA	A	IMPORTANTE
	[E.28] Indisponibilidad del personal	4	-	-	A	M	MEDIO
	[A.7] Uso no previsto	3	3	5	A	MA	IMPORTANTE
	[A.8] Difusión de software dañino	4	4	4	A	M	MEDIO
	[A30] Ingeniería social (picaresca)	-	-	4	A	MA	IMPORTANTE
Almacenamiento en la nube	[I.8] Fallo de servicios de comunicaciones	5	-	-	MA	A	IMPORTANTE
	[E.1] Errores de los usuarios	3	-	-	M	M	BAJO
	[E.2] Errores del administrador	4	-	-	A	B	BAJO
	[E.14] Escapes de información	-	4	-	A	B	BAJO
	[E.15] Alteración accidental de la información	-	-	4	M	B	BAJO
	[E.18] Destrucción de información	2	-	3	MA	B	BAJO
	[E.19] Fugas de información	-	5	-	A	B	MEDIO
	[A.11] Acceso no autorizado	-	4	-	A	B	BAJO
	[A.15] Modificación deliberada de la información	-	-	4	A	B	BAJO
	[A18] Destrucción de información	4	-	4	A	B	BAJO
	[A19] Divulgación de información	-	4	-	A	B	BAJO
	[A24] Denegación de servicio	4	-	-	A	M	MEDIO

Sistema Operativo	[E.4] Errores de configuración	4	-	4	A	B	BAJO
	[E.8] Difusión de software dañino	4	-	4	A	B	BAJO
	[E.20] Vulnerabilidades de los programas (software)	5	-	5	MA	B	MEDIO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	B	BAJO
Antivirus	[A.4] Manipulación de la configuración	-	-	5	MA	B	MEDIO
	[A.6] Abuso de privilegios de acceso Antivirus	4	-	-	A	B	BAJO
	[E.2] Errores del administrador	3	-	-	M	M	BAJO
	[E.4] Errores de configuración	3	-	-	M	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	3	-	-	M	M	BAJO
Software Microsoft Office	[I.8] Fallo de servicios de comunicaciones	5	-	-	MA	A	IMPORTANTE
	[E.1] Errores de los usuarios	3	-	-	M	M	BAJO
	[E.2] Errores del administrador	4	-	-	A	B	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	4	-	-	A	B	BAJO
	[A.11] Acceso no autorizado	-	4	-	A	B	BAJO
	[A.15] Modificación deliberada de la información	-	-	4	A	B	BAJO
Servidor	[N.1] Fuego	5	-	-	MA	A	IMPORTANTE
	[N.2] Daños por agua	5	-	-	MA	MB	BAJO
	[N.*] Desastres naturales	5	-	-	MA	B	MEDIO
	[I.5] Avería de origen físico o lógico	4	-	-	A	B	BAJO
	[I.6] Corte del suministro eléctrico	5	-	-	MA	M	MEDIO
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	MA	M	MEDIO
	[A25] Robo	5	-	-	MA	B	MEDIO
	[A26] Ataque destructivo	5	-	-	MA	B	MEDIO
Equipos informáticos	[N.1] Fuego	5	-	-	MA	B	MEDIO
	[N.2] Daños por agua	5	-	-	MA	MB	BAJO
	[N.*] Desastres naturales	5	-	-	MA	B	MEDIO
	[I.5] Avería de origen físico o lógico	4	-	-	A	B	BAJO
	[I.6] Corte del suministro eléctrico	5	-	-	MA	M	MEDIO

	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	MA	M	MEDIO
	[A25] Robo	5	5	-	MA	A	IMPORTANTE
	[A26] Ataque destructivo	5	-	-	MA	B	MEDIO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	MA	B	MEDIO
	[E.19] Fugas de información	-	5	-	MA	A	IMPORTANTE
	[E.25] Pérdida de equipos	-	5	-	MA	A	IMPORTANTE
Access Point	[N.1] Fuego	5	-	-	MA	B	MEDIO
	[N.2] Daños por agua	5	-	-	MA	B	MEDIO
	[N.*] Desastres naturales	5	-	-	MA	MB	BAJO
	[I.5] Avería de origen físico o lógico	5	-	-	MA	M	MEDIO
	[I.6] Corte del suministro eléctrico	5	-	-	MA	M	MEDIO
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	MA	B	MEDIO
	[E.2] Errores del administrador	4	-	3	A	B	BAJO
	[E.4] Errores de configuración	4	-	3	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	A	MA	IMPORTANTE
	[E.25] Pérdida de equipos	5	5	-	MA	MB	BAJO
	[A.4] Manipulación de la configuración	4	-	3	A	B	BAJO
	[A.6] Abuso de privilegios de acceso	4	-	3	A	B	BAJO
	[A.11] Acceso no autorizado	4	-	3	A	B	BAJO
	[A.14] Interceptación de información (escucha)	2	4	2	M	M	BAJO
	[A.23] Manipulación de los equipos	5	-	5	MA	M	MEDIO
	[A.25] Robo	5	-	-	MA	B	MEDIO
Red	[E.2] Errores del administrador	4	-	-	A	B	BAJO
	[E.3] Errores de monitorización (log)	4	-	-	A	B	BAJO
	[E.9] Errores de [re-]encaminamiento	4	-	-	A	B	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	5	-	-	MA	B	MEDIO
	[E.28] Indisponibilidad del personal	5	-	-	MA	M	MEDIO
	[A.12] Análisis de tráfico	-	5	-	MA	M	MEDIO

	[A.14] Interceptación de información (escucha)	-	5	-	MA	B	MEDIO
Internet	[E.2] Errores del administrador	4	-	-	A	B	BAJO
	[E.3] Errores de monitorización (log)	4	-	-	A	B	BAJO
	[E.9] Errores de [re-]encaminamiento	4	-	-	A	B	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	5	-	-	MA	A	IMPORTANTE
	[E.28] Indisponibilidad del personal	5	-	-	MA	M	MEDIO
	[A.12] Análisis de tráfico	-	5	-	MA	M	MEDIO
	[A.14] Interceptación de información (escucha)	-	5	-	MA	B	MEDIO
Dispositivos de almacenamiento	[N.1] Fuego	5	-	-	MA	A	IMPORTANTE
	[N.2] Daños por agua	5	-	-	MA	MB	BAJO
	[I.5] Avería de origen físico o lógico	4	-	-	A	B	BAJO
	[I.7] Condiciones inadecuadas de temperatura o humedad	4	-	-	A	B	BAJO
	[A25] Robo	5	-	-	MA	A	IMPORTANTE
	[A26] Ataque destructivo	5	-	5	MA	MA	CRITICO
Dispositivos de Protección eléctrica	[N.1] Fuego	5	-	-	MA	A	IMPORTANTE
	[N.2] Daños por agua	5	-	-	MA	MB	BAJO
	[I.5] Avería de origen físico o lógico	4	-	-	A	B	BAJO
	[I.7] Condiciones inadecuadas de temperatura o humedad	4	-	-	A	B	BAJO
	[A25] Robo	5	-	-	MA	A	IMPORTANTE
	[A26] Ataque destructivo	5	-	-	MA	B	MEDIO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	MA	M	MEDIO
Cableado Estructurado	[N.2] Daños por agua	3	-	-	M	B	BAJO
	[I.11] Emanaciones electromagnéticas	4	-	-	A	B	BAJO
	[A26] Ataque destructivo	5	-	-	MA	B	MEDIO
Centro de datos	[N.1] Fuego	5	-	-	MA	B	MEDIO
	[N.2] Daños por agua	4	-	-	A	B	BAJO
	[N.*] Desastres naturales	5	-	-	MA	MB	BAJO
	[I.1] Fuego	5	-	-	MA	A	IMPORTANTE
	[A.11] Acceso no autorizado	5	5	-	MA	MA	CRITICO
Recursos humanos	[E.28] Indisponibilidad del personal	5	-	-	MA	A	IMPORTANTE
	[E.7] Deficiencias en la organización	4	-	-	A	B	BAJO

Fuente: Elaboración propia

6.2.7 Actividad 7: Análisis de resultados matriz de riesgos.

Después de haber calificado el nivel de riesgo por cada vulnerabilidad encontrada en los activos de información, se realiza el análisis de dichos resultados para definir estrategias de cómo serán manejados y tratados.

Tabla 15 Niveles de tratamiento de riesgos

Nivel de Riesgo	Tratamiento del Riesgo
Crítico	Se mitiga el riesgo por medio de estrategias y controles.
Importante	Se mitiga el riesgo por medio de controles preventivos.
Medio	El riesgo puede ser reducido con pólizas de seguros.
Bajo	Finaliza el proceso.

Fuente: Elaboración propia

A continuación, visualizaremos la tabla con los resultados totales de la cantidad de riesgos por cada nivel descrito:

Tabla 16 Conteo de amenazas según el nivel de riesgo

		PROBABILIDAD				
RIESGO		**MB**	**B**	**M**	**A**	**MA**
IMPACTO	**MA**	5	23	12	14	3
	A	0	41	15	7	3
	M	0	7	13	5	2
	B	0	0	2	1	0
	MB	0	0	0	0	0

Fuente: Elaboración propia

El siguiente es el análisis de los resultados en la cantidad de vulnerabilidades por riesgo según los dos niveles en situación grave:

- **Nivel Crítico**

La seguridad en el centro de datos principal del hospital es muy baja, tanto en la infraestructura física como en la lógica. Actualmente dicho sitio es el lugar de almacenamiento de los principales dispositivos de interconexión y almacenaje de información del Hospital, lo que incrementa su importancia. Existen controles de acceso para acceder a dicho lugar, pero son muy mínimos, ya que no se cuenta con puertas y ventanas reforzadas, el cuarto no está sellado herméticamente, la puerta principal es de madera, no existen dispositivos para supervisar y mantener un ambiente apropiado para que los equipos allí resguardados no presenten fallas.

La pérdida de información en bases de datos, dispositivos de almacenamiento y equipos informáticos es un riesgo muy latente en la institución. El área de sistemas cuenta con un disco duro extraíble en donde conserva copias de seguridad de la base de datos del sistema de información institucional SIHOS y resguarda copias de seguridad de los equipos que manejan información privilegiada, pero estos no son controles suficientes para evitar la pérdida de archivos.

En la zona, constantemente, se presentan fallas en la infraestructura del sistema de fluido eléctrico, por lo cual los equipos que no cuentan con UPS se apagan repentinamente y de manera abrupta, lo que ha ocasionado en varias veces que el Disco Duro de computadores entre en corto y dejen de funcionar, lo que no permite poder salvar la información en ellos resguardados. También se presenta perdida de información debido al mal uso de dispositivos como Discos Duros Extraíbles y memorias USB ya que son conectados a equipos externos siendo así contagiadas por virus informáticos que cifran la información y archivos guardados bloqueando permanentemente el acceso a ellas.

- **Nivel Importante**

El hospital no se encuentra exento de presentar problemas en sus instalaciones por causas de desastres naturales. Este siempre es y será un riesgo latente que puede perjudicar muchos procesos entre si relacionados, lo que podría entorpecer la prestación de servicios de salud oportunamente. En el hospital no se cuenta con dispositivos sensores contra incendios e inundaciones lo que permite que este tipo de riesgos puedan ser fácilmente materializables en cualquier área de la institución.

El centro de datos principal de la institución no cuenta con dispositivos de protección como firewalls, IDS, IPS, DNS, VPN, herramientas utilizadas con el fin de aumentar la seguridad y evitar el acceso de intrusos y atacantes a la red y equipos de alta importancia para la arquitectura informática del hospital. A pesar de que el personal recibe capacitaciones y charlas sobre la implementación de seguridad informática y de la

información, no aplican lo socializado. Generalmente son víctimas de perdida de información, ingeniería social, infección de dispositivos por virus, desconfiguración de plataformas y sistemas, entre otros incidentes.

Actualmente se cuenta con una base pequeña de políticas o estrategias con el fin de incrementar la seguridad y privacidad de la información, se recomienda que estas sean revisadas, actualizadas y fortalecidas con el fin de generar controles de seguridad más estrictos en el uso de plataformas y equipos dentro de las instalaciones y red del hospital.

La institución cuenta con servicio de apoyo contratado anualmente para dar soporte, actualizar y solucionar errores en el sistema de información institucional. Sucede constantemente que los ingenieros de desarrollo, al implementar la solución a un caso presentado y anteriormente notificado por parte del administrador del sistema, realizan cambios en algunos módulos afectando y cambiando las funciones de otros módulos, lo que atrasa los procesos asistenciales y administrativos creando un cuello de botella en la recolección de información en la base de datos principal y materializando el riesgo de pérdida de información.

6.3 DESARROLLAR EL DOCUMENTO DE APLICABILIDAD BASADO EN LOS RESULTADOS DEL ANÁLISIS Y EVALUACIÓN DEL RIESGO EN EL ÁREA DE TIC, CON EL FIN DE DETERMINAR LOS CONTROLES REQUERIDOS PARA EL ENDURECIMIENTO DE LA SEGURIDAD.

6.3.1 Documento de Aplicabilidad.

Este documento es una lista de chequeo que permite establecer los controles y políticas de la ISO 27001 que se implementaran con el fin de contar con una información segura, disponible y confiable[35].

Tabla 17 Documento de aplicabilidad

Política para la seguridad de la información		**Control seleccionado**		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**
Políticas para la seguridad de la información	**Control:** Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes	X		En el Hospital San Vicente de Paul se realiza la socialización de acuerdo a la política de seguridad.
Revisión de las políticas para la	**Control:** Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios	X		Establezca un cronograma anual para revisar la política y actualícelo según sea necesario.

[35] Andres Felipe. Tips Para Implementar La Declaración De Aplicabilidad (incluye Modelo En Excel). [EN LINEA]. 2020. [Citado en 25 de febrero de 2022]. Disponible en internet: <https://blog.kawak.net/mejorando_sistemas_de_gestion_iso/tips-para-implementar-la-declaracion-de-aplicabilidad-descarga-excel>

seguridad de la información	significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.			
Organización de seguridad de la información		**Control seleccionado**		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**
Roles y responsabilidades para la seguridad de la información	**Control:** Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	X		Asignación de resoles y responsabilidades según manual de funciones al personal que corresponda.
Separación de deberes	**Control:** Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	X		El personal de la institución adopta las políticas para proteger la información según sea su cargo o área.
Contacto con las autoridades	**Control:** Se deben mantener contactos apropiados con las autoridades pertinentes	X		Documentación de informes de incidentes de seguridad y procedimientos.
Seguridad de los recursos humanos		**Control seleccionado**		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**

Términos y condiciones del empleo	**Control:** Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información	X	Establecer acuerdo de confidencialidad de la información.
Responsabilidades de la dirección	**Control:** La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización	X	Gestionar el cumplimiento de las políticas y planes de seguridad de la información y desarrollar pautas y estrategias de seguridad de la información adecuadas a las diversas funciones de los funcionarios.
Toma de conciencia, educación y la formación en la seguridad de la información	**Control:** Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo	X	Incluir en el cronograma de capacitaciones, la inducción y reinducción sobre la seguridad de la información.
Proceso disciplinario	**Control:** Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender	X	Cumplir por parte de los funcionarios, las políticas y planes de seguridad y privacidad implementadas en la

	acciones contra empleados que hayan cometido una violación a la seguridad de la información.		institución y realizar las acciones pertinentes en caso de violación de las políticas de seguridad implantados.
Terminación o cambio de responsabilidades de empleo	**Control:** Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	X	Se debe socializar a los funcionarios las políticas y reglas referentes a la seguridad de la información y la vigencia de éstos aún después de la desvinculación. Se debe emitir paz y salvo de entrega de activo de información

Gestión de activos		**Control seleccionado**		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**
Inventario de activos	**Control:** Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	X		Crear documentación de todos los activos, estableciendo su ciclo de vida, los mecanismos de destrucción y correcta disposición de los mismos.

Propiedad de los activos	**Control:** Los activos mantenidos en el inventario deben tener un propietario.	X	Realizar la asignación de los activos a los funcionas encargados de cada uno de ellos, permitiendo crear y transferirlos.
Uso aceptable de los activos	**Control:** Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	X	Capacitación sobre la responsabilidad relacionada con el uso de los activos, especialmente para los contratistas por ser actores externos
Clasificación de la información	**Control:** La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada	X	Actualizar las tablas de retención documental parametrizando el almacenamiento de la información digital.
Etiquetado de la información	**Control:** Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X	Estandarizar el rotulado de la información digital.
Manejo de activos	**Control:** Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo	X	Los procedimientos para usar, manejar, almacenar, comunicar y destruir

	con el esquema de clasificación de información adoptado por la organización.			información se establecen en las tablas de retención de documentos.
Gestión de medios removibles	**Control:** Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización	X		Definir la gestión de medios extraíbles, implementando los parámetros para la eliminación temporal o permanente.
Disposición de los medios	**Control:** Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	X		Crear estrategias para el almacenamiento seguro de soportes físicos y establecer estándares para el manejo de documentos, especialmente aquellos clasificados como confidenciales.
Control de acceso		**Control seleccionado**		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**
Política de control de acceso	**Control:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	X		Presentar la política de control de acceso y realizar su respectivo seguimiento

Gestión de derechos de acceso privilegiado	**Control:** Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	X	Supervisar las tareas de acceso con privilegios.
Gestión de información de autenticación secreta de usuarios	**Control:** La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	X	Establecer un procedimiento para la autenticación secreta de usuarios
Uso de información de autenticación secreta	**Control:** Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	X	Definir parámetros de seguridad para la protección con contraseña
Restricción de acceso a la información	**Control:** El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	X	Controlar los permisos a los usuarios asignados
Procedimiento de ingreso seguro	**Control:** Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	X	Mantenga un registro de intentos de inicio de sesión exitosos y fallidos para rastrear posibles intentos de acceso no autorizado

Sistema de gestión de contraseñas	**Control:** Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	X		Establecer contraseñas seguras, realizar cambio frecuente de las mismas e impedir el reusó de las contraseñas.
Uso de programas utilitarios privilegiados	**Control:** Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	X		Fijar parámetros para el uso de programas utilitarios.
Control de acceso a códigos fuente de programas	**Control:** Se debe restringir el acceso a los códigos fuente de los programas	X		Establecer reglas para controlar y restringir el acceso al código fuente y almacenar copias del código de forma segura.
	Criptografía	**Control seleccionado**		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**
Políticas sobre el uso de controles criptográficos	**Control:** Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	X		Implementar la política de controles criptográficos que permita garantizar un uso adecuado y eficaz de la criptografía.
	Seguridad física y del entorno	**Control seleccionado**		

Objetivo	Descripción	Si	No	Justificación
Perímetro de seguridad física	**Control:** Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información	X		Definir las zonas seguras y límites de seguridad, verificando y ajustando regularmente las cerraduras de las puertas para diferentes dependencias, instalar sistemas de video vigilancia
Controles de acceso físicos	**Control:** Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	X		Solicitar carnet de identificación en físico y realizar seguimiento al libro de registro de acceso.
Seguridad de oficinas, recintos e instalaciones.	**Control:** Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	X		Documentar las normas de acceso a oficinas e instalaciones de la entidad
Protección contra amenazas externas y ambientales	**Control:** Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes	X		Socializar plan de contingencia ante desastres naturales
Trabajo en áreas seguras	**Control:** Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	X		Establecer protocolos para trabajo en áreas seguras

Ubicación y protección de equipos	**Control:** Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado	X	Realizar la ubicación correcta de los equipos, previniendo que los visitantes visualicen la información que se está manipulando.
Servicios de suministros	**Control:** Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro	X	Realizar inspección y evaluación periódica del funcionamiento de los servicios de suministro.
Seguridad en el cableado	**Control:** El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	X	Verificar periódicamente la red de energía y datos. Mantenimiento preventivo y correctivo de redes eléctricas y de datos
Mantenimientos de equipos	**Control:** Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas	X	Realizar seguimiento al cronograma de mantenimiento de equipos
Retiro de activos	**Control:** Los equipos, información o software no se deben retirar de su sitio sin autorización previa	X	Sustentar con actas los retiros de los activos, para verificar la devolución de los mismos

Política de escritorio limpio y pantalla limpia	**Control:** Se debe 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.	X		Establecer y supervisar políticas de escritorio y pantalla limpia.
Seguridad de operaciones		**Control seleccionado**		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**
Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	X		Actualizar los software antivirus y supervisar los informes de amenazas
Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas	X		Establecer las políticas para realizar las copias de seguridad y contar con un almacenamiento fuera de la entidad.

Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X	Implementar un mecanismo de registro de actividad del usuario
Instalación de software en sistemas operativos	**Control:** Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	X	Realizar seguimiento a la instalación de software y a sus licenciamientos.
Gestión de vulnerabilidades técnicas	**Control:** Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	X	Implementar mecanismo de registro de vulnerabilidades técnicas.
Restricción sobre la instalación de software	**Control:** Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	X	implementar las restricciones necesarias para la instalación de software no permitidos por la entidad

Seguridad de las comunicaciones		Control seleccionado		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**
Controles de redes	**Control:** Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	X		Diseñar plan de auditoria para analizar el funcionamiento de la red de datos, buscando así corregir anomalías en infraestructura, fluido eléctrico, ubicación, riesgo ambientales, etc
Acuerdos de confidencialidad o de no divulgación	**Control:** Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información	X		Implementación de protocolo de confidencialidad para el manejo de información.
Gestión de incidentes de seguridad de la información		**Control seleccionado**		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**
Responsabilidades y procedimientos	**Control:** Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida,	X		Asignar responsabilidades de seguridad de la información para planificar y definir planes de acción de respuesta a incidentes

	eficaz y ordenada a los incidentes de seguridad de la información			
Reporte de eventos de seguridad de la información	**Control:** Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	X		Implementar un mecanismo para reportar incidentes relacionados con la seguridad de la información de los funcionarios
Reporte de debilidades de seguridad de la información	**Control**: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios	X		Implementar procedimientos para el reporte de amenazas de seguridad TI, por parte de los funcionarios.
Aspectos de seguridad de la información de la gestión de continuidad de negocio		**Control seleccionado**		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**
Verificación, revisión y evaluación de la continuidad de la	**Control:** La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con	X		Implementación de procedimientos de verificación, evaluación y seguimiento de la seguridad de la información

seguridad de la información	el fin de asegurar que son válidos y eficaces durante situaciones adversas.			
Cumplimiento		**Control seleccionado**		
Objetivo	**Descripción**	**Si**	**No**	**Justificación**
Protección de registros	**Control:** Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	X		Implementar políticas de protección de registros
Privacidad y protección de información de datos personales	**Control:** Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	X		Diseño e implementación de la política de protección y tratamiento de datos personales
Revisión independiente de la seguridad de la información	**Control:** El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los	X		Realizar capacitación a los auditores externos para efectuar las revisiones

	objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.		
Cumplimiento con las políticas y normas de seguridad	**Control:** Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	X	Implementación de procedimientos de verificación, evaluación y seguimiento
Revisión del cumplimiento técnico	**Control:** Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	X	Implementar procedimientos de verificación, evaluación y seguimiento.

Fuente: NTC-ISO-IEC 27001:2013

6.4 PROPONER POLÍTICAS DE SEGURIDAD ALINEADAS AL PROCESO, BASADA EN LA EVALUACIÓN DE GESTIÓN DE RIESGO REALIZADA, CON EL FIN DE GESTIONAR Y BRINDAR SEGURIDAD AL ÁREA TIC DEL HOSPITAL SAN VICENTE DE PAÚL.

6.4.1 Política General De Seguridad Y Privacidad De La Información Del Hospital San Vicente De Paúl de Fresno[36]

6.4.1.1 Introducción

Hoy en día, el tema de la seguridad en las tecnologías de la información es cada vez más importante y a su vez, más exigente, esto es debido al repentino desarrollo que ha realizado el internet en el transcurso de los últimos años. La seguridad de información y el monitoreo de red de acceso de atacantes o intrusos son únicamente ejemplos de la finalidad que se debe obtener para garantizar el buen funcionamiento y conexión de la infraestructura informática y sus servicios de manera segura.

En cuanto a la posibilidad de extender la cobertura de servicios, de conectar bases de información y de aproximar a los usuarios que se encuentran separados por enormes distancias, ha excedido al hallazgo de aparentemente nuevas amenazas en los sistemas que ahora mismo se encuentran de manera virtual, puesto que, innovar en aspectos tecnológicos, a su vez, implica que aumentarán las vulnerabilidades.

Hasta el día de hoy, la mayor parte de las entidades gubernamentales y a su vez, las no gubernamentales, las nacionales e internacionales, implementan normas y estrategias que brindan mayor seguridad y por esta misma, dirigen el uso más conveniente de la tecnología; y por medio de esta misma, forman sugerencias para prevalecerse de sus ventajas y así mismo precaver su uso inapropiado, previniendo inconvenientes o errores graves en el uso o aplicación de los bienes y servicios tecnológicos de las diferentes entidades.

Por ello es que la adopción de estrategias de seguridad en la información, renace como una herramienta a nivel organizacional de alta utilidad necesaria para concientizar a cada funcionario sobre del valor, la importancia, la importancia de la información y la precisión de su cuidado con el menor límite de riesgos y un alto nivel de protección que acoja el crecimiento de una organización, de esta forma, que asegure su excelente

[36] HOSPITAL SAN VICENTE DE PAÚL E.S.E., Plan De Seguridad Y Privacidad De La Información Hsvp 2022. [EN LÍNEA]. 2022. [Citado en 18 de marzo de 2022]. Disponible en internet: <http://www.hospital-fresno-tolima.gov.co/planes/plan-de-seguridad-y-privacidad-de-la-informacion-hsvp>

funcionamiento y su optimo uso de los equipos y recuperación de datos o información rápidamente por si se presenta algún tipo de percance o diferentes tipos de catástrofes.

6.4.1.2 Objetivos

- Definir estrategias para el cuidado y buen uso de equipos, dispositivos informáticos y manejo de información.
- Crear una cultura de sensibilización en todos los usuarios del Hospital San Vicente de Paúl sobre la necesidad de impartir medidas y políticas de seguridad y privacidad en la institución.
- Reglamentar y controlar el uso y manipulación de software con el fin de evitar intrusiones y materialización de riesgos informáticos en los activos de información de la E.S.E.
- Documentar las políticas de seguridad y privacidad, creadas para el Hospital San Vicente de Paul y establecer los parámetros principales de integridad y confiabilidad del área informática de la institución.

6.4.1.3 Alcance

Esta política está diseñada para ser seguida estrictamente por todos los empleados, contratistas, proveedores y terceros de E.S.E. quienes de alguna manera utilizan los equipos o recursos del Hospital San Vicente de Paúl.

6.4.1.4 Responsabilidades de la Oficina de Sistemas de Información

- Gestionar de manera constante los procesos de Privacidad y Seguridad Informática del Hospital San Vicente de Paúl.
- Ser el pilar de todas las operaciones de seguridad y poder educar a los usuarios y al personal de la entidad sobre las buenas prácticas para proteger los recursos informáticos de la institución.
- Desarrollar procesos de mejora continua que fortalezcan las políticas de seguridad de la información institucional.
- Atender y responder inmediatamente los llamados en caso de un incidente de seguridad o de materialización de riesgos.
- Elaborar planes de contingencia, que permitan dar pronta y eficiente respuesta a los posibles incidentes que ocurran en la institución.

6.4.1.5 Clasificación de las Políticas de seguridad

Para efectos de comprensión de este documento, la oficina de sistemas del Hospital San Vicente de Paul E.S.E ha clasificado las políticas de seguridad en los siguientes grupos que corresponden a los actores principales que existen en un sistema de información.

- **Equipos:** Hardware o dispositivos y todo lo relacionado con su buen uso y cuidado.
- **Usuarios:** Personal que hace uso de servicios informáticos en la entidad.
- **Software:** Aplicaciones que se usan para la resolución de tareas; tales como: programas, suites de aplicativos, etc.
- **Redes e Internet:** Estrategias que se deben establecer para el buen uso de conexiones intra y extracurriculares en la red de la entidad.
- **Datos e Información:** Políticas que regulan la manipulación, transporte y almacenamiento de la información de la institución.
- **Administración de seguridad informática:** Imparte la manera en la que el área de sistemas y TICs gestiona la seguridad y privacidad de la infraestructura informática del Hospital San Vicente de Paul E.S.E.

6.4.1.6 Políticas de seguridad y privacidad de equipos.

Los equipos son una parte esencial del procesamiento y la administración de la información. Oficina de Sistemas de Información tiene como misión preservar el normal funcionamiento de la topología informática de una organización o desarrollar medidas preventivas y correctivas en caso de robo, incendio, catástrofe natural, avería eléctrica y cualquier otro elemento que amenace la infraestructura informática de la organización.

En este caso, se considerarán las siguientes políticas:

a. Todos los equipos de cómputo, periféricos o accesorios conectados a la red de cómputo del Hospital San Vicente de Paúl sean o no de propiedad de la institución, deberán cumplir con las normas y el procedimiento de instalación establecido por la Oficina de Sistemas de Información. Si no es el caso, no se permitirá la conexión de dispositivos que no sean propiedad de la institución, de lo contrario se debe diligenciar el formulario asumiendo la responsabilidad sobre el equipo ya que la institución no se hará cargo de ellos.

b. La Oficina de Sistemas de Información llevará un registro de todos los equipos propiedad del Hospital San Vicente de Paúl. Si es necesario trasladar computadoras, periféricos o accesorios, se requiere la aprobación de la oficina de

Sistemas de Información. Si necesita alquilar equipos (por horas o días), por favor notifique a la Oficina de Sistemas de Información y diligencie el formulario correspondiente.

c. Cualquier dispositivo, periférico o accesorio del Hospitales San Vicente de Paul E.S.E que necesite ser retirado de la institución deben obtener el permiso de la Oficina de Sistemas de Información.

d. Todo equipo de la institución debe estar en un área que cumpla con los siguientes requisitos: seguridad física, condiciones ambientales apropiadas, seguridad y estabilidad de los componentes eléctricos, se deben brindar garantías relacionadas con el área de mantenimiento de San Vicente Hospital de Paul E.S.E. En general, todos los equipos, periféricos y accesorios computacionales en la red del Hospital San Vicente de Paul E.S.E deben mantenerse alejados de dos factores principales: la luz solar directa y la humedad, los derrames y otros medios pueden exponer el dispositivo al agua.

e. Todo equipo o periférico que forme parte de la red del Hospital San Vicente de Paul deberá tener un sistema de protección eléctrica, ya sea un regulador de voltaje o UPS, para proteger el dispositivo de cambios bruscos en la fuente eléctrica de la institución o del área donde se ubica. Por lo anterior:

- Todo equipo de propiedad de la institución, no se puede poner en uso sin ninguna de estas medidas de protección. Si el funcionario conecta el dispositivo, será directamente responsable de los daños causados y se tomaran las medidas correspondientes.
- Si existe la necesidad de poner en marcha equipos sin UPS o estabilizador, esto se puede hacer de manera temporal y contando con la aprobación y acompañamiento de la Oficina de Sistemas de Información.

f. Los usuarios responsables de los dispositivos en cualquier dependencia deberán cumplir con los reglamentos y normas de instalación correspondientes al dispositivo y deben solicitar permiso para actualizar o instalar cualquier software, reubicación del dispositivo y todo lo que implique cambios respecto a su instalación. Los equipos de cómputo no podrán ser transferidos o trasladados sin la autorización previa de la Oficina de Sistemas de Información, la cual evaluará la factibilidad de dichos cambios.

g. El funcionario de la institución a quien se le asigno la custodia de los equipos se encargará de su cuidado, protección física, limpieza externa y mantenimiento de las estaciones de trabajo, en caso de daño o perdidas se debe notificar en el menor tiempo posible a la oficina de sistemas de información de la institución.

h. Está prohibido consumir o colocar alimentos cerca de dispositivos e impresoras, así como etiquetarlos. En caso de que se derrame comida sobre el dispositivo, periférico o accesorios, apáguelo, desconéctelo y notifique de inmediato a la Oficina de Sistemas de Información, quien será responsable de realizar el mantenimiento correspondiente e informar a quien corresponda para que se tomen las acciones correctivas necesarias.

i. Los dispositivos de almacenamiento extraíbles (como USB, CD o DVD) y las nuevas tecnologías no están permitidos en los equipos del Hospital San Vicente de Paúl, a menos que lo requieran casos de fuerza mayor y con previa notificación por escrito a la oficina de sistemas de información quien revisará y dará aprobación. Para garantizar lo anterior, la Oficina de Sistemas de Información deshabilitó el puerto USB (solo para uso de memoria) y la unidad de CD/DVD. Si algún usuario necesita levantar este bloqueo, deberá presentar una solicitud a la oficina de Sistemas de Información que, a su vez la enviará a la gerencia para su revisión y evaluación. Esta medida involucra a los funcionarios y contratistas que trabajan en la institución y utilizan de alguna manera los equipos del hospital.

j. Para solicitar servicio de mantenimiento a un equipo, periférico o accesorio, se debe diligenciar un formato anexo.

k. Los equipos de cómputo del hospital San Vicente de Paúl no deben ser alterados o mejorados por ningún motivo (cambio de procesador, cambio de memoria o adición de tarjeta); El incumplimiento de esta política dará lugar a sanciones de acuerdo con la normativa interna de la organización.

l. El mantenimiento o soporte a nivel de hardware no está disponible para equipos de cómputo que no sean del Hospital San Vicente de Paul.

m. Los funcionarios de la Oficina de Sistemas de Información del Hospital San Vicente de Paúl son los únicos funcionarios con permisos para administrar, mantener y velar por la integridad y seguridad del servidor principal de la organización, y custodian las contraseñas de estos.

n. El servidor central de la red del hospital San Vicente de Paul debe estar ubicado en un lugar separado, inaccesible para personas ajenas a la oficina de sistemas de información, dadas las condiciones de espacio, temperatura, iluminación, entre otras.

o. Los equipos de propiedad del hospital San Vicente de Paúl sólo podrán ser utilizados para el funcionamiento del mismo, por lo que el usuario no debe utilizarlos para fines personales, Delito contra los bienes de la administración pública.

p. La compra de nueva infraestructura tecnológica para el procesamiento de información (hardware, software, aplicaciones y configuraciones físicas) o la mejora de la infraestructura existente será aprobada por la Oficina de Sistemas de Información y el jefe de la dependencia que lo requiera.

q. Todo equipo asignado a un funcionario o contratista deberá ser entregado a la persona responsable en las mismas condiciones que al momento de la recepción del equipo, como parte de las actividades especificadas en la terminación del contrato o cambio de puesto.

r. Todos los equipos de cómputo que se adscriban al área asistencial y deban ser retirados del área para su mantenimiento, reparación, reubicación o sustitución, deberán ser previamente desinfectados en el sitio para evitar la posible contaminación que pueda ocurrir.

6.4.1.7 Política de uso de dispositivos móviles

La gestión tecnológica atribuye las políticas que se presentan a continuación con relación a los dispositivos móviles, incluyendo computadores personales y tabletas:

a) Todo tipo de dispositivo móvil debe poseer un código de inventario, el cual se encontrará registrado frente a sus datos en una base de datos de inventario único.
b) Como requisito, su información deberá estar codificada o con protección de contraseña, ya que, será importante, bien sea para su defensa y seguridad del mismo, en caso de presentarse algún tipo de extravío o hurto.
c) La red inalámbrica, mediante la cual se conectan estos dispositivos, deberá mantener en inspección y observación, relacionando su respectiva seguridad de desconexión frente a dichas redes.

d) Todo tipo de mecanismo móvil mantendrá una alta configuración para su dicho uso, sin pasar por alto la documentación basándose en su predominio de potestad del Hospital San Vicente de Paúl.

e) El hurto o perdida que se presente con algún tipo de dispositivo tendrá que ser comunicada a gerencia y área de almacén, no obstante, recordar que dicho reporte debe ser presentado en el menor tiempo posible.

f) Recuerde que el uso del celular en horario laboral debe ser mínimo, a no ser que sus funciones lo requieran.

g) No está permitido el uso del celular durante la prestación de un servicio y/o atención a un usuario.

6.4.1.8 Políticas de seguridad de los recursos humanos

a) Todo funcionario que requiera en sus actividades trabajar en el sistema de información institucional, deberá diligenciar el acuerdo de confidencialidad, proceso asignado al área de Recursos Humanos.

b) Todos los funcionarios e intermediarios deberán otorgar cumplimiento a todas las políticas de seguridad.

c) Se deben realizar capacitaciones y campañas de sensibilización respecto a temas enlazados a la seguridad informática y de la información.

d) Si se toma una acción de seguridad de la información, se sujeta al proceso que se le aplicará al infractor de acuerdo con las normas internas de la institución.

e) A la culminación de los contratos laborales se realizará un formato de paz y salvo, mediante el cual se establezca constancia de la entrega de documentos físicos y/o virtuales por los cuales se establecen acuerdos de confidencialidad sobre dicha información.

6.4.1.9 Política de gestión de activos

a) Los procesos de identificar y categorizar los activos de información de la institución, se realizará mediante un método formal con reglas para su dicha ejecución y se realizará proceso de actualización constante sobre dichos activos y el análisis de vulnerabilidades de seguridad de cada uno de ellos.

b) Los activos de información deben llevar consigo una placa o etiqueta de acuerdo a lo establecido en la ley 1712 de 2014.

6.4.1.10 Política de manejo de medios removibles

a) Deberá asegurar absolutamente todos los dispositivos y documentación importante como todo tipo de disco duro externo, Memorias USB para así mismo evitar cualquier tipo de acceso por personal no autorizado.

b) El uso de medios removibles por parte de funcionarios deberá permitirse llevando a cabo el proceso indicado para esto, realizando solicitud al área de almacén.

c) Los dispositivos extraíbles permitidos para uso dentro de la institución deberán mantener libre de virus o software dañino. Sin embargo, para eso se llevarán a cabo diferentes tipos de análisis con un antivirus en un periodo de tiempo determinado.

d) Si por cualquier motivo, se debe realizar traslado de medios extraíbles, se llevará a cabo el uso de los transportes más confiables para proteger la integridad, confidencialidad y privacidad de la información guardada en estos dispositivos o medios.

e) La información resguardada en dispositivos extraíbles deberá mantenerse protegida con contraseña para así mismo, poder ser traslada y trasportada de manera segura y confiable.

f) Tendrá que almacenarse de manera segura los medios fundaméntales cuando llegan a una determinada etapa de vida útil, continuando con un proceso de manera formal que indique como se deben desechar los medios de almacenamiento. Así mismo que se establezcan responsables para realizar dicho procedimiento en la guía.

g) Cualquier tipo de medio removible que haya salido de la entidad y es utilizado por el Hospital, debe ser analizado antes de volver a ingresar a uso cotidiano.

6.4.1.11 Política de control y administración de acceso

a) La oficina de gestión tecnológica debe inspeccionar el acceso de usuarios a los sistemas de información y limitar su acceso por módulos, pero solo al personal autorizado.

b) El ingreso de personal al sistema de información principal se concederá solo cuando se haya realizado de manera formal este acceso por medio de su contrato, con aprobación dada por el líder de proceso donde ingresará, cabe resaltar que no se hará ningún tipo de aceptación de solicitudes mediante otro medio

c) La oficina de sistemas de información realizará periódicamente auditoria a los usuarios y permisos asignados con el fin de salvaguardar la información de accesos sin autorizaciones.

d) La oficina de sistemas de información llevará a cabo la desactivación de las diferentes cuentas de acceso del personal al recibir la notificación del área de

talento humano, ya sea por fin de contrato o finalización de labores en la institución.

6.4.1.12 Política de gestión de contraseñas

a) Los funcionarios tienen un único usuario de ingreso al sistema de información institucional y él mismo es el responsable de todo lo sucedido con su usuario.

b) Las contraseñas de acceso a las distintas plataformas de uso institucional son personales y no transferibles. El usuario se encargará de identificar y dar lugar al buen uso estas mismas y vigilar que no sea obtenida por personal no autorizado.

c) Las plataformas tecnológicas de uso oficial tendrán de manera obligatoria la modificación de dichas contraseñas de acceso de manera periódica.

d) Al momento de asignar una contraseña a un usuario, se debe tener presente que deben tener longitud mínima de ocho caracteres y máxima de diez, debe ser obligatorio el uso de mayúsculas, minúsculas, números y símbolos. El sistema de información realizará automáticamente dicha validación.

e) No será permitido el uso de esta misma contraseña al momento de ser actualizada, tampoco se permite el cambio por una similar o igual a las ultimas 5 modificaciones.

f) El resguardo de contraseñas en las plataformas y sistemas de información estará cifrado de tal manera que no pueda ser consultado por terceros.

6.4.1.13 Política de seguridad para uso de servicio de internet

a) Todos los equipos de la institución contarán con acceso a internet y conexión a la red local.

b) EL ingreso a la red del Hospital se realizará exclusivamente por medio de equipos autorizados por la oficina de sistemas de información.

c) El ingreso a la red inalámbrica se realizará únicamente por medio de equipos y dispositivos aprobados y reglamentados por la oficina de sistemas, en el caso de los equipos invitados en aulas y eventos, el acceso se realizará a la red pública destinada para este tipo de solicitudes.

d) El funcionario deberá tener un aplicativo de navegación en su equipo que le facilitará el acceso al servicio de internet.

e) Es importante tener en cuenta que dicha navegación a sitios obscenos o cualquier sitio web que genere riesgo, se restringirán mediante el sistema filtrado del Router principal.

f) El acceso al servicio de internet está permitido para todas las plataformas oficiales y gubernamentales, enlazadas con el cumplimiento misional de la institución.

g) El acceso a servicios de internet brindado por la oficina de sistemas será vigilado y podrá ser cancelado si la amenaza detectada afecta la seguridad de la red y la infraestructura tecnológica.
h) El acceso al servicio de internet se realizará únicamente con propósitos laborales

6.4.1.14 Política sobre controles criptográficos

a) La oficina de sistemas de información asegura que en la base de datos del sistema de información se implementen algoritmos de codificación para el resguardo de la información.
b) Los algoritmos de encriptación usados serán resguardados de manera segura para evitar que se presente algún tipo de alteración o copia sin ninguna autorización.
c) Las contraseñas o claves de acceso se guardarán de manera codificada y encriptada en cada uno de los sistemas o plataformas de información usados en la institución y se asegurará que mantendrá la confidencialidad e integridad de estas mismas en su resguardo y entrega al funcionario.
d) El líder de la oficina de sistemas de información será el único funcionario autorizado de manipular las firmas digitales del representante legal y contador oficial, y debe velar por su seguridad y evitar uso no autorizado.

6.4.1.15 Política sobre seguridad física y del entorno

a) Los dispositivos y equipos que hacen parte de la infraestructura del datacenter principal del Hospital se encontrarán fuera del alcance de terceros en áreas restringidas, el ingreso a estos lugares será monitoreado y se le permite únicamente a personal que si este autorizado.
b) El registro de acceso a dichos lugares se realizará por medio de dispositivos de seguridad biométrica con el fin de llevar registro de acciones del personal.
c) El acceso al espacio por parte de terceros se llevará a cabo en compañía de un usuario de la oficina de sistemas, durante todo el tiempo que pueda llevarse a cabo la visita.
d) las áreas restringidas o privadas en donde se pueden localizar equipos de alta importancia tecnológica contarán siempre con sistemas de protección contra accidentes eléctricos, incluyendo el medio ambiental como la humedad y la alta o baja temperatura y de daños naturales como lo son los provocados por los incendios.

e) En caso de crear nuevas áreas restringidas de esta índole, se tendrán en cuenta los tipos de seguridad contra los riesgos evaluados con el fin de no materializar dichas amenazas.

6.4.1.16 Política de seguridad de equipos de computo

a) La oficina de sistemas de información se encargará de realizar anualmente análisis de la cantidad de equipos instalados con el fin de evaluar la necesidad de adquisición de suministros y equipos de sistemas.
b) Se realizarán dos jornadas de mantenimiento preventivo en cada uno de los equipos de la institución.
c) El traslado de dispositivos de cómputo entre áreas se llevará a cabo solo cuando haya diligenciado el formato en el área de almacén y oficina de sistemas con una firma que se llevará a cabo por el funcionario a cargo del inventario de activos.

6.4.1.17 Política de protección de software malicioso

a) La oficina de sistemas administrará la aplicación de antivirus con el fin de aumentar la seguridad en la red y así mismo detectar códigos maliciosos en equipos que ofrecen un determinado servicio en la institución, como celulares, dispositivos removibles o cualquier equipo que esté conectado a la red de datos de la entidad.
b) Se realizará análisis de códigos maliciosos en todos los dispositivos y servidores por un determinado periodo de tiempo que no afecte el buen funcionamiento del equipo.
c) Se concientizará al personal de las amenazas que se encuentran ligadas al daño que puede producir un malware.
d) El usuario deberá pasar un reporte de inmediato sobre cualquier sospecha o evento inseguro que evidencien en los dispositivos que están a su cargo.
e) No estará permitido la desactivación de software por parte de personal ajeno a la oficina de tecnologías.
f) Los sistemas operativos de los distintos dispositivos y servidores, se mantendrán actualizados en cuanto a la última versión que se encuentre disponible.

6.4.1.18 Política de seguridad en las comunicaciones

a) La oficina de sistemas monitoreará y analizará las conexiones de la red que se encuentran vinculadas, para así mismo garantizar su intervención.

b) La oficina de sistemas divide la red para así mismo poder clasificar la infraestructura tecnológica interna de los dispositivos de los usuarios externos, canales de conexión y otros servicios ofrecidos por intermediarios.

c) Se evidenciarán los procedimientos de seguridad y acuerdos de servicio para estos mismos que se otorgan, ya sean de manera interna o que tengan convenio con proveedores o terceros.

d) La transferencia de informes por medios físicos, se llevarán a cabo mediante lo pactado por el centro de información documental.

e) El cruce y envío de información que se presentan con otras entidades se llevara a cabo después de realizar análisis de seguridad entre ambas infraestructuras, para que la difusión sea realizada de manera muy segura, siempre en la base de un contrato.

f) La transferencia de informes digitales dentro del Hospital, la oficina de sistemas pondrá en práctica las herramientas que evidencien seguridad para la difusión de información.

g) El correo electrónico corporativo es utilizado solo con fin laboral, por ende, está prohibido los correos electrónicos personales para remitir o recibir informes en relación con a la institución.

6.4.1.19 Política de gestión de incidentes de seguridad de la información

a) Todos los funcionarios, contratistas y terceros de los sistemas informáticos deberán informar de manera oportuna todo tipo de vulnerabilidad o fragilidad de seguridad que haya sido detectada, siguiendo el procedimiento que se estableció para realizar el reporte correspondiente.

b) El encargado de mantener la seguridad de la información en la entidad, recibirá cualquier tipo de notificación de percances de seguridad y les realizará la gestión y seguimiento correspondiente.

c) Debido a cada percance de seguridad se llevará a cabo un registro y una valoración para así mismo poder determinar el nivel del impacto, debido al procedimiento de evaluación de percances de seguridad.

d) Es importante llevar registro de los inconvenientes o amanezcas detectadas respecto a los percances de seguridad de tal información, para que el procedimiento que se aplico sea útil para la solución de próximos percances de alta similitud.

e) El nivel de prioridad de cada servicio en cuanto a seguridad y estabilidad informática, deberán estar bajo monitoreo permanente y se define en el siguiente orden:

Asistenciales

1. Servicio de urgencias
2. Servicio de hospitalización
3. Servicio de Facturación
4. Servicio de Consulta Externa
5. Servicio de Auxiliares en oficina

Administrativos

1. Sistema de Información
2. Archivo Clínico
3. Financiera
4. Nomina
5. Archivo y correspondencia
6. Otros

F) Los jefes de oficina son los responsables en la implementación y garantía inicial del cumplimiento de políticas que hayan sido publicadas, modificadas o adicionadas recientemente. Cualquier violación a las políticas y normas de seguridad establecidas en este documento y aprobadas mediante acto administrativo será sancionada disciplinaria o penalmente. Para las infracciones más graves, se acatará lo estipulado en la ley 1273 de 2009 de delitos informáticos, y Ley 734 de 2002 Código Único Disciplinario.

7 CONCLUSIONES

Se realizó análisis del estado actual del área de las TICS del Hospital San Vicente de Paúl, utilizando el instrumento propuesto por el ministerio de las TICS, con el fin de conocer si se cuentan con controles de seguridad implementados. Al aplicar el instrumento se obtiene una calificación de 28/100, ubicando a la entidad en una fase repetible, demostrando así la existencia de pocos procesos de gestión de la seguridad y privacidad de la información abriendo brechas a las diferentes vulnerabilidades existentes en los sistemas de información.

Determinamos las vulnerabilidades, amenazas y riesgos de seguridad informáticos a los activos de información existentes en el área de TIC del Hospital San Vicente de Paúl, basándonos en una metodología de gestión de riesgos, con el fin de minimizar los riesgos. Por medio de la metodología MAGERIT, se logró identificar los activos de información y los posibles riesgos que puedan llegar a afectarlos, asignándole una dimensión de valoración que los conlleva a los respectivos niveles de riesgos, con el fin de demostrar las amenazas encontradas y que son significativas para la institución.

En este proyecto se desarrolló el documento de aplicabilidad basándonos en los resultados de análisis y evaluación del riesgo en el área de TIC, con el fin de determinar los controles requeridos para el endurecimiento de la seguridad. Implementando la aplicabilidad de la norma ISO 27001/2013 con el propósito de establecer los controles y las políticas a ejecutar para tener una información segura, disponible y confiable.

Se presentaron las políticas de seguridad alineadas al proceso, basados en la evaluación de gestión de riesgo realizada, con el fin de gestionar y brindar seguridad al área de TIC del Hospital San Vicente de Paúl. Por medio del cual se busca guiar a los funcionarios y contratistas de la institución sobre la importancia de resguardar la información manejada, realizando buenas prácticas de seguridad cumpliendo así los requisitos legales.

Después de realizadas las anteriores acciones y de dar cumplimiento a los objetivos del proyecto, se puede concluir que el desarrollo de un Sistema de Gestión de Seguridad de la Información en el Hospital San Vicente de Paúl de Fresno, permitirá implementar nuevas políticas y procedimientos que buscan, de manera controlada, incrementar el nivel de seguridad en el tratamiento de información y en todos los procedimientos que se involucre el uso de activos de información de la entidad, generando un gran impacto en todos los procesos, tanto asistenciales y administrativos, ya que procurará por mantener actualizada su infraestructura tecnológica, mejorará la rapidez de respuesta de sus

sistemas de información conectados a la red de datos haciendo así la consulta de pacientes más efectiva, se evitará la pérdida o daño de información gracias a la disminución en el desconocimiento o analfabetismo digital por parte de sus funcionarios y manejará planes de acción con el fin de evitar la materialización de vulnerabilidades y amenazas ante posibles ataques a los activos de información, generando tratamiento de los mismos e implementando estándares de seguridad y mejoras en sus procedimientos.

8 RECOMENDACIONES

Implementar las políticas de seguridad propuestas en el Sistema de Gestión de Seguridad de la Información y así permitir al Hospital San Vicente de Paúl incrementar la seguridad de sus activos de información e infraestructura tecnológica y de esta manera evitar la materialización de riesgos y amenazas latentes en los diversos procesos de la institución.

Definir clausulas en los contratos generados por el Hospital San Vicente de Paúl en donde se estipule la privacidad y seguridad que se debe tener con la información interna y clasificada de la institución, esto con el fin de generar una cultura de protección de la información entre los funcionarios contratistas, proveedores y terceros que tengan un vínculo con el hospital.

Realizar periódicamente evaluación y auditoria a los controles y políticas de seguridad establecidas con el fin de mejorar los procesos y fortalecer las estrategias ya definidas por el equipo de profesionales en seguridad del hospital.

Actualizar de manera continua las versiones y parches de seguridad de sistemas operativos y aplicativos usados en los equipos de cómputo del Hospital San Vicente de Paúl como método de prevención ante ataques y aprovechamiento de vulnerabilidades por parte de usuarios malintencionados.

Implementar un sistema de Cortafuegos o Firewall en el data center del Hospital San Vicente de Paúl con el objetivo de administrar la seguridad de la red a nivel lógico y definir un método seguro de control de acceso a internet y red de datos local.

Definir métodos de acceso remoto a equipos y servidores por medio de conexiones seguras, implementando estrategias como un canal VPN, uso de protocolo SSH y desactivación de puertos de conexión cuyo uso no es necesario.

Capacitar a todos los funcionarios del Hospital San Vicente de Paúl en temas importantes como el uso seguro de medios informáticos, seguridad y protección de la información y tratamiento de datos personales en las bases de datos de la entidad.

Diseñar y definir un plan de contingencia tecnológico con el fin de garantizar la continuidad de los servicios informáticos y evitar trastornos en los procesos misionales del Hospital San Vicente de Paúl. En Dicho plan, se contemplarán temas de generación

de copias de seguridad del sistema, remplazo de equipos que presenten fallas, métodos físicos de recolección de información, entre otros.

BIBLIOGRAFÍA

ACADEMY, ¿Qué Es Norma ISO 27001? [EN LÍNEA]. [Citado en 10 de noviembre de 2021]. Disponible en internet: https://advisera.com/27001academy/es/que-es-iso-27001/

Andres Felipe. Tips Para Implementar La Declaración De Aplicabilidad (incluye Modelo En Excel). [EN LINEA]. 2020. [Citado en 25 de febrero de 2022]. Disponible en internet: https://blog.kawak.net/mejorando_sistemas_de_gestion_iso/tips-para-implementar-la-declaracion-de-aplicabilidad-descarga-excel

AMBIT, Tipos De Vulnerabilidades Y Amenazas Informáticas. [EN LINEA]. 2020. [Citado en 10 de diciembre de 2021]. Disponible en internet: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

ALEMÁN NOVOA, Helena. y RODRIGUEZ BARRERA, Claudia. Metodologías Para El Análisis De Riesgos En Los SGSI. Boyacá.: Fundación Universitaria Juan De Castellanos. 2014. 7-10p.

AMBIT, Tipos De Vulnerabilidades Y Amenazas Informáticas. [EN LÍNEA]. 2020. [Citado en 9 de noviembre de 2021]. Disponible en internet: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 De 2009. (5, enero, 2009). Por El Cual Se Crea El Bien Jurídico Denominado La Protección De La Información Y De Los Datos. Bogotá, 2009.

COLOMBIA. FUNCIÓN PÚBLICA. Ley 1712 De 2014. (6, marzo, 2014). Or Medio Del Cual Se Crea La Ley De Transparencia Y Del Derecho De Acceso A La Información Pública Nacional. Bogotá, 2014.

COLOMBIA. SENADO DE LA REPUBLICA. Ley 1266 De 2008. (31, diciembre, 2008). Por La Cual Se Dictan Las Disposiciones Generales Del Hábeas Data. Bogotá, 2009.

CONGRESO DE COLOMBIA. Ley estatutaria 1581 del 17 de octubre de 2012. [online]. 17 de octubre de 2012. [citado abril 2020]. Disponible en internet: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

Controles de Seguridad y Privacidad de la Información. [En línea]. <https://www.mintic.gov.co/gestionti/615/articles- 5482_G8_Controles_Seguridad.pdf> [citado en 28 de septiembre de 2017]

DE LEÓN, Juan Carlos. Diseño De Un Sistema De Gestión De Seguridad De La Información (SGSI) Basado En La Norma ISO/IEC 27001 Para Entidades Del Estado. Trabajo De Grado Especialista En Seguridad Informática. La Guajira.: Universidad Nacional Abierta Y A Distancia - UNAD. 2019. 118p.

DIAZ, Luis Carlos. Diseño De Un Sistema De Gestión De La Seguridad De La Información En La Ips Assalud De Corozal Sucre, Mediante La Implementación De La Metodología Magerit Y La Norma Iso 27001:2013. Trabajo De Grado Especialista En Seguridad Informática. Sucre.: Universidad Nacional Abierta Y A Distancia - UNAD. 2017. 205p.

ENRIQUEZ EDGAR RODRIGO, NICOLAR SOLARTE FRANCISCO: metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Santiago de Cali. 2016

FIRMA-E, ¿Qué Es Un SGSI – Sistema De Gestión De Seguridad De La Información? [EN LÍNEA]. 2013. [Citado en 10 de noviembre de 2021]. Disponible en internet: https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA, Gestión De Riesgo En La Seguridad Informática. [EN LÍNEA]. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/>

GOBIERNO DE COLOMBIA. FUNCIÓN PÚBLICA Sistemas de Información: Modelo Integrado de Planeación y Gestión MIPG. Santa Fe de Bogotá. 2017

GOBIERNO DE ESPAÑA, ISO/IEC 27001. [EN LINEA]. [Citado en 10 de diciembre de 2021]. Disponible en internet: <http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/isoirc_27001_pdca.html>

GOBIERNO DIGITAL, ¿Qué es el MSPI?. [EN LINEA]. [Citado en 28 de agosto de 2022]. Disponible en internet: <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>

HOSTDIMEBLOG, ¿Qué Es Una Amenaza Informática? ¿cómo Contenerla? [EN LÍNEA]. 2020. [Citado en 9 de noviembre de 2021]. Disponible en internet: https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/

HOSPITAL SAN VICENTE DE PAÚL E.S.E., Plan De Seguridad Y Privacidad De La Información Hsvp 2022. [EN LÍNEA]. 2022. [Citado en 18 de Marzo de 2022]. Disponible en internet: <http://www.hospital-fresno-tolima.gov.co/planes/plan-de-seguridad-y-privacidad-de-la-informacion-hsvp>

IBERO TIJUANA, ¿Qué es La investigación aplicada y cuáles son sus principales características? [EN LINEA]. 2020. [Citado en 07 de noviembre de 2021]. Disponible en internet: <https://blogposgrados.tijuana.ibero.mx/investigacion-aplicada/>

ICONTEC, Certificación ISO 27001, Sistemas De Gestión De Seguridad De La Información. [EN LÍNEA]. 2018. [Citado en 16 de octubre de 2021]. Disponible en internet: <https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/>

ISOTOOLS, ¿Cuáles Son Las Metodologías Para La Gestión De Riesgo? [EN LÍNEA]. 2017. [Citado en 10 de noviembre de 2021]. Disponible en internet: https://www.isotools.com.mx/cuales-las-metodologias-la-gestion-riesgo/
ISOTOOLS, Software ISO Riesgos Y Seguridad. [EN LÍNEA]. [Citado en 10 de noviembre de 2021]. Disponible en internet: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISOTOLLS, ¿qué Es La ISO 27001? [EN LINEA]. [Citado en 10 de diciembre de 2021]. Disponible en internet: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

INCIBE, Amenaza Vs Vulnerabilidad, ¿sabes En Qué Se Diferencian? [EN LINEA]. 2017. [Citado en 10 de diciembre de 2021]. Disponible en internet: <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT: versión 3.0Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas. Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica, Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones. Madrid, octubre de 2012

MINTIC, Ciberseguridad. [En línea]. <https://www.mintic.gov.co/portal/604/w3- article-6120.html> [citado en 03 de octubre de 2021]

MINTIC, Instructivo Para El Diligenciamiento De La Herramienta De Diagnostico De Seguridad Y Privacidad De La Información. [EN LINEA]. 2017. [Citado en 28 de agosto de 2022]. Disponible en internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf>

MIRANDA CAIRO MICHEL, VALDÉS PUGA OSMANY: Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. Santiago de Cali, 2017.

Modelo de Seguridad y Privacidad de la Información. [En línea]. <https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf> [citado en 28 de septiembre de 2021]

NOVASEC, ¿Qué Es La Gestión De Activos De Información? [EN LÍNEA]. [Citado en 9 de noviembre de 2021]. Disponible en internet: <https://www.novasec.co/blog/67-gestion-de-activos-de-informacion>

PAEPORTALADMINISTRACIONELECTRONICA, Magerit V.3: Metodología De Análisis Y Gestión De Riesgos De Los Sistemas De Información. [EN LÍNEA]. [Citado en 11 de noviembre de 2021]. Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

PENSEMOS, Claudia Victoria Alvarado. Sistema De Gestión De Seguridad De La Información: Qué Es Y Sus Etapas. [EN LÍNEA]. 2021. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas>

PORTAFOLIO, ¿qué Tipos De Ciberataques Realizó Anonymous En Colombia? [EN LÍNEA]. Economía. 2021. [Citado en 4 de octubre de 2021]. Disponible en internet: <https://www.portafolio.co/economia/que-tipos-de-ciberataques-realizo-anonymous-en-colombia-551839>

PULIDO BARRETO, A. (16 de 04 de 2016). Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático. Obtenido de Recuperado de http://hdl.handle.net/10596/6327

RAMIREZ, Carlos. ¡pilas! El 90 % De Incidentes Informáticos Ocurren Al Hacer Clic En Mensajes Sospechosos. [EN LÍNEA]. 2021. [Citado en 4 de octubre de 2021]. Disponible en internet: https://www.semana.com/finanzas/guias-basicas/articulo/pilas-el-90-de-incidentes-informaticos-ocurren-al-hacer-clic-en-mensajes-sospechosos/202113/

SECURITYARTWORK, Antonio Huerta. Introducción Al Análisis De Riesgos – Metodologías (i). [EN LÍNEA]. 2012. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/>

SECURITYARTWORK, Antonio Huerta. Introducción Al Análisis De Riesgos – Metodologías (ii). [EN LÍNEA]. 2012. [Citado en 11 de noviembre de 2021]. Disponible en internet: <https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/>

SEGURIDAD7A, CORAS Methodology (construct A Platform For Risk Analysis Of Security Critical System). [Citado en 11 de noviembre de 2021]. Disponible en internet: <http://seguridades7a.blogspot.com/p/coras.html>

SEMLER, Ricardo. Soberanía De Nuestros Datos. [EN LÍNEA]. 2021. [Citado en 4 de octubre de 2021]. Disponible en internet: https://elartedemedir.com/blog/soberania-de-nuestros-datos/

SGSI, ¿Cómo Realizar Un Inventario De Activos De Información? [EN LÍNEA]. 2017. [Citado en 9 de noviembre de 2021]. Disponible en internet: https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

SGSI, Metodología Octave Para El Análisis De Riesgos En SGSI. [EN LINEA]. 2021. [Citado en 11 de noviembre de 2021]. Disponible en internet: <https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-analisis-de-riesgos-en-sgsi/>

SGSI, ISO 27001. Aspectos Claves Y Relación Con Las Normas ISO 22301 E ISO/IEC 20000. [EN LINEA]. 2019. [Citado en 10 de diciembre de 2021]. Disponible en internet: https://www.pmg-ssi.com/2019/08/iso-27001-aspectos-claves-y-relacion-con-las-normas-iso-22301-e-iso-iec-20000/

SGSI, ISO 27001: El Método Magerit. [EN LINEA]. 2015. [Citado en 10 de diciembre de 2021]. Disponible en internet: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

UNIR, ¿Qué Es La Seguridad Informática Y Cuáles Son Sus Tipos? [EN LÍNEA]. 2021. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/>

VIU, Vulnerabilidad Informática, Tipos Y Debilidades Principales. [EN LÍNEA]. [Citado en 10 de noviembre de 2021]. Disponible en internet: https://www.universidadviu.com/es/actualidad/nuestros-expertos/vulnerabilidad-informatica-tipos-y-debilidades-principales

WEBINARS KAWAK, Estándares Seguridad De La Información ISO 27001. [EN LÍNEA]. 2020. [Citado en 10 de noviembre de 2021]. Disponible en internet: https://www.kawak.net/project/webinar-estandares-iso-27001-seguridad-de-la-informacion-mantenga-la-confidencialidad/

ANEXOS

Anexo A Autorización ejecución proyecto aplicado.

V0.1

Freno Tolima, 18 de octubre de 2021

Doctora:
DIANA MARÍA TABARES CLAVIJO
Gerente

Asunto: Autorización para la ejecución del proyecto titulado: DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DEL HOSPITAL SAN VICENTE DE PAÚL DE FRESNO.

Cordial saludo estimada Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado al Hospital San Vicente de Paúl, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DEL HOSPITAL SAN VICENTE DE PAÚL DE FRESNO. El cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente: Diseñar un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001/2013 que permita gestionar la integridad, confidencialidad y disponibilidad de la información del área de Tecnologías de la información y las comunicaciones (TIC) en el Hospital San Vicente de Paúl de Fresno; al mismo tiempo será apoyado por los objetivos específicos:

- Analizar el estado actual del área de las TICS del hospital San Vicente de Paúl mediante un instrumento propuesto por el ministerio de las TIC, con el fin de conocer si cuentan con controles de seguridad implementados.
- Determinar la vulnerabilidades, amenazas y riesgos de seguridad informáticos a los activos de información existentes en el área de TIC del Hospital San Vicente de Paúl, basados en una metodología de gestión de riegos, con el fin de minimizar los riesgos.
- Establecer el documento de aplicabilidad basado en los resultados del análisis y evaluación del riesgo en el área de TIC, con el fin de determinar los controles requeridos para el endurecimiento de la seguridad.
- Proponer políticas de seguridad alineadas al proceso, basada en la evaluación de gestión de riesgo realizada, con el fin de gestionar y brindar seguridad al área TIC del Hospital San Vicente de Paúl.

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por el *Hospital San Vicente de Paúl.*
- La empresa *Hospital San Vicente de paúl* deberá establecer qué tipo de información es privada y cuál es pública para delimitar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de pruebas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El documento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de nuestra carrera profesional.

Firman en Fresno, a los (18) días del mes de (octubre) de 2021

Cordialmente,

ROGER MARINO ORTIZ MERCHAN
Estudiante UNAD.

German Alexis Prada

GERMAN ALEXIS PRADA OSPINA
Estudiante UNAD.

Diana Ma Tabares C

DIANA MARÍA TABARES
Gerente

Anexo B Acuerdo de confidencialidad.

V 0.1

ACUERDO DE CONFIDENCIALIDAD ENTRE ROGER MARINO ORTIZ, GERMAN ALEXIS PRADA OSPINA Y EL HOSPITAL SAN VICENTE DE PAÚL DEL MUNICIPIO DE FRESNO TOLIMA

Por la **parte reveladora**
Nombre: Hospital San Vicente de Paúl
Dirección: Carrera 9 N° 2-42
Teléfono: 31189
E-mail: hospitalfresnotolima@gmail.com

Por la parte **receptora de la información**
Nombre: Roger Marino Ortiz Merchán
Dirección: Calle 8
Teléfono: 3122
E-mail: rmortizme@unadvirtual.edu.co

Por la parte **receptora de la información**
Nombre: German Alexis Prada Ospina
Dirección: Calle 5
Teléfono: 3104
E-mail: gapradaos@unadvirtual.edu.co

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece al Hospital San Vicente de Paúl del municipio de Fresno Tolima, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto

aplicado con el título: DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DEL HOSPITAL SAN VICENTE DE PAÚL DE FRESNO.

2. Que la información de propiedad del Hospital San Vicente de Paúl del municipio de Fresno Tolima ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera

   único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DEL HOSPITAL SAN VICENTE DE PAÚL DE FRESNO, Roger Marino Ortiz Merchán y German Alexis Prada Ospina que para el presente caso actual como **reveladores, guardas y administrados** de la información de propiedad de Nombre de la empresa.

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente al Hospital San Vicente de Paúl del municipio de Fresno Tolima**,** así como también a no utilizar dicha

información en beneficio propio ni de terceros, sólo con fines estadísticos y de mejoramiento del Hospital San Vicente de Paúl del municipio de Fresno Tolima.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DEL HOSPITAL SAN VICENTE DE PAÚL DE FRESNO, lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes,

películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma Hospital San Vicente de Paúl del municipio de Fresno Tolima, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte del Hospital San Vicente de Paúl del municipio de Fresno Tolima.

9. La **parte receptora** se compromete a establecer que los datos a utilizar serán usados de manera en que ninguna forma se pudiera causar perjuicio directo o indirecto a los titulares o terceros de la información suministrada por el Hospital San Vicente de Paúl conforme a las disposiciones de Protección de Datos Personales establecidas por la ley 1581 de 2012.

10. La información capturada por la **parte receptora** se observará como *datos de información* no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad toda la persona Hospital san Vicente de Paúl del municipio de Fresno Tolima no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de Hospital san Vicente de Paúl del municipio de Fresno Tolima, ni violentará la ley de delitos informáticos colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. Los estudiantes Roger Marino Ortiz Merchán y German Alexis Prada Ospina se comprometen a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa Hospital san Vicente de Paúl del municipio de Fresno Tolima para

salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el repositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la empresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de su alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes *(Roger Marino Ortiz Merchán, German Alexis Prada Ospina* y el Hospital san Vicente de Paúl del municipio de Fresno Tolima*)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las clausulas del presente acuerdo de confidencialidad por parte de *Roger Marino Ortiz Merchán y German Alexis Prada Ospina.*

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los (18) días del mes de (octubre) de 2021

Como Parte Receptora:

Roger Marino Ortiz Merchán
Estudiante UNAD.

Por la parte reveladora:

Diana María Tabares Clavijo
Hospital San Vicente de Paúl

German Alexis Prada

German Alexis Prada Ospina
Estudiante UNAD.

Anexo C Resumen Analítico Especializado RAE

Fecha de Realización:	15/09/2022
Programa:	Especialización en Seguridad informática
Línea de Investigación:	Proyecto de Desarrollo tecnológico
Título:	Diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de tecnologías de la información y la comunicación del Hospital san Vicente de paúl de fresno.
Autor(es):	Ortiz Merchán Roger Marino y Prada Ospina German Alexis
Palabras Claves:	Control, Información, Riesgos, Seguridad, Vulnerabilidad.
Descripción:	Con el desarrollo de este proyecto aplicado, se busca diseñar nuevas políticas de seguridad y privacidad de la información en el Hospital San Vicente de Paúl de Fresno Tolima, para fortalecer todos los procesos que manejen información dentro de la institución, apoyándonos en la mitología MAGERIT para realizar el análisis de riesgo y en el instrumento MSPI para diagnosticar la madurez del modelo de seguridad y privacidad de la información.

Fuentes bibliográficas destacadas:

GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA, Gestión De Riesgo En La Seguridad Informática. [EN LÍNEA]. [Citado en 10 de noviembre de 2021]. Disponible en internet: <https://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/>

ICONTEC, Certificación ISO 27001, Sistemas De Gestión De Seguridad De La Información. [EN LÍNEA]. 2018. [Citado en 16 de octubre de 2021]. Disponible en internet: <https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/>

MINTIC, Instructivo Para El Diligenciamiento De La Herramienta De Diagnostico De Seguridad Y Privacidad De La Información. [EN LINEA]. 2017. [Citado en 28 de agosto de 2022]. Disponible en internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf>

Modelo de Seguridad y Privacidad de la Información. [En línea]. <https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf> [citado en 28 de septiembre de 2021] SGSI, ISO 27001: El Método Magerit. [EN LINEA]. 2015. [Citado en 10 de diciembre de 2021]. Disponible en internet: <https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/>	
Contenido del documento:	Introducción Definición del problema Justificación Objetivos Marco Referencial Diseño Metodológico Desarrollo de los Objetivos Conclusiones Recomendaciones
Marco Metodológico:	El proyecto aplicado se desarrolló de acuerdo con los lineamientos del ministerio de tecnologías de información y las comunicaciones – MINTIC, relacionados con el diseño de un SGSI.
Conceptos adquiridos:	Articulación de un modelo de seguridad a los fines de la seguridad informática en una organización con el fin de mantener la integridad, disponibilidad y privacidad de la información. Implementación del instrumento MSPI para una organización. Gestión del riesgo y diseño de controles con base en la ISO/IEC 27001:2013
Conclusiones:	Es importante la socialización de la fase de planificación del SGSI ante los directivos del Hospital San Vicente de Paúl de Fresno Tolima, con el fin de establecer estrategias a corto, mediano y largo plazo, que propendan por la implementación del SGSI. El Hospital San Vicente de Paúl de Fresno, necesita implementar nuevas políticas y procedimientos que busquen, de manera controlada, incrementar el nivel de seguridad en el tratamiento de información y en todos los procedimientos en los que se involucre el uso

	de activos de información de la entidad, generando un gran impacto en todos los procesos, tanto asistenciales y administrativos