

UNIVERSIDAD CATÓLICA DE CUENCA



Maestría en Ciberseguridad

**Informe de Investigación previo a la obtención del título de Magíster en
Ciberseguridad**

Tema: Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI)
para Hospitales Tipo B del Ecuador: Caso Hospital Santa Teresita

Autor: Ing. Alex Enrique Blacio Roca

Asesores: Ing. Daniel Jacobo Andrade Pesántez. Mgs

Ing. Juan Carlos Ortega Castro. Mgs

Cuenca, 2024

Certificación de Asesores

Se certifica que:

El informe de investigación “Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para Hospitales tipo B del Ecuador: Caso Hospital Santa Teresita”, de autoría del Señora Ingeniero de Sistemas Alex Enrique Blacio Roca, CC: 07037799411, ecuatoriana, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Cuatro Ríos de Cuenca

Julio, 2024.

Ing. Daniel Jacobo Andrade Pesántez. Mg
Asesor Científico

Ing. Juan Carlos Ortega Castro. Mg
Asesor Metodológico

Certificación de Autoría

Certifico que:

“Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para Hospitales tipo B del Ecuador: Caso Hospital Santa Teresita”, es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Cuatro Ríos de Cuenca

Julio, 2024.

Ing. Alex Enrique Blacio Roca

CC: 07037799411

Agradecimiento

Agradezco Dios, por haberme dado la firmeza necesaria para terminar satisfactoriamente mi tema de Tesis, como también a mis padres que han sido un factor fundamental en todo este tiempo dándome su apoyo constante.

De igual manera agradezco a mi madre Mirian Roca, a mi esposa Juana Reyes y mis hijas por ser parte de este logro conseguido, ya que sus palabras de aliento me han incentivado para lograr que mi tema sea terminado con total éxito.

Así mismo agradezco a los docentes de la carrera de Ciberseguridad ya que han sido pilar fundamental para mi aprendizaje en mi carrera y en la obtención de este título.

De manera especial, expreso mis más sinceros agradecimientos al Ing. Daniel Jacobo Andrade Pesántez. Mg, por ser mi guía en mi trabajo de investigación, ya que con su ayuda desinteresada y sus consejos, exitosamente he terminado mi tema logrando cumplir con mi meta para mi vida profesional.

Y por supuesto, no puedo dejar de mencionar a mi familia, ya que han sido participes claves en el logro de mi meta.

Alex Blacio

Dedicatoria

Dedico este proyecto de investigación a Dios, porque gracias a su sabiduría y bendición he logrado felizmente terminar mi presente tema, logrando cumplir con mi meta.

Así mismo se lo dedico principalmente a mis padres, y mi familia ya que sin su apoyo diario jamás hubiera podido cumplir con mi proyecto de investigación, ellos han sido un soporte primordial en mi vida y en el presente tema.

Y por supuesto dedico este trabajo a mis hijas y esposa, sus palabras constantes de aliento, ánimos y superación han sido de gran importancia en el desarrollo de este tema, siendo parte fundamental en mi proyecto de investigación.

Alex Blacio

Resumen

El trabajo de investigación, se lo realizó mediante un estudio en los equipos tecnológicos que administran la red en el departamento de Tecnologías de la Información y la Comunicación (TIC) en el hospital tipo B del Cantón Santa Rosa de la Provincia de El Oro como es el Hospital Santa Teresita de donde se diseñó las políticas de seguridad bajo el modelo de un Sistema de Gestión de Seguridad de la Información (SGSI), las mismas que permitió evaluar la integridad, confidencialidad y disponibilidad de la información y de los activos del departamento TIC para fortalecer la infraestructura tecnológica y enfrentar los continuos cambios tecnológicos que implica el manejo de información sensible, ya que estos pueden ser propensos a ser víctimas de robo, secuestro de información y ataques de servicios, esto debido a la mala implementación en la seguridad de sus equipos. Además la ausencia de un SGSI que les permita establecer parámetros de seguridad para regular y proteger la información, el plantear el diseño de un SGSI para el departamento de TIC mitigará los riesgos a los que se expone esta institución.

La finalidad de diseñar las políticas de seguridad bajo el modelo SGSI con la normativa ISO 27001:2013 y la metodología MAGERIT propuesta se logró garantizar una alta calidad de implementación de políticas en el uso de los equipos, en mantener contraseñas robustas, en capacitación y concienciación sobre seguridad y el manejo de activos. Sin embargo, es importante tener en cuenta que, a pesar de estos esfuerzos, no se puede asegurar una seguridad absoluta. Siempre existe el riesgo de que los controles de seguridad de tecnologías de la información y la disponibilidad de la información no se cumplan en su totalidad.

Palabras claves: SGSI, Políticas, MAGERIT, ISO 27001:2013.

Abstract

The research work was carried out through a study of the technological equipment that manages the network in the Department of Information and Communication Technologies (ICT) in the type B hospital of the Santa Rosa Canton of the Province of El Oro, such as the Santa Teresita Hospital, where an Information Security Management System (ISMS) was designed. It made it possible to evaluate the integrity, confidentiality and availability of the information and assets of the information and communication technology (ICT) department due to the fact that they did not have an adequate technological infrastructure to face the continuous technological changes involved in the management of sensitive information, since these can be prone to be victims of theft, hijacking of information and attacks of services, this due to the poor implementation in the security of their computers. In addition to the fact that they did not have an Information Security Management System (ISMS) that would allow them to establish security parameters to regulate and protect information, proposing the design of an ISMS for the ICT department will mitigate the risks to which this institution is exposed.

The purpose of designing the security policies under the ISMS model with the ISO 27001:2013 standard and the proposed MAGERIT methodology was to guarantee a high quality of policy implementation. However, it is important to note that despite these efforts, absolute security cannot be assured. There is always a risk that Information Technology (IT) Security controls and information availability will not be fully complied with.

Keywords: SGSI, MAGERIT, ISO 27001:2013.

Índice de contenidos

Capítulo I. Introducción.....	1
1.1 Situación problemática	1
1.2 Problema científico.	3
1.3 Objeto de estudio.	3
1.4 Campo de acción.....	4
1.5 Objetivos.	5
1.6 Justificación	5
1.7 Fundamentación teórica	7
Capítulo II. Diagnóstico situacional.....	13
2.1 Metodología.....	13
2.2 Análisis situacional	15
2.3 Análisis comparativo.....	16
2.4 Herramientas	17
2.5 Operacionalización de Variables.....	17
Capítulo III. Propuesta	19
3.1 Organización	19
3.1.1 Reseña Histórica de la Institución.	19
3.1.2 Misión	20
3.1.3 Visión	21

3.1.4 Organigrama	22
3.1.5 Matriz de análisis FODA.	23
3.2 Análisis del problema.....	24
3.3 Impacto del problema en el Hospital.....	25
3.4 Causas del problema.....	25
3.5 Solución al problema	26
3.6 Resultados esperados.....	27
3.7 Análisis actual de la seguridad y privacidad del Hospital Santa Teresita.....	28
3.8 Diseño del SGSI.	32
3.9 Identificación de activos.....	33
3.10 Evaluación de activos.....	33
3.11 Valoración de los activos.....	36
3.12 Medidas de protección de activos de información.....	41
3.13 Políticas de seguridad de la información.....	108
3.14 Política de seguridad de la información para los empleados.	109
3.15 Política de seguridad de la información a empleados con funciones y responsabilidades técnicas.....	112
3.16 Control de acceso.	113
3.17 Uso de cifrado.....	119
3.18 Seguridad de las Operaciones.....	120
3.19 Seguridad de la red.	123

3.20 Seguridad de eliminación y reutilización de activos.....	124
3.21 Incidentes de seguridad.	124
3.22 Capacitación de concientización sobre seguridad.....	125
3.23 Cumplimiento.....	126
3.24 Documentación mínima para establecer un SGSI.	127
3.25 Diseño del sistema de gestión de seguridad de la información para el Hospital Santa Teresita	129
Conclusiones	133
Recomendaciones	134
Bibliografía	135
Anexos.....	139
Anexo 1	139
Anexo 2	139
Anexo 3	140
Anexo 4	143
Anexo 5	139

Índice de figuras

Figura 1. Organigrama Institucional de Hospital Santa Teresita.....	22
--	-----------

Índice de tablas

Tabla 1. Conceptualización de variables.....	18
Tabla 2. Análisis FODA aplicada en el departamento de TIC en marco a la seguridad informática.	23
Tabla 3. Análisis de la Seguridad y privacidad del Hospital Santa Teresita.....	29
Tabla 4. Identificación de Riesgos	33
Tabla 5. Categoría activos de información MAGERIT	34
Tabla 6. Activo de información por tipo Activo	35
Tabla 7. Criterios de valoración de activos.....	38
Tabla 8. Valoración de riesgo	39
Tabla 9. Valoración de activos	39
Tabla 10. Medidas de protección de los activos de información de tipo Activo.....	44
Tabla 11. Medidas de protección de los activos de información de tipo Datos.	55
Tabla 12. Medidas de protección de los activos de información de tipo Servicios.....	57
Tabla 13. Medidas de protección de los activos de información de tipo Hardware.	64
Tabla 14. Medidas de protección de los activos de información de tipo Comunicaciones.....	88
Tabla 15. Medidas de protección de los activos de información de tipo Auxiliar.....	92
Tabla 16. Medidas de protección de los activos de información de tipo Instalaciones.	99
Tabla 17. Medidas de protección de los activos de información de tipo personal.	104
Tabla 18. Resumen de medidas de protección a aplicar a las amenazas identificadas.	107

Capítulo I. Introducción

1.1 Situación problemática

El Hospital Santa Teresita actualmente es el único Hospital con varias especialidades del Cantón Santa Rosa el cual atiende emergencias las 24 horas y brinda servicios de hospitalización. Por tal motivo la información ingresa constantemente en los equipos informáticos y a los servidores del departamento de tecnología por esta razón la protección de los datos de los pacientes es fundamental para las organizaciones de salud. El sector salud se ha convertido cada vez más en un objetivo frecuente de ciberataques, en particular el ataque de código malicioso conocido como ransomware, que altera la funcionalidad de los equipos o sistemas infectados al cifrar archivos, bloquear el acceso, interrumpir operaciones, causar pérdida de datos, afectar el desempeño del sistema y generar costos de recuperación y estrés en el entorno de trabajo.(Plaza, 2021)

Los hospitales, debido a la sensibilidad de la información que manejan, son vulnerables al robo y secuestro de datos. Es importante garantizar la integridad, confidencialidad y disponibilidad de los datos para evitar ser víctimas de extorsión. Como en el caso del hospital Tallahassee Memorial HealthCare que en febrero de 2023 tras un ataque de ransomware obligó al hospital a cancelar cirugías y a trasladar pacientes a otros hospitales en Florida debido a que estuvo fuera de línea por casi una semana. (James, 2023)

Otro caso es el ataque cibernético al Hospital Ciudad Neily, Caja Costarricense Seguro Social el 31 de mayo de 2022 donde un ransomware afectó a servidores y terminales finales que carecían del software Microclaudia o tenían versiones desactualizadas, así como aquellos que se encontraban encendidos en el momento del ataque, los perpetradores fueron un grupo llamado Hive Ransomware Group. (Ulloa, 2023)

Garantizar la protección de la información se ha convertido en una prioridad para las entidades de salud, quienes están implementando SGSI. El diseño de estos sistemas permite a los hospitales fortalecer sus capacidades tecnológicas y garantizar la confidencialidad de las historias clínicas, especialmente en proyectos de interoperabilidad de datos y telemedicina, donde la información puede ser expuesta a canales informáticos externos.

Los dispositivos tecnológicos desplegados en el Hospital Santa Teresita responsables de la gestión de la red comprenden un Router Mikrotik rb750gr3, 4 dispositivos Switch, 3 Access Points, 2 Routers y 3 servidores (servidor local de un sistema interno para inventario, servidor de correo institucional y servidor de archivos).

El servidor de correo constantemente recibe ataques de phishing, spam, ataques de fuerza bruta y ransomware a través del correo, debido a estas incidencias el servidor ha tenido que suspender su servicio por varios días hasta poder corregir estos problemas.

El servidor de archivos constantemente recibe ataques de acceso no autorizado y ataques de denegación de servicio (DoS/DDoS) debido a esto se ha tenido que suspender el servicio hasta levantar medidas de seguridad que mitiguen este tipo de problemas.

El enrutador Mikrotik rb750gr3 es responsable de la administración de la red dentro del hospital, sin embargo, las medidas de seguridad implementadas son inadecuadas como lo demuestra la presencia de puertos abiertos y acceso a sitios web dañinos, entre otras vulnerabilidades. Lo anteriormente mencionado se identificó mediante la utilización de las herramientas como Nmap, Zenmap, Nessus, Snort, Wireshark, entre otras. Que permitieron identificar puertos abiertos en la red del hospital para evaluar posibles vulnerabilidades, además

permitieron detectar sitios web maliciosos que puedan comprometer la seguridad de la red del hospital.

El personal en encargado de la seguridad de la red y que administra los equipos tecnológicos no ha recibido la formación de seguridad informática adecuada.

La alta dirección está comprometida con los procesos y la dotación de los recursos que involucran la implementación de políticas de seguridad como la que se ha planteado.

1.2 Problema científico.

¿Cómo el diseño de un SGSI bajo la norma ISO 27001:2013 ayudara a reducir los riesgos y amenazas de seguridad de la información en el Hospital Santa Teresita?

1.3 Objeto de estudio.

El objeto de estudio será la gestión de la seguridad de las redes en los equipos tecnológicos y servicios en el Hospital Santa Teresita ya que es de suma importancia en un entorno hospitalario por la necesidad de proteger datos sensibles de los pacientes, garantizar la disponibilidad de los sistemas críticos de atención médica y cumplir con normativas y estándares de seguridad internacionales.

Determinar el objeto de estudio ayuda a definir las métricas necesarias para cubrir todos los procesos requeridos.

Algunas de las métricas que se han considerado en el objeto de estudio son:

- Métricas de seguridad de la red (número de incidentes de seguridad de red, tiempo de respuesta a incidentes, tasa de detección de intrusiones, disponibilidad de la red).
- Métricas de seguridad de los equipos informáticos (número de equipos actualizados, frecuencia de auditorías de seguridad, tasa de incidentes por malware)

- Métricas de seguridad de los servicios (disponibilidad de servicios críticos, tiempo medio entre fallos, tasa de satisfacción del usuario).
- Métricas protección de datos sensibles (número de violaciones de datos, tiempo de detección de violaciones de datos, frecuencia de capacitación en seguridad).
- Métricas cumplimiento normativo (número de auditorías de cumplimiento, resultados de auditorías de cumplimiento, implementación de políticas de seguridad).

1.4 Campo de acción.

En el campo de acción se desarrollará el diseño de las políticas de seguridad bajo el modelo de un SGSI conforme con los requisitos de la normativa ISO 27001:2013.

Este proceso se realizará considerando las siguientes actividades y delimitaciones:

- Determinar la evolución de las amenazas y vulnerabilidades de los activos de información de la gestión de la seguridad de las redes en los equipos tecnológicos y servicios en el Hospital Santa Teresita.
- Valorar la situación actual de los activos de información de la gestión de la seguridad de las redes en los equipos tecnológicos y servicios en el Hospital Santa Teresita.
- Fundamentar teóricamente el diseño de las políticas de seguridad bajo el modelo de un SGSI basado en la norma ISO 27001:2013.
- Elaborar las recomendaciones metodológicas para el diseño de las políticas de seguridad bajo el modelo de un SGSI basado en la norma ISO 27001:2013.
- Elaborar el informe técnico al concluir el proceso, detallando los resultados obtenidos y proporcionando recomendaciones y sugerencias finales que puedan guiar en la toma de decisiones.

1.5 Objetivos.

General

Diseñar las políticas de seguridad bajo el modelo de un SGSI basado en la normativa ISO 27001:2013 para la gestión de la seguridad de las redes en los equipos tecnológicos y servicios del departamento de TIC del Hospital Santa Teresita, con el fin de proteger los activos de información y garantizar la continuidad operativa de manera segura.

Específicos

- Analizar el estado actual de la gestión de la seguridad de las redes en los equipos tecnológicos y servicios del departamento de TIC del Hospital Santa Teresita para determinar si cuenta con controles de seguridad.
- Describir las vulnerabilidades, amenazas y riesgos de la gestión de la seguridad de las redes en los equipos tecnológicos y servicios del departamento de TIC del Hospital Santa Teresita basado en la metodología MAGERIT, la misma que permitirá minimizar los riesgos.
- Entregar un informe técnico, detallando los resultados obtenidos y proporcionando recomendaciones y sugerencias finales que puedan guiar en la toma de decisiones.

1.6 Justificación

Los casos de ataques y vulnerabilidades en los sistemas informáticos son un problema común a diario en todo el mundo. Es ampliamente reconocido que América Latina todavía tiene un largo camino por recorrer para abordar los desafíos de la ciberseguridad. Los gobiernos de la región recién están comenzando a comprender la importancia de este campo dentro del ámbito de la informática, así como los marcos legales correspondientes que son esenciales para este contexto. (Antonio, 2021)

Las organizaciones han empleado numerosos mecanismos y medidas de seguridad para salvaguardar sus activos informáticos. Sin embargo, estos han demostrado ser insuficientes para cumplir sus objetivos de seguridad. Como resultado, la legislación y la comunidad internacional han colaborado para crear estándares y regulaciones relativas a la seguridad de la información. Estos marcos establecen criterios para evaluar, medir, prevenir, mitigar y abordar riesgos que podrían provocar pérdidas comerciales, daños a la reputación corporativa, repercusiones legales e incluso el cierre de negocios. (Alemán & Helena, 2015)

Por esta razón, la investigación tiene como objetivo fortalecer la infraestructura de ciberseguridad del Hospital Santa Teresita. Se diseñó políticas de seguridad bajo el modelo de un SGSI adaptado a las necesidades del departamento de TIC, para poder recuperarse satisfactoriamente de un fallo ante amenazas digitales. Se identificaron vulnerabilidades y se tomarán medidas de seguridad adecuadas para proteger la información confidencial y garantizar la continuidad de las operaciones del hospital.

Además, la investigación también se centró en la concientización del personal, promoviendo una cultura de seguridad de la información. Esto creó un entorno seguro y colaborativo, donde cada miembro del equipo está comprometido con la protección activa de la información. En resumen, el SGSI propuesto es una herramienta integral para salvaguardar los datos médicos y administrativos, asegurando los servicios de salud del Hospital Santa Teresita.

El SGSI propuesto cumple con las obligaciones éticas de proteger la privacidad del paciente y garantizar la continuidad de la atención. Además, aumentará la resiliencia del hospital ante posibles incidentes de seguridad, permitiendo una acción rápida y eficiente.

1.7 Fundamentación teórica

Actualmente, la información es crucial para todas las organizaciones, por lo tanto, es necesario protegerla de cualquier peligro o debilidad que pueda comprometer su confidencialidad, disponibilidad e integridad.

Activo de información

Todo lo que se considera valioso se considera un activo organizacional, incluida la información física y digital, el software, el hardware, los servicios de información y las comunicaciones, y debe protegerse. Servicios, servicios de hosting, personas, imagen, reputación (Poveda, 2015).

Amenazas informáticas

La seguridad de los sistemas de información es importante debido a la posibilidad de que ocurran eventos que puedan causar daño material o inmaterial. Estos eventos se pueden clasificar en diferentes categorías:

Amenazas criminales: acciones realizadas por personas que violan las normas y las leyes.(Perdomo & Mateus, 2018)

Sucesos de origen físico: eventos naturales o provocados por el ser humano que causan daños físicos.(Ruiz, 2018)

Negligencia: omisiones, decisiones o acciones realizadas por personas que pueden deberse a desconocimiento, falta de capacitación o abuso de autoridad.(Delgado, 2017)

Es importante tener en cuenta que las amenazas a los sistemas de información están presentes en diferentes situaciones, como el uso de dispositivos de almacenamiento externos, la

navegación en sitios web o incluso la insatisfacción de los empleados dentro de una compañía. Los tipos de amenazas pueden variar según el efecto que causen en el sistema. (Guzmán, 2015)

Seguridad informática

La seguridad informática es una disciplina que busca proteger la información guardada en un sistema informático. No hay una técnica infalible para garantizar la seguridad de un sistema.

Existen dos formas de proteger un sistema informático: desde el punto de vista lógico, mediante el desarrollo de software; y desde el punto de vista físico, a través del mantenimiento eléctrico y los dispositivos de almacenamiento.

Las amenazas a la seguridad informática pueden surgir de programas dañinos instalados en la computadora del usuario, como virus, o pueden llegar de forma remota a través de conexiones no autorizadas a Internet. (Hernández, 2016)

La seguridad informática se ocupa de salvaguardar la información dentro de un sistema informático; sin embargo, lograr una seguridad absoluta sigue siendo un objetivo difícil de alcanzar. Se pueden implementar acciones a nivel lógico como físico, y es importante considerar los posibles riesgos tanto originados desde el interior como desde el exterior.(Yuver, 2018)

Seguridad de la información

Esto incluye proteger la información de una variedad de amenazas para garantizar la continuidad del negocio, minimizar los riesgos y maximizar el retorno de la inversión y las oportunidades comerciales.(Yanez, 2007)

Los principales objetivos de la seguridad de la información son:

Confidencialidad: Una característica que indica que solo pueden acceder a un activo empleados, procesos o entidades autorizadas con los privilegios adecuados.(Rojas, 2023)

Integridad: Características que protegen la exactitud, calidad, honestidad, equidad e integridad de un activo.(Moreno & Otalora, 2020)

Disponibilidad: Característica que indica que un activo es oportuno. Esto significa que individuos, organizaciones o procesos pueden acceder a los activos y utilizarlos cuando sea necesario. (Niño, 2019)

Análisis de riesgos

El primer paso en la gestión de riesgos es el análisis de riesgos. Para evaluar el nivel de riesgo, se pretende identificar los componentes del sistema que requieren protección, las vulnerabilidades que los debilitan y las amenazas que los ponen en riesgo. (Markus, 2018)

Existen varios métodos para la evaluación de riesgos, pero el punto de partida es identificar los activos de información, que son todos los recursos involucrados en la gestión de la información. Es necesaria una gestión de riesgos adecuada para ayudar a las instituciones a identificar vulnerabilidades clave en sus activos de información y las amenazas que pueden explotar esas vulnerabilidades. Siempre que una institución entienda claramente la identificación de este riesgo, se podrán establecer medidas preventivas y correctivas. Construiremos un sistema para garantizar un mayor nivel de seguridad de la información. (Palacios, 2015)

Sistema de gestión de la seguridad de la información

Según ISO 27001:2013, la seguridad de la información implica mantener la confidencialidad, integridad y disponibilidad de los sistemas involucrados en el procesamiento de información dentro de una organización. (Guerrero & Tabango, 2014)

Por lo tanto, los siguientes tres términos forman la base de toda la arquitectura de seguridad de la información:

- **Confidencialidad:** La información no se proporciona ni se divulga a personas, organizaciones o procesos no autorizados.
- **Integridad:** Mantener la exactitud e integridad de la información y cómo se procesa.
- **Disponibilidad:** Acceso y uso de la información y los sistemas de procesamiento de información por parte de personas, organizaciones o procesos autorizados, según sea necesario. Para garantizar que la seguridad de la información se gestione adecuadamente, se debe utilizar, registrar y comunicar en toda la organización un proceso sistemático basado en un enfoque de riesgo empresarial.

El SGSI debe lograrse a través de procesos sistemáticos y documentados en toda la organización. Este modelo de gestión de la seguridad debe prever procesos adecuados, así como la planificación e implementación de controles de seguridad basados en el análisis y evaluación de riesgos y la medición de su eficacia. (Ruiz, 2024)

Por tanto, un SGSI ayuda a establecer estas políticas y procedimientos en relación con los objetivos de negocio de la organización para mantener siempre un nivel de riesgo inferior al que asume la propia organización. La adopción de este estándar debe verse como una decisión estratégica de la organización.

El ciclo PHVA a un SGSI basado en ISO27001.

El ciclo de PHVA se puede definir de la siguiente manera:

- La planificación se inicia el establecimiento de un SGSI. Esta fase implica realizar análisis y evaluación de riesgos, desarrollar un plan de tratamiento de riesgos y formular políticas de seguridad.
- Desarrollar y mantener en funcionamiento el SGSI. Esto implica llevar a cabo la implementación y el mantenimiento de los controles correspondientes.
- La verificación del SGSI implica la evaluación de logros, la realización de auditorías internas y la revisión por parte de la alta dirección de la entidad.
- Se busca mejorar continuamente el SGSI a través de la implementación de medidas preventivas y correctivas.

No se puede garantizar una protección absoluta, incluso con recursos financieros ilimitados. El objetivo de un sistema de gestión de seguridad de la información es asegurar que la organización adquiera, gestione y disminuya los riesgos de seguridad de la información de manera formal, metódica, organizada, repetible, eficaz y adaptable a los cambios en los riesgos, el entorno y las tecnologías.

MAGERIT

Es la metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que, en la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. (Ministerio de Hacienda y Administraciones Públicas, 2012)

Ciberseguridad

La ciberseguridad se refiere a las medidas y procedimientos diseñados para proteger diversos elementos tecnológicos, como computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos, de posibles amenazas provenientes de ataques malintencionados. Además, esta área de protección también es referida como seguridad de la tecnología de la información o seguridad de la información electrónica. La expresión se utiliza en una variedad de situaciones, abarcando desde el ámbito empresarial hasta el campo de la tecnología móvil, y se puede clasificar en varias categorías.(Torres, 2024)

Ciberamenazas

Las ciberamenazas se refieren a las actividades llevadas a cabo en el ciberespacio con el fin de utilizar la información circulante para cometer diversos delitos a través de su manipulación, control o sustracción. Dado que el ciberespacio es el entorno donde se originan las amenazas cibernéticas, es importante comprender su concepto previamente.(Ruiz, 2016)

Cyberwarfare o Ciberguerra

Podemos definir el término ciberespionaje de manera amplia y sencilla como cualquier acción emprendida por individuos, competidores, oponentes, grupos y gobiernos, especialmente enemigos, para obtener una ventaja, ya sea personal, económica, política o militar, utilizando recursos. Tecnología de Internet, computadoras personales y redes, mediante el uso de técnicas de piratería informática y malware, incluidos troyanos y spyware. De esta forma, todo el procedimiento podrá realizarse desde los ordenadores personales de expertos en estas operaciones, ya sean aficionados locales o espías gubernamentales entrenados en estas actividades.(Quiñones, 2021)

Capítulo II. Diagnóstico situacional

2.1 Metodología

La metodología propuesta para el diseño del SGSI se basará en MAGERIT de la norma ISO 27001:2013.

La metodología MAGERIT, enfocada en la SGSI, es una herramienta fundamental para el diseño de un SGSI en entornos hospitalarios.

En la fase de planificación, se identifican los objetivos del SGSI, los recursos disponibles y se establece el alcance del proyecto. Es crucial comprender el entorno tecnológico hospitalario, incluyendo la infraestructura de IT, los sistemas de información utilizados y los riesgos específicos asociados a la seguridad de la información en este contexto.

Se debe realizar un análisis exhaustivo de los activos de información crítica en el hospital, como registros médicos, datos de pacientes, información administrativa y de investigación, entre otros. Esto implica identificar las amenazas potenciales que podrían comprometer la confidencialidad, integridad y disponibilidad de estos activos. Además, se evalúan las vulnerabilidades existentes en los sistemas tecnológicos hospitalarios que podrían ser explotadas por amenazas internas o externas.

La fase de planificación también incluye la definición de los criterios de evaluación de riesgos y la selección de las técnicas adecuadas para su análisis, como el análisis cuantitativo o cualitativo. Es esencial involucrar a todas las partes interesadas relevantes, incluyendo personal médico, administrativo, de IT y seguridad, para garantizar una comprensión completa de los riesgos y una colaboración efectiva en la implementación del SGSI.

En la fase de diseño, se elabora un plan detallado para implementar el SGSI en los equipos tecnológicos del hospital, basado en los resultados obtenidos durante la fase de planificación. Esto implica la definición de políticas, procedimientos y controles de seguridad de la información que mitiguen los riesgos identificados y cumplan con los requisitos legales y regulatorios pertinentes.

La metodología MAGERIT proporciona un marco estructurado para la selección e implementación de controles de seguridad, clasificándolos en preventivos, detectivos y correctivos. Se deben establecer medidas de seguridad técnicas, como firewalls, sistemas de detección de intrusos, encriptación de datos y autenticación multifactorial, así como medidas organizativas, como la sensibilización y formación del personal, la gestión de accesos y la continuidad del negocio.

Es esencial realizar pruebas y simulacros de los controles implementados para garantizar su eficacia y realizar ajustes según sea necesario. Además, se debe documentar todo el proceso de diseño del SGSI, incluyendo los criterios de selección de controles, las decisiones tomadas y los cambios realizados en función de las pruebas realizadas.

La fase de evaluación consiste en verificar si el SGSI diseñado en los equipos tecnológicos del hospital cumple con los objetivos establecidos y proporciona un nivel adecuado de seguridad de la información.

La metodología MAGERIT facilita la realización de evaluaciones de riesgos periódicas para garantizar que el SGSI se adapte a los cambios en el entorno tecnológico y a las nuevas amenazas emergentes. Se deben revisar y actualizar regularmente las políticas y procedimientos de seguridad.

En resumen, el diseño de un SGSI en los equipos tecnológicos de la seguridad de la red utilizando la metodología MAGERIT requiere una planificación cuidadosa, un diseño detallado y una evaluación continua para garantizar la protección de la información sensible y la continuidad de las operaciones clínicas y administrativas del hospital.

2.2 Análisis situacional

El Hospital Santa Teresita, clasificado como un hospital tipo B en Ecuador, enfrenta desafíos específicos en la gestión de la información debido a su infraestructura y recursos limitados. Internamente, el hospital debe lidiar con la falta de políticas y procedimientos documentados para la seguridad de la información, un problema común en muchos hospitales de tamaño similar. La formación y concienciación del personal sobre la seguridad de la información también es insuficiente, lo que aumenta el riesgo de errores humanos y vulnerabilidades.

Externamente, el hospital debe cumplir con las regulaciones nacionales e internacionales relacionadas con la protección de datos de pacientes, como la Ley Orgánica de Protección de Datos Personales de Ecuador. Además, la creciente amenaza de ciberataques en el sector de la salud plantea un riesgo significativo. La interoperabilidad con otros sistemas de salud y la necesidad de compartir información médica de manera segura con entidades externas también son consideraciones importantes.

Por esta razón es necesario el diseño de un SGSI conforme a la normativa ISO 27001:2013 no solo ayudará a mitigar los riesgos identificados, sino que también fortalecerá la confianza de los pacientes en la capacidad del hospital para proteger sus datos personales. La clave del éxito radica en el compromiso continuo del personal y la alta dirección, la actualización tecnológica, y la creación de una cultura organizacional orientada a la seguridad de la información.

2.3 Análisis comparativo

La elección de ISO 27001:2013 para el diseño del SGSI del Hospital Santa Teresita está justificada por su reconocimiento internacional, popularidad en América Latina, capacidad para asegurar conformidad regulatoria, enfoque sistemático en la gestión de riesgos, énfasis en la mejora continua, facilidad de integración con otros sistemas de gestión y la disponibilidad de recursos y apoyo. Estas ventajas hacen de ISO 27001:2013 sea la opción más adecuada y estratégica para mejorar la seguridad de la información en el Hospital Santa Teresita, protegiendo así los datos sensibles de los pacientes y fortaleciendo la confianza en la institución.

Aunque existen otras normativas que pueden apoyar la implementación de un SGSI como NIST (National Institute of Standards and Technology) SP 800-53, está diseñado principalmente para organizaciones gubernamentales en los Estados Unidos y puede no ser directamente aplicable o reconocible en el contexto ecuatoriano y latinoamericano en general. Su adopción en sectores privados y fuera de EE.UU. es menos común.

La COBIT (Control Objectives for Information and Related Technologies) incluye aspectos de seguridad de la información, no está específicamente enfocado en la seguridad de la información y puede ser menos detallado en comparación con ISO 27001:2013 en este aspecto.

HIPAA (Health Insurance Portability and Accountability Act) está específicamente diseñada para el contexto de EE.UU. y puede no alinearse con las regulaciones y necesidades del sector salud en Ecuador. Además, no tiene el enfoque holístico y la estructura de gestión sistemática que ofrece ISO 27001:2013.

Otras normativas pueden apoyar la implementación de un SGSI, pero ISO 27001:2013 ofrece ventajas significativas en términos de reconocimiento internacional, compatibilidad con

otros estándares, enfoque holístico, y adecuación al contexto específico de América Latina. Estas razones hacen de ISO 27001:2013 la elección más adecuada y estratégica para el Hospital Santa Teresita, garantizando un alto nivel de seguridad y conformidad regulatoria.

2.4 Herramientas

Las herramientas que se utilizaron para el desarrollo del proyecto fueron las siguientes:

- Software: Microsoft Project, Nessus, Wireshark, Splunk, Microsoft Office Suite, Winbox, Putty, software gestor de citas bibliográficas Mendeley, Navegadores de internet entre otros.
- Hardware: PC portatil, Impresora, Tester de red.
- Otros: Encuestas impresas, lapiceros, hojas.

2.5 Operacionalización de Variables

Variable Independiente:

- Sistema de Gestión de Seguridad de la Información (SGSI)

Variable Dependiente:

- Identificación de las amenazas de los equipos tecnológicos.
- Analizar las vulnerabilidades de los equipos tecnológicos.
- Determinar los riesgos de los equipos de tecnológicos.

Tabla 1.*Conceptualización de variables.*

Conceptualización	Unidad de medida	Instrumento
Identificación de las amenazas mediante la escala de Likert. Determina los criterios específicos que se utilizarán para evaluar cada riesgo. Estos criterios pueden incluir la probabilidad de ocurrencia, el impacto potencial, la criticidad, la exposición, entre otros factores relevantes para tu contexto.	Niveles cualitativos de adopción (Alto, Medio, Bajo)	Escala de Likert
Analizar las vulnerabilidades mediante la escala de Likert es necesario identificar las vulnerabilidades relevantes en el sistema, red o proceso que se está evaluando. Esto puede hacerse a través de una revisión exhaustiva del sistema, análisis de código, pruebas de penetración, entre otros métodos.	Niveles cualitativos de adopción (Alto, Medio, Bajo)	Escala de Likert
Determinación de Riesgos mediante la escala de Likert, es fundamental identificar los riesgos potenciales que podrían afectar al sistema, proyecto o proceso que se está evaluando. Esto puede hacerse mediante revisión de documentos, análisis de incidentes previos, entre otros métodos.	Niveles cualitativos de adopción (Alto, Medio, Bajo)	Escala de Likert

Nota. Elaborado por el autor del documento.

Capítulo III. Propuesta

3.1 Organización

3.1.1 Reseña Histórica de la Institución.

El 27 de febrero de 1949, fueron traídas a esta ciudad las Hermanas Misioneras de Santa Teresita, de nacionalidad colombiana, Beatriz, Anunciación Nazaret, Inocencia y Catalina, gracias a la gestión realizada por el Padre Ángel Tinoco Ruíz, Párroco de ese entonces, de la ciudad de Santa Rosa las mismas que a partir de esa fecha, trabajaron en una forma humanitaria y abnegada por el bienestar de cada uno de los pacientes que acuden a esta Unidad Operativa, tanto físico como espiritual.

En vista que el Hospital, conocido en ese entonces como María de Lourdes, y con el pasar del tiempo, su infraestructura física se fue deteriorando, y es por esta razón, que el pueblo santarroseño juntamente con las Hermanas Misioneras de Santa Teresita, creyeron conveniente realizar actividades para conseguir fondos económicos para la construcción de nuevos pabellones, y es así que el 11 de julio de 1.964 se coloca la primera piedra, obra que fue alcanzada, gracias al trabajo místico y abnegado de personas de sentimientos nobles, por lo que se pudo cristalizar este objetivo.

Y es así, que en el año de 1.972, se inaugura el nuevo Hospital, y en el año de 1974, el presidente de la República del Ecuador, a través del Sr. Ministro de Salud Pública, acuerda cambiarle el Nombre de María de Lourdes a “SANTA TERESITA”, según Acuerdo Ministerial No. 3080 del 28 de Febrero de 1.974, en homenaje a sus Bodas de Plata y en tributo de agradecimiento del pueblo de Santa Rosa, a la Congregación Religiosa de las HERMANAS MISIONERAS DE SANTA TERESITA, por su admiración y respeto a la fecunda misión desarrollada en beneficio de la sociedad.

La Conformación de las Coordinaciones Zonales, dio paso a la creación de los diferentes Distritos, así la Dirección Distrital 07D06 Santa Rosa - Salud, fue creada el 14 de julio del 2014 con Acuerdo Ministerial 4921 constituyendo EOD.

El Distrito 07D06 Santa Rosa, se encuentra localizado en el cantón Santa Rosa ubicado en las calles Av. Joffre Lima 506 y Franco Romero, cuenta con 19 Establecimientos de Salud, 17 de Primer Nivel y 1 de Segundo Nivel y un CETAD establecidos con la siguiente tipología:

CENTROS DE SALUD: teniente Hugo Ortiz, Las Cañas, 29 de noviembre, La Avanzada, Jumón, Santa Rosa.

PUESTOS DE SALUD: Bellavista, Martha Bucarán, San José, San Antonio, San Agustín, Bellamaria, Valle Hermoso, La Victoria, Rio Negro, Jambelí y Costa Rica.

SEGUNDO NIVEL: Hospital Básico Santa Teresita.

CETAD: Centros Especializados en Tratamiento a Personas con Consumo Problemático de Alcohol y otras Drogas.

3.1.2 Misión

Ejercer la rectoría, regulación, planificación, coordinación, control y gestión de la Salud Pública ecuatoriana a través de la gobernanza y vigilancia y control sanitario y garantizar el derecho a la Salud a través de la provisión de servicios de atención individual, prevención de enfermedades, promoción de la salud e igualdad, la gobernanza de salud, investigación y desarrollo de la ciencia y tecnología; articulación de los actores del sistema, con el fin de garantizar el derecho a la Salud.

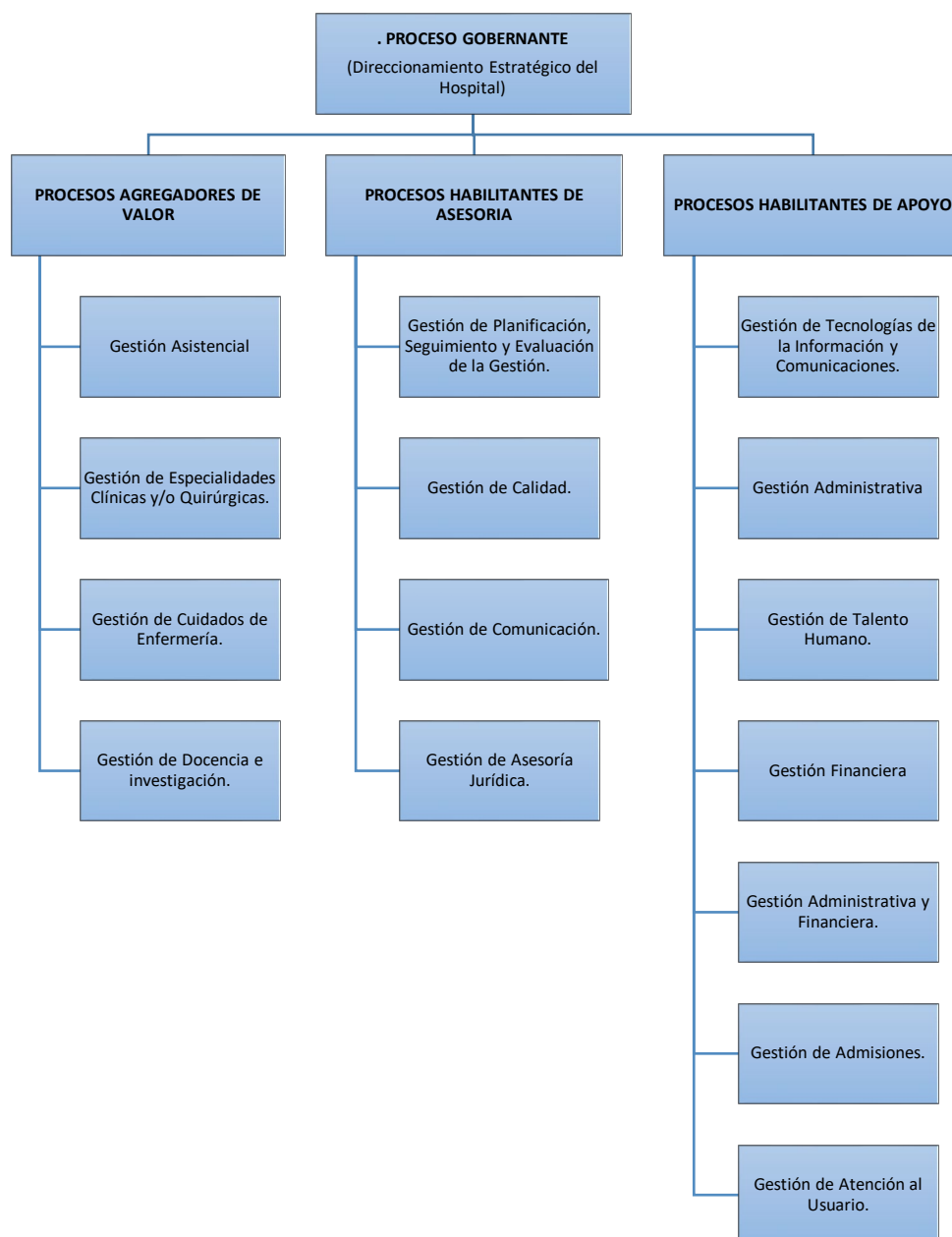
3.1.3 Visión

El Ministerio de Salud Pública, ejercerá plenamente la gobernanza del Sistema Nacional de Salud, con un modelo referencial en Latinoamérica que priorice la promoción de la salud y la prevención de enfermedades, con altos niveles de atención de calidad, con calidez, garantizando la salud integral de la población y el acceso universal a una red de servicios, con la participación coordinada de organizaciones públicas, privadas y de la comunidad.

3.1.4 Organigrama

Figura 1.

Organigrama Institucional de Hospital Santa Teresita.



Nota. Elaborado por el autor del documento.

3.1.5 Matriz de análisis FODA.

La elaboración de la matriz FODA nos permitió obtener una visión clara de la situación actual y desarrollar estrategias para mejorar la seguridad informática, aprovechando las fortalezas y oportunidades mientras mitigan las debilidades y amenazas.

Mediante la siguiente tabla mostraremos un análisis de fortalezas, debilidades, oportunidades y amenazas que se aplicó en el departamento de TIC de Hospital Santa Teresita.

Tabla 2.

Análisis FODA aplicada en el departamento de TIC en marco a la seguridad informática.

FODA		
	INTERNO DEBILIDADES	EXTERNO AMENAZAS
NEGATIVOS	• Presupuesto limitado para la adquisición de nuevas tecnologías y la actualización de equipos existentes. • Resistencia por parte del personal del hospital a adoptar nuevas tecnologías y métodos de trabajo. • Ausencia de políticas y procedimientos claros en cuanto a la gestión de la seguridad de la información. • Capacidad limitada para responder a incidentes de ciberseguridad de manera rápida y efectiva.	• Aumento de las amenazas cibernéticas, como malware, ransomware y ataques de phishing, que pueden comprometer la seguridad de la información del hospital. • Riesgo de no cumplir con las regulaciones y normativas de seguridad de la información, lo que puede resultar en sanciones y pérdida de confianza. • Rápido avance tecnológico que puede dejar obsoletos los sistemas y equipos actuales. • Riesgo de pérdida o robo de datos sensibles de los pacientes, lo que puede afectar la reputación del hospital y la confianza de los pacientes.
POSITIVOS	FORTALEZAS	OPORTUNIDADES

	• El hospital cuenta con equipos y redes de alta calidad que soportan las operaciones diarias. • El departamento de TIC está compuesto por profesionales con experiencia y conocimientos actualizados en tecnología y ciberseguridad. • Disponibilidad de soporte técnico rápido y eficaz para resolver problemas tecnológicos y mantener el sistema funcionando sin interrupciones. • Los sistemas de información del hospital están bien integrados, lo que facilita la gestión de datos y mejora la eficiencia operativa.	• Posibilidad de adoptar tecnologías emergentes como inteligencia artificial y big data para mejorar la atención al paciente y la gestión hospitalaria. • Disponibilidad de fondos y subvenciones para proyectos de mejora tecnológica y ciberseguridad. • Oportunidades para establecer alianzas con otros hospitales y organizaciones para compartir recursos y conocimientos en tecnología de la información. • Adopción de estándares internacionales como ISO 27001 para mejorar la gestión de la seguridad de la información y cumplir con las regulaciones.
--	---	---

Nota. Elaborado por el autor del documento y Analista de TIC de Hospital Santa Teresita.

3.2 Análisis del problema

Los problemas que se identificaron en la seguridad de la red en los equipos tecnológicos y servicios del departamento de TIC del Hospital Santa Teresita fueron:

- Ataques continuos en el servidor de correo institucional, se evidencio en el log eventos en las redes externas e internas. A pesar de contar con equipos de seguridad, no se analizan las evidencias de ataques ni hay un plan de remediación. No tienen procedimientos para acceder y manejar la información en todos los ámbitos.
- Perdida de datos confidenciales propios y de pacientes. La información está en un Servidor de Archivos sin restricciones de acceso ni clasificación de información. En el servidor se aloja información variada como copias de seguridad, datos de pacientes,

informes de trabajo y proyectos, y análisis financiero. El hospital no tiene respaldo de la información confidencial.

- Políticas implementadas de manera incorrecta el cual permite la manipulación de la información de los pacientes y de varios documentos importantes.

3.3 Impacto del problema en el Hospital

El impacto que provoca estos problemas en la seguridad de la red en los equipos tecnológicos y servicios del departamento de TIC del Hospital Santa Teresita son los siguientes:

- El impacto de los ataques continuos, la falta de análisis de logs, la ausencia de un plan de remediación y la carencia de procedimientos claros para manejar la información incrementan la vulnerabilidad del sistema, afectan la operatividad del hospital y ponen en riesgo la privacidad y seguridad de la información de los pacientes.
- El impacto de la privacidad de los pacientes se ve comprometida, la reputación del hospital puede sufrir daños irreparables, y las consecuencias legales pueden ser significativas. Además, la falta de clasificación y restricciones de acceso a la información incrementa los riesgos de acceso no autorizado y pérdida de datos, mientras que la ausencia de respaldos puede resultar en una pérdida irreversible de información crítica y costosas interrupciones operativas.
- El impacto de la manipulación indebida de información y documentos puede resultar en pérdida de confianza, problemas financieros, y riesgos legales y de ciberseguridad.

3.4 Causas del problema

Las causas que podrían generar los problemas antes mencionados son los siguientes:

- Las causas incluyen la falta de análisis de evidencias de ataques a pesar de contar con equipos de seguridad. Esto señala una carencia en la implementación de un plan de remediación efectivo y en la gestión proactiva de la seguridad de la información tanto en redes internas como externas.
- La causa de la pérdida de datos confidenciales es originada por la ausencia de restricciones de acceso y de una clasificación adecuada de la información en el Servidor de Archivos. Esto resulta en la exposición de datos sensibles como copias de seguridad, información de pacientes, informes y análisis financieros, sin contar con respaldos adecuados para proteger la información crítica.
- La manipulación indebida de la información de pacientes y otros documentos importantes sugiere una falta de implementación efectiva de políticas de seguridad. Esto puede deberse a la falta de capacitación, supervisión y revisión de las políticas establecidas para proteger la información sensible del hospital.

3.5 Solución al problema

Debido a los problemas de seguridad en la red que fueron identificados en la administración de los equipos tecnológicos y servicios del departamento de TIC, se consideró imprescindible adoptar un modelo o sistema disponible a nivel mundial que pudiera ofrecer una solución completa y a largo plazo a los desafíos enfrentados. Basándose en esta premisa, el Hospital Santa Teresita considera que sería beneficioso implementar un Sistema de Gestión de Seguridad de la Información, el cual se sustenta en la normativa ISO/IEC 27001:2013. Dentro de sus procedimientos y lineamientos internos, este SGSI permitirá a la organización llevar a cabo las siguientes acciones:

- Clasificar los activos de información más importantes que forman parte de la seguridad de la red del departamento de Tecnologías de la Información y Comunicación del Hospital Santa Teresita.
- Identificar y analizar los posibles peligros relacionados con la seguridad que amenazan la protección de los recursos de información en el entorno del departamento de TIC del Hospital Santa Teresita y sugerir un plan detallado para gestionar los riesgos involucrados en la situación en cuestión.

3.6 Resultados esperados.

Los resultados esperados son los siguientes:

- Conseguir la categorización de los activos de información según los principios fundamentales de la Seguridad de la Información, que incluyen la protección de la confidencialidad, la garantía de la integridad de los datos y la disponibilidad de los mismos.
- Identificar con precisión las vulnerabilidades más significativas en cuanto a seguridad de la información, analizando cómo la ejecución de posibles amenazas podría afectar al activo de información valuado en caso de que se concretase.
- Establecer un modelo detallado para gestionar de manera efectiva los riesgos relacionados con los activos de información que tienen un valor significativo.
- Crear la Declaración de Aplicabilidad (SOA) que incluya los controles de seguridad necesarios y previamente identificados, los cuales deben ser seleccionados de acuerdo a cada nivel de riesgo relacionado con cada activo de información y su respectivo valor.

- Definir los roles y responsabilidades conforme a la estructura organizacional de seguridad de la información.

3.7 Análisis actual de la seguridad y privacidad del Hospital Santa Teresita

Este punto se llevan a cabo consultas relacionadas con la actual situación de seguridad y privacidad del hospital, investigando y analizando a fondo la protección de datos y la gestión de riesgos en el entorno organizacional.

Donde se establecen tres niveles de conformidad de acuerdo con lo señalado en la normativa ISO/IEC 27001:2013.

Los estados son definidos y descritos a continuación:

- **Satisfactoriamente:** La organización lo acepta y maneja de manera adecuada. Está registrado en un documentado y es conocimiento general del personal. Su implementación cumple con la norma ISO 27001:2013. Se cumple en su totalidad al 100%.
- **Parcialmente:** Su aplicación cumple parcialmente con los requisitos de la norma ISO 27001:2013. Aunque fue aprobado por el personal de TIC, no está gestionado ni documentado.
- **No cumple:** No existe.

Bajo los niveles de conformidad establecidos se procedió a realizar las siguientes preguntas al personal que administra la seguridad de la red:

Tabla 3.

Análisis de la Seguridad y privacidad del Hospital Santa Teresita.

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
1	¿Existe en la organización un plan de proyecto que contemple las prioridades y metas para la implementación del Sistema de Gestión de Seguridad de la Información?	Parcialmente	La organización planea diseñar un SGSI, pero todavía no lo han iniciado. Tiene un objetivo principal definido pero no documentado todavía. Se basará en el diseño de este proyecto.	Diseñar un plan inicial del proyecto que defina prioridades, objetivos y la estructura del SGSI.
2	¿Se obtuvo la autorización de las autoridades superiores para dar inicio al proceso de implementación del Sistema de Gestión de Seguridad de la Información (SGSI)?	Parcialmente	La Alta Dirección y Gerencia General aprobaron el inicio de un SGSI, pero no se ha diseñado todavía.	Se necesita un documento firmado por la dirección para aprobar el inicio del proyecto.
3	¿La organización dispone de un mecanismo de autoevaluación para medir el progreso en el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información?	No cumple	La organización no tiene implementado un SGSI en este momento.	Después de implementar el SGSI, se recomienda realizar una autoevaluación.

4	¿La entidad ha analizado los factores internos y externos que podrían incidir en la ejecución del Sistema de Gestión de Seguridad de la Información?	Parcialmente	La organización ha identificado posibles obstáculos para implementar el Sistema de Gestión de Seguridad de la Información para la seguridad de la red, pero no hay un documento formal con esta información.	Los aspectos internos y externos que afectan la implementación del SGSI deben documentarse y revisarse por la Alta Gerencia y el personal involucrado en el proyecto.
5	¿Se ha registrado la información relacionada con el Sistema de Gestión de Seguridad de la Información por parte de la organización?	No cumple	La organización no tiene documentación ni ha implementado un Sistema de Gestión de Seguridad de la Información.	La documentación del Sistema de Gestión de Seguridad de la Información debe estar documentada durante su implementación y despliegue.
6	¿Se han identificado las partes interesadas y sus necesidades en la implementación del SGSI?	Parcialmente	Aunque se ha incluido a la Alta Dirección como interesada, la organización no ha definido documentación ni creado un plan de necesidades y expectativas por el momento.	Identificar partes interesadas, internas y externas, con sus necesidades y expectativas para el SGSI.
7	¿Se han evaluado los objetivos y necesidades relacionados con la gestión de la Seguridad de la Información en la organización?	Parcialmente	La organización ha evaluado el objetivo general y los objetivos específicos de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), pero aún no los ha documentado.	Documentar el objetivo general y objetivos específicos del SGSI.

8	¿Existe un Comité de Seguridad de la Información dentro de la organización?	No cumple	No hay una clasificación jerárquica para definir roles y responsabilidades en Seguridad de la Información en la Organización. La organización incluye la seguridad de la red en su Sistema de Gestión de Seguridad de la Información (SGSI). No hay documentación disponible todavía. No se ha revisado la implementación de una Política de Seguridad de la Información vinculada al SGSI en ninguna reunión. No hay documentación al respecto. No se ha realizado ninguna reunión para definir los roles, responsabilidades y autoridades en Seguridad de la Información. No hay documentación disponible.	Definir y documentar la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información para comunicarla a todos los empleados de la organización.
9	¿Se han establecido el alcance y los límites del Sistema de Gestión de Seguridad de la Información?	Parcialmente		Elaborar un documento formal que defina el alcance organizativo del SGSI.
10	¿La Alta Dirección ha aprobado una Política de Seguridad de la Información?	No cumple		Crear un documento de política de seguridad de la información.
11	¿Hay un documento oficial que describa roles, responsabilidades y autoridades en seguridad de la información?	No cumple		Definir, documentar y comunicar la estructura de seguridad de la información a los colaboradores.
12	¿Existe un proceso para gestionar los riesgos de seguridad de la información en la organización?	Parcialmente	La organización incluye la seguridad de la red en el alcance de su SGSI. No hay documentación aún.	La organización debe utilizar una metodología reconocida o propia para gestionar los riesgos. Describe los resultados en una matriz de riesgos según los criterios de aceptación de riesgos de la organización.

13	¿Se ha hecho un SOA (Declaración de aplicabilidad) con los controles de seguridad necesarios en la organización?	No cumple	No hay un SOA que especifique qué controles adoptar para la Gestión de Riesgos en los activos de información.	Redactar un documento de declaración de aplicabilidad que justifique la inclusión/exclusión de controles de ISO 27001:2013.
14	¿Se ha establecido un modelo de comunicación interna y externa vinculado a la seguridad de la información?	No cumple	No hay un modelo de comunicaciones para informar los avances sobre el SGSI o la Seguridad de Información.	Se requiere un modelo que identifique y rastree el contenido de la comunicación a lo largo del tiempo.
15	¿La organización ha revisado las habilidades de sus colaboradores sobre seguridad de la Información?	No cumple	No se evalúan las competencias de los colaboradores relacionadas con la Seguridad de la Información.	Deben comprobar las competencias del personal que trabaja con la seguridad de la información en la organización. Sin ellas, se debe crear un plan de capacitación para que las personas las adquieran. competencias respectivas.

Nota. Elaborado por el autor del documento

3.8 Diseño del SGSI.

Es importante tener presente que en este proyecto de investigación es fundamental considerar la delimitación del alcance del SGSI, así como establecer la política y objetivos, identificar y evaluar los riesgos, elegir los objetivos de control y los controles correspondientes, elaborar el plan de tratamiento de riesgos y el enunciado de aplicabilidad, y finalmente, llevar a cabo el diseño de las políticas de seguridad de la información basadas en los controles seleccionados de acuerdo a la normativa ISO/IEC 27001:2013.

3.9 Identificación de activos

Los criterios de valoración de que se ha considerado para proceso del diseño de políticas de seguridad bajo el modelo SGSI con la normativa ISO 27001:2013 y la metodología MAGERIT son las siguientes:

Tabla 4.

Identificación de Riesgos

R1	Riesgos Tecnológicos
R2	Riesgos Humanos
R3	Riesgo Operativo

Nota. Elaborado por el autor del documento

3.10 Evaluación de activos

El proceso de identificación de activos de información se realizó mediante la metodología MAGERIT, a continuación se describe los pasos para el análisis de riesgos que se llevó a cabo:

- Determinación y valoración de los activos relevantes en el departamento de TIC del Hospital Santa Teresita, asignando el tipo y valor.
- Identificación y valoración de amenazas categorizando los niveles de riesgos e impactos sobre los activos.
- Identificación de medidas de protección adecuadas y funcionales frente al riesgo.
- Realizar una evaluación del impacto del daño causado por la concreción de la amenaza en el activo.

- Realizar una evaluación del riesgo de impacto asociado a la aparición de la amenaza.

Se efectuaron reuniones vía zoom con el Representante Legal y el personal del departamento de TIC para identificar y clasificar los activos, encontrando un total de 39 activos de información de diferentes tipos.

Se utiliza el enfoque descrito en los libros I y II de MAGERIT para llevar a cabo la evaluación de los riesgos, donde se identifican las posibles amenazas que pueden afectar a los activos de información de la institución. Esta evaluación considera las dimensiones de valoración (Disponibilidad, Integridad, Confidencialidad) y los criterios de valoración.

Tabla 5.

Categoría activos de información MAGERIT

Activos Esenciales	
Nombre Categoría	ID
Información	Info
Servicio	Service
Activos Relevantes	
Nombre Categoría	ID
Datos/informacion	[D]
Servicios	[S]
Software	[SW]
Hardware	[HW]
Redes de comunicación	[COM]
Soporte de información	[MEDIA]

Nota. Elaborado por el autor del documento

La tabla muestra categorías de activos de información con sus respectivos ID, según MAGERIT, para facilitar la creación de inventario de activos de información.

Las siguientes tablas se podrá ver la relación que existe en el inventario de activos de información.

Tabla 6.

Activo de información por tipo Activo

DATOS DEL ACTIVO DE INFORMACION				
No.	Tipo de Riesgo	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
1	R3	Historias Clínicas	Margarita Torres	ACTIVO
2	R1	Base de datos Inventarios	Davis Sánchez	ACTIVO
3	R1	Base de datos pacientes	Luz Ochoa	ACTIVO
4	R1	Base de datos médicos	Luz Ochoa	ACTIVO
5	R1	Base de datos Administrativos	Christian Gómez	ACTIVO
6	R1	Copias de seguridad	Christian Gómez	DATOS
7	R1	Servidor de Correo	Davis Sánchez	SERVICIOS
8	R1	Servidor de Archivos	Christian Gómez	SERVICIOS
9	R1	Servidor Local	Christian Gómez	SERVICIOS
10	R1	Equipo computo Tecnología	Davis Sánchez	HARDWARE
11	R1	Equipo computo Tecnología	Christian Gómez	HARDWARE
12	R1	Equipo computo Tecnología	Luz Ochoa	HARDWARE
13	R1	Equipo computo Tecnología	Christian Gómez	HARDWARE
14	R1	Router Cisco	Christian Gómez	HARDWARE
15	R1	Router Mikrotik rb750gr3	Christian Gómez	HARDWARE
16	R1	Router HP	Christian Gómez	HARDWARE
17	R1	Switch Cisco	Christian Gómez	HARDWARE
18	R1	Switch HP	Davis Sánchez	HARDWARE

19	R1	Switch HP	Davis Sánchez	HARDWARE
20	R1	Switch HP	Davis Sánchez	HARDWARE
21	R1	Access Points	Christian Gómez	HARDWARE
22	R1	Access Points	Davis Sánchez	HARDWARE
23	R1	Access Points	Luz Ochoa	HARDWARE
24	R1	Telefonía móvil	Christian Gómez	COMUNICACIONES
25	R1	Internet	Christian Gómez	COMUNICACIONES
26	R1	Red local	Christian Gómez	COMUNICACIONES
27	R1	Rack de datos	Christian Gómez	AUXILIAR
28	R1	Fuentes de alimentación	Davis Sánchez	AUXILIAR
29	R1	Cableado	Davis Sánchez	AUXILIAR
30	R1	Oficina TIC	Christian Gómez	INSTALACIONES
31	R1	Oficina Gerencia Distrital	Laura Sánchez	INSTALACIONES
32	R1	Oficina Gerencia Hospital	Raúl Aguirre	INSTALACIONES
33	R1	Oficina Estadística	Margarita Torres	INSTALACIONES
34	R2	Laura Sánchez	Laura Sánchez	PERSONAL
35	R2	Raúl Aguirre	Raúl Aguirre	PERSONAL
36	R2	Margarita Torres	Margarita Torres	PERSONAL
37	R2	Christian Gómez	Christian Gómez	PERSONAL
38	R2	Luz Ochoa	Luz Ochoa	PERSONAL
39	R2	Davis Sánchez	Davis Sánchez	PERSONAL

Nota. Elaborado por el autor del documento

Podemos evidenciar en la tabla que los activos se clasifican según su Tipos de Archivo en “ACTIVO”, “SERVICIOS”, “HARDWARE”, “COMUNICACIONES”, “AUXILIAR”, “INSTALACIONES” y “PERSONAL”.

3.11 Valoración de los activos

Siguiendo la metodología MAGERIT del libro en el apartado 3. Las dimensiones de valoración determinan el valor de un activo y se utilizan para evaluar las consecuencias de una amenaza. A continuación se determina las dimensiones:

- **D.** La Disponibilidad afecta a todos los activos. Es valioso porque las consecuencias serán graves si una amenaza impacta la disponibilidad del activo.
- **I.** La integridad de los datos es muy valorada cuando alteraciones intencionadas causan daños graves a la organización.
- **C.** La confidencialidad de los datos es importante cuando su divulgación podría causar un daño significativo y no es importante cuando carece de valor, no genera preocupaciones.

Se definen las dimensiones de los activos y se valora su costo de recuperación después de un incidente. MAGERIT en su Libro I v.3 establece las acciones pertinentes. (Vargas, 2024)

- Coste de reposición: adquisición e instalación
- Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo
- Lucro cesante: pérdida de ingresos
- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- Sanciones por incumplimiento de la ley u obligaciones contractuales
- Daño a otros activos, propios o ajenos
- Daño a personas
- Daños medioambientales

A continuación se define el criterio de valoración de activos para Hospital Santa Teresita.

Tabla 7.*Criterios de valoración de activos*

Valoración Cualitativa	Escala de Valoración	Escala Cuantitativa Millones
21 a 25	Crítico	200
16 a 20	Importante	100 a 200
10 a 15	Apreciable	50 a 100
5 a 9	Bajo	10 a 50
1 a 4	Despreciable	0 a 10

Nota. Elaborado por el autor del documento

La tabla previa demuestra la definición de los criterios utilizados para evaluar los activos de información del departamento de TIC, utilizando una escala de valoración cualitativa de 1 a 25 y una escala de valoración que va desde despreciable hasta crítico, junto con una escala cuantitativa expresada en millones.

Se valora la información del departamento de TIC usando la Matriz Evaluación del Riesgo una vez definidos los criterios de valoración.

Se consideraron las amenazas a los activos de información según el catálogo del libro II Magerit v3.0 y las dimensiones (C, I, D) afectadas por cada amenaza.

Tabla 8.*Valoración de riesgo*

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoración del riesgo	MA	Crítico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Nota. Elaborado por el autor del documento

Tabla 9.*Valoración de activos*

Ítem	Nombre	Riesgo	Confidencialidad	Integridad	Disponibilidad	Valor
1	Historias Clínicas	CRITICO	20	25	20	22
2	Base de datos Inventarios	CRITICO	25	25	25	25
3	Base de datos pacientes	CRITICO	25	25	25	25
4	Base de datos médicos	CRITICO	25	25	25	25
5	Base de datos Administrativos	CRITICO	25	25	25	25

6	Copias de seguridad	CRITICO	25	25	25	25
7	Servidor de Correo	CRITICO	25	25	25	25
8	Servidor de Archivos	CRITICO	25	25	25	25
9	Servidor Local	CRITICO	25	25	25	25
10	Equipo computo Tecnología	APRECIABLE	15	15	15	15
11	Equipo computo Tecnología	APRECIABLE	15	15	15	15
12	Equipo computo Tecnología	APRECIABLE	15	15	15	15
13	Equipo computo Tecnología	APRECIABLE	15	15	15	15
14	Router Cisco	IMPORTANT E	20	20	20	20
15	Router Mikrotik rb750gr3	IMPORTANT E	20	20	20	20
16	Router HP	IMPORTANT E	20	20	20	20
17	Switch Cisco	APRECIABLE	15	15	15	15
18	Switch HP	APRECIABLE	15	15	15	15
19	Switch HP	APRECIABLE	15	15	15	15
20	Switch HP	APRECIABLE	15	15	15	15
21	Access Points	IMPORTANT E	20	20	20	20
22	Access Points	IMPORTANT E	20	20	20	20
23	Access Points	IMPORTANT E	20	20	20	20
24	Telefonía móvil	APRECIABLE	9	9	20	13
25	Internet	CRITICO	25	25	25	25
26	Red local	CRITICO	25	25	25	25
27	Rack de datos	CRITICO	25	25	25	25
28	Fuentes de alimentación	APRECIABLE	15	15	15	15
29	Cableado	IMPORTANT E	20	20	20	20
30	Oficina TIC	IMPORTANT E	20	20	20	20
31	Oficina Gerencia Distrital	IMPORTANT E	20	20	20	20
32	Oficina Gerencia Hospital	IMPORTANT E	20	20	20	20
33	Oficina Estadística	IMPORTANT E	20	20	20	20
34	Laura Sánchez	IMPORTANT E	20	20	20	20
35	Raúl Aguirre	IMPORTANT E	20	20	20	20
36	Margarita Torres	IMPORTANT E	20	20	20	20

37	Christian Gómez	IMPORTANT E	20	20	20	20
38	Luz Ochoa	IMPORTANT E	20	20	20	20
39	Davis Sánchez	IMPORTANT E	20	20	20	20

Nota. Elaborado por el autor del documento

Utilizando la metodología MAGERIT, se llevó a cabo un análisis evaluación de riesgos teniendo en cuenta la identificación minuciosa de los activos de información y las potenciales amenazas que podrían presentarse en la seguridad. El propósito principal fue identificar el costo de estos activos en caso de que los riesgos se materialicen.

3.12 Medidas de protección de activos de información.

Es crucial informar al Hospital Santa Teresita sobre el nivel de riesgo actual y como mitigarlo con salvaguardas siguiendo la norma ISO/IEC 27001:2013.

El Anexo 1 tiene 114 controles de seguridad para mejorar la seguridad de la información del departamento de TIC.

Es esencial aplicar estos controles para implementar el SGSI, aunque en algunos casos no serán aplicables todos.

Los controles cubren todos los aspectos, no solo ciberseguridad; en el Anexo 1 se detallan las 14 sesiones.

- A.5: Políticas de Seguridad de la Información: controla la redacción y revisión de políticas de seguridad.
- A.6: Organización de la Seguridad de la información: controles para establecer responsables de la seguridad de la información. También se enfoca en dispositivos móviles y teletrabajo.

- A.7: Seguridad de los Recursos Humanos: controles para procesos de contratación y finalización de personal.
- A.8: Gestión de Recursos: se establecen para realizar inventario, clasificación y manejo de almacenamiento.
- A.9: Control de Acceso: regular el acceso a la información y a las aplicaciones que la contienen.
- A.10: Criptografía: controles de encriptación de datos.
- A.11: Seguridad física y ambiental: Proteger factores externos que puedan comprometer la seguridad.
- A.12: Seguridad Operacional: controles de seguridad para proteger contra malware y vulnerabilidades.
- A.13: Seguridad de las comunicaciones: aborda la seguridad de las comunicaciones y el control de las redes, transmisiones y mensajería.
- A.14: Adquisición, desarrollo y mantenimiento de Sistemas: controles para seguridad en desarrollo y soporte de sistemas.
- A.15: Relaciones con los proveedores: gestión de contratos y seguimiento.
- A.16: Gestión de Incidentes en Seguridad de la Información: reportan eventos y debilidades, y establecen procedimientos de respuesta.
- A.17: Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio: se refieren a la planificación de continuidad.
- A.18: Cumplimiento: control para identificar y hacer cumplir las normas de seguridad de la información.

Se evaluaron 120 amenazas según el Libro II MAGERIT v3 para proponer salvaguardas, y se encontró que el departamento de TIC del Hospital Santa Teresita carece de suficientes controles.

El Anexo 2 muestra el tratamiento de riesgos según ISO 27001:2013.

A continuación, se presenta la tabla de medidas de protección activos de información.

Tabla 10.

Medidas de protección de los activos de información de tipo activo

No. De Amenazas y Vulnerabilidades	Activos de Información				Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual	Plan de Tratamiento								Requerimiento Legal	Obligación Contractual	Requerimiento de Negocio	Análisis de Riesgo	Exclusión	
	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades										Indique el control a aplicar a partir de la norma ISO 27001:2013	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control					
1	ACTIVO	Historias Clínicas	[A19]Divulgación de información	Revelación de las Historias Clínicas a terceros. Eliminación o pérdida de las Historias Clínicas.	1	2	44	C	1	No existe control ya que no se cuenta con procesos y procedimientos dedicados al manejo de historias clínicas	44	C		X				DOMINIO_A5	OBJETIVO_A5_1	A5.1.1 Políticas para la seguridad de la información, y la política de transferencia de información. Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y	Se debe definir la política de clasificación y manejo de la información, y la política de transferencia de información. Donde se establezca como se debe tratar la información de terceros, la clasificación de la información y el manejo de los tres pilares de la seguridad (disponibilidad, integridad y confidencialidad).	X		X	X	

[E18]Destrucción de información	I	2	44	C	1	44	C	X	DOMINIO_A5	OBJETIVO_A5_1	comunicad a a los empleados y a las partes externas pertinentes	X	X	X
											· A5.1.1 Políticas para la seguridad de la informació n -- Control: Se debe definir un conjunto de políticas para la seguridad de la informació n, aprobada por la dirección, publicada y comunicad a a los empleados y a las partes externas pertinentes			

2	ACTIVO	Base de datos Inventarios	[A19]Divulgación de información	1	3	75	C	1	75	C	X	Dominio_A5	Objetivo_A5_1	A5.1.1 Políticas para la seguridad de la información -- Control: Se debe definir un conjunto de políticas para la seguridad de la información, n, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes. A5.1.1 Políticas para la seguridad de la información -- Control: Se debe definir un conjunto de políticas para la	Se debe definir la política de clasificación y manejo de la información, y la política de transferencia de información. Donde se establezca como se debe tratar la información, la clasificación de la información y el manejo de los tres pilares de la seguridad (disponibilidad, integridad y confidencialidad). También se debe establecer un proceso desde el área de bodega donde se plasme los procedimientos del manejo de los comprobantes, los roles y responsabilidades de estas.	X	X	X
			Alteración en los registros de Inventarios. Eliminación de las comprobantes de ingreso/egresos					No existe control ya que no se cuenta con procesos y procedimientos dedicados a proteger la información de las bases de datos del inventario										
			[A15]Modificación deliberada de la información	1	3	75	C	1	75	C	X	Dominio_A5	Objetivo_A5_1			X	X	X

3	Base de datos pacientes	[A19]Divulgación de información	Revelación información confidencial e interna. Eliminación o perdida de información	I	4	100	C	1	No existe control ya que no se cuenta con procesos y procedimient os dedicado a proteger la información de las bases de datos de pacientes	100	C	X	DOMINIO_ A5	OBJETIVO_A5 _1	A5.1.1 Políticas para la seguridad de la información -- Control: Se debe definir un conjunto de políticas para la seguridad de la información, Se debe definir la política de clasificación y manejo de la información, y la política de transferencia de información. Donde se establezca como se debe tratar la información de terceros, la clasificación de la información y el manejo de los tres pilares de la seguridad (disponibilidad, integridad y confidencialidad). externas pertinentes	X	X	X
---	----------------------------	------------------------------------	---	---	---	-----	---	---	---	-----	---	---	----------------	-------------------	---	---	---	---

ACTIVO	[E18]Destrucción de información	1	4	100	C	1	100	C	X	Dominio_A5	Objetivo_A5_1	A5.1.1 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	X	X
	[A15]Modificación deliberada de la información	1	4	100	C	1	100	C	X	Dominio_A5	Objetivo_A5_1	A5.1.1 Políticas para la seguridad de la información -- Control: Se debe definir un conjunto de políticas para la	X	X	X

4	ACTIVO	Base de datos médicos	[A19]Divulgación de información	Revelación información confidencial e interna. Eliminación o pérdida de información	I	4	100	C	1	No existe control ya que no se cuenta con procesos y procedimientos dedicados a proteger la información de las bases de datos de médicos	100	C	X	DOMINIO_A5	OBJETIVO_A5_1	seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes pertinentes. A5.1.1 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 pertinentes. Se debe definir la política de clasificación y manejo de la información, y la política de transferencia de información. Donde se establezca como se debe tratar la información de terceros, la clasificación de la información y el manejo de los tres pilares de la seguridad (disponibilidad, integridad y confidencialidad).	X	X	X
---	--------	-----------------------	---------------------------------	--	---	---	-----	---	---	--	-----	---	---	------------	---------------	---	---	---	---

										externas pertinentes .														
										A5.1.1 Políticas para la seguridad de la informació n -- Control: Se debe definir un conjunto de políticas para la seguridad de la informació n, aprobada por la dirección, publicada y comunicad a a los empleados y a las partes externas pertinentes .														
[E18]Destrucció n de información										I	4	100	C	1		100	C	X	DOMINIO_ A5	OBJETIVO_ A5_1	X	X	X	
ACTIV O	[A15]Modificaci ón deliberada de la información									I	4	100	C	1		100	C	X	DOMINIO_ A5	OBJETIVO_ A5_1	A5.1.1 Políticas para la seguridad de la informació n -- Control: Se debe	X	X	X

										comunicad a a los empleados y a las partes externas pertinentes . A5.1.1 Políticas para la seguridad de la informació n -- Control: Se debe definir un conjunto de políticas para la seguridad de la informació n, aprobada por la dirección, publicada y comunicad a a los empleados y a las partes externas pertinentes .				
ACTIV O	[E18]Destrucció n de información	I	4	100	C	1	100	C	X	DOMINIO_ A5	OBJETIVO_A5 _1	X	X	X

[A15]Modificaci ón deliberada de la información				I	4	100	C	1	100	C	X	DOMINIO_ A5	OBJETIVO_ A5_1	A5.1.1 Políticas para la seguridad de la informació n -- Control: Se debe definir un conjunto de políticas para la seguridad de la informació n, aprobada por la dirección, publicada y comunicad a a los empleados y a las partes externas pertinentes	X	X	X
---	--	--	--	---	---	-----	---	---	-----	---	---	----------------	-------------------	--	---	---	---

Nota. Elaborado por el autor del documento.

Como se puede visualizar la Tabla 7 se relacionan con el dominio “A_5 Política para la seguridad de la información” y “el control A.5.1.1 Política para la seguridad de la información” en las medidas de protección de tipo Activo.

Tabla 11.

Medidas de protección de los activos de información de tipo datos.

No. De Amenazas y Vulnerabilidades	Activos de Información				Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Críticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Críticidad residual	Plan de Tratamiento								Requerimiento Legal	Obligación Contractual	Requerimiento de Negocio	Análisis de Riesgo	Exclusión	
	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Indique el control a aplicar a partir de la norma ISO 27001:2013																						
	Transferir	Aceptar	Eliminar	Mitigar									DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control										
6	DATOS	Copias de seguridad	[E2]Errores del administrador	Equivocación en la operación de Backup. Alteración o pérdida de la información.	I	4	100	C	1	No existe control ya que no se cuenta con procesos y procedimientos dedicados a proteger la información.	100	C			X	DOMINIO_A12	OBJETIVO_A12_3	A12.3.1 Respaldo de la información --Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a	Se debe definir la política de copia de respaldo, para contar con un estándar relacionando, la periodicidad, los responsables, de las copias y	X		X	X			

[E18]Destrucción de información	I	4	100	C	1	100	C	X	DOMINIO_A12	OBJETIVO_A12_3	prueba regularment e de acuerdo con una política de copias de respaldo acordadas.	clasificación , definir los servicios que requieren copia de seguridad.	
											A12.3.1 Respaldo de la información --Control: Se deben hacer copias de respaldo de la información , software e imágenes de los sistemas, y ponerlas a prueba regularment e de acuerdo con una política de copias de respaldo acordadas.		

Nota. Elaborado por el autor del documento.

Como se puede visualizar la Tabla 8 se relacionan con el dominio “A_12 Seguridad de las operaciones y el control A.12.3.1 Respaldo de información” en las medidas de protección de tipo Datos.

Tabla 12.

Medidas de protección de los activos de información de tipo servicios.

No. De Amenazas y Vulnerabilidades	Activos de Información				Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Críticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Críticidad residual	Plan de Tratamiento										Requerimiento Legal	Obligación Contractual	Requerimiento de Negocio	Análisis de Riesgo	Exclusión
	Nombre del activo de información	Amenazas Metodología Magerit												Indique el control a aplicar a partir de la norma ISO 27001:2013														
	Transferir	Aceptar	Eliminar	Mitigar										DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control											
7	SERVICIOS	Servidor de Correo	[E.1]Errores de los usuarios	Inadecuado uso de los privilegios de acceso, para provecho de fraude. Alteración accidental o intencional del servicio. Sobrecarga de los servicios	I	4	100	C	1	No existe control ya que no se cuenta con procesos y procedimientos dedicados a proteger la información.	100	C		X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.2 Suministro de acceso de usuarios -- Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para	Se debe implementar un proceso relacionado con la asignación y revocación de accesos a los sistemas de aplicación	X		X	X						

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

[A.11] Acceso no autorizado	I	4	100	C	1	100	C	X	DOMINIO_A9	OBJETIVO_A9_4	requerido del sistema.				
											A9.4.5 Control de acceso a códigos fuente de programas -- Control: Se debe restringir el acceso a los códigos fuente de los programas.	Se debe definir la política de control de acceso, relacionando quienes están autorizados y quienes no al código fuente de las aplicaciones, versión y verificación de errores	X	X	X
											A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Se debe definir la política de confidencialidad de la información que garantice la protección y el manejo óptimo de los activos			
[A15] Modificación deliberada de la información	I	4	100	C	1	100	C	X	DOMINIO_A8	OBJETIVO_A8_2		X	X	X	

8	SERVICIOS	Servidor de Archivos	[A.6]Abuso de privilegios de acceso	I	4	100	C	1		100	C	X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.5 Revisión de los derechos de acceso de usuarios -- Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Cada uno de los responsables de los activos debe validar que los permisos sean acordes a las funciones, asegurando que no se tiene privilegios no autorizados.	X	X	X
			[A.7]Uso no previsto	I	4	100	C	1	No existe control ya que no se cuenta con procesos y procedimientos dedicados a proteger la información.	100	C	X	DOMINIO_A8	OBJETIVO_A8_2	A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Se debe definir la política de confidencialidad de la información que garantice la protección y el manejo óptimo de los activos	X	X	X
			[A.11]Acceso no autorizado	I	4	100	C	1		100	C	X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.5 Control de acceso a códigos fuente de programas -- Control: Se debe	Se debe definir la política de control de acceso, relacionando quienes están autorizados y	X	X	X

[A15]Modificaci ón deliberada de la información	I	4	100	C	1	100	C	X	DOMINIO_A 8	OBJETIVO_A8 _2	restringir el acceso a los códigos fuente de los programas.	quienes no al código fuente de las aplicaciones, versión y verificación de errores	X	X	X
											A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar procedimient os para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización .	Se debe definir la política de confidencialid ad de la información que garantice la protección y el manejo óptimo de los activos			
											A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar procedimient os para el manejo de activos, de acuerdo con el esquema de clasificación de información	Se debe definir la política de confidencialid ad de la información que garantice la protección y el manejo óptimo de los activos			
[A18]Destrucci ón de información	I	4	100	C	1	100	C	X	DOMINIO_A 8	OBJETIVO_A8 _2			X	X	X

9	SERVICIO	Servidor Local	[E2]Errores del administrador	I	4	100	C	1	100	C	X	DOMINIO_A 9	OBJETIVO_A9 _4	adoptado por la organización .	X	X	X
														A9.4.1 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.			
														Establecer roles y perfiles de acceso de acuerdo con las funciones del cargo teniendo en cuenta el cumplimiento de la confidencialidad			
														No existe control ya que no se cuenta con procesos y procedimientos dedicados a proteger la información.			
	SERVICIO	Servidor Local	[A15]Modificación deliberada de la información	I	4	100	C	1	100	C	X	DOMINIO_A 8	OBJETIVO_A8 _2	A8.2.3 Manejo de activos --Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la	X	X	X
														Se debe definir la política de confidencialidad de la información que garantice la protección y el manejo óptimo de los activos			

[A18]Destrucción de información	I	4	100	C	1	organización							
						A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización	Se debe definir la política de confidencialidad de la información que garantice la protección y el manejo óptimo de los activos	X	X	X			

Nota. Elaborado por el autor del documento.

Como se puede visualizar la Tabla 9 se relacionan con el dominio “A_9 Control de acceso con el control A.9.2.2 Suministro de acceso de usuarios y A.9.4.1 Restricciones de acceso a la información, dominio A_8 Gestión de activos y el control A.8.2.3 Manejo de activos y el dominio A_12 Seguridad de las operaciones con el control A.12.1.3 Gestión de capacidad de los activos de información tipo servicios” en las medidas de protección de tipo Servicios.

Tabla 13.

Medidas de protección de los activos de información de tipo hardware.

No. De Amenazas y Vulnerabilidades						Niveles de aceptación del riesgo		Probabilidad de vulneración		Cálculo del riesgo neto		Críticidad neta		Calificación de Gestión		Si la opción es 2 - 3 o 4 Indique el Control aplicado actual		Riesgo residual		Críticidad residual		Plan de Tratamiento										Requerimiento Legal		Obligación Contractual		Requerimiento de Negocio		Análisis de Riesgo		Exclusión	
Activos de Información		Nombre del activo de información		Amenazas Metodología Magerit		Vulnerabilidades																Indique el control a aplicar a partir de la norma ISO 27001:2013																			

[N2]Daños por agua	I	3	45	C	1	45	C	X	DOMINIO_A11	OBJETIVO_A11_1	accidentes				
											A11.1.4 Protección contra amenazas externas y ambiental es. -- Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes	Para protección de los activos se debe contar con el conocimien to pertinente para el manejo de los daños causados por el recurso humano o por desastres naturales.			
													X	X	X

[I.3]Contaminación mecánica	I	3	45	C	1	45	C	X	DOMINIO _A11	OBJETIVO_ A11_1	A11.1.4 Protección contra amenazas externas y ambiental es. -- Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes	Para protección de los activos se debe contar con el conocimien to pertinente para el manejo de los daños causados por el recurso humano o por desastres naturales.	X	X	X
											.				
[I.5]Avería de origen físico o lógico	I	3	45	C	1	45	C	X	DOMINIO _A11	OBJETIVO_ A11_1	A11.1.4 Protección contra amenazas externas y ambiental es. -- Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques	Para protección de los activos se debe contar con el conocimien to pertinente para el manejo de los daños causados por el recurso humano o por	X	X	X

[I.6]Corte de suministro electrico	I	3	45	C	1	45	C	X	DOMINIO _A11	OBJETIVO_ A11_2	maliciosos o accidentes .	desastres naturales.			
											A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupci ones causadas por fallas en los servicios de suministro .	Se debe asegurar y garantizar el servicio de potencia para los equipos de computo	X	X	X

[I.7]Condiciones inadecuadas de temperatura o humedad	I	3	45	C	1	45	C	X	DOMINIO _A11	OBJETIVO_ A11_1	A11.1.4 Protección contra amenazas externas y ambiental es. -- Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes	Para protección de los activos se debe contar con el conocimien to pertinente para el manejo de los daños causados por el recurso humano o por desastres naturales.	X	X	X
											.	.			
[E.23]Errores de mantenimiento/actualización de equipo	I	3	45	C	1	45	C	X	DOMINIO _A11	OBJETIVO_ A11_2	A11.2.4 Mantenim iento de los equipos. -- Control: Los equipos se deben mantener correctam ente para asegurar su disponibili dad e	Implementa r lineamiento s para el mantenimie nto de equipos establecien do la periodicida d, especificaci ones del servicio siendo este registrado en bitácoras	X	X	X

										autorizado			

Router HP	Robo. Falta de mantenimiento					ente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.						Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	s apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.							
[N2]Daños por agua		I	3	48	C	1	48	C		X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X		X	X		
[I.3]Contaminación mecánica		I	3	48	C	1	48	C		X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.8 Equipos de usuario desatendidos	Se debe aclarar y concientizar a los	X		X	X		

[I.5]Avería de origen físico o lógico	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	o -- usuarios los			
											Control: lineamiento			
Los s														
usuarios apropiados														
deben para el														
asegurarse manejo de														
de que a los equipos														
los cumpliendo														
equipos con la														
desatendid confianza														
os se les lidad,														
da integridad y														
protección disponibilid														
apropiada. ad de la														
informació														
n.														
A11.2.8 aclarar y														
Equipos concientiza														
de usuario r a los														
desatendid usuarios los														
o -- lineamiento														
Control: s														
Los apropiados														
usuarios para el														
deben manejo de														
asegurarse los equipos														
de que a cumpliendo														
los con la														
equipos confianza														
desatendid lidad,														
os se les integridad y														
da disponibilid														
protección ad de la														
apropiada. informació														
n.														

[I.6]Corte de suministro electrico	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	A11.2.8 Equipos de usuario desatendid o -- Control: Los usuarios deben asegurarse de que a los equipos desatendid os se les da protecció n apropiada.	Se debe aclarar y concientiza r a los usuarios los lineamiento s apropiados para el manejo de los equipos cumpliendo con la confidencia lidad, integridad y disponibilid ad de la informació n.	X	X	X
											A11.2.8 Equipos de usuario desatendid o -- Control: Los usuarios deben asegurarse de que a los equipos desatendid os se les da protecció n apropiada.	Se debe aclarar y concientiza r a los usuarios los lineamiento s apropiados para el manejo de los equipos cumpliendo con la confidencia lidad, integridad y disponibilid ad de la	X	X	X
[I.7]Condiciones inadecuadas de temperatura o humedad	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	A11.2.8 Equipos de usuario desatendid o -- Control: Los usuarios deben asegurarse de que a los equipos desatendid os se les da protecció n apropiada.	Se debe aclarar y concientiza r a los usuarios los lineamiento s apropiados para el manejo de los equipos cumpliendo con la confidencia lidad, integridad y disponibilid ad de la	X	X	X
											A11.2.8 Equipos de usuario desatendid o -- Control: Los usuarios deben asegurarse de que a los equipos desatendid os se les da protecció n apropiada.	Se debe aclarar y concientiza r a los usuarios los lineamiento s apropiados para el manejo de los equipos cumpliendo con la confidencia lidad, integridad y disponibilid ad de la	X	X	X

[E.23]Errores de mantenimiento/actualización de equipo	I	3	48	C	1	48	C	X	DOMINIO_A11	OBJETIVO_A11_2	información.			
											Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
[E.25]Pérdida de equipos	I	3	48	C	1	48	C	X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.			
											Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad.	X	X	X

														os se les da integridad y protección apropiada. disponibilidad de la información.				
														A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da integridad y protección apropiada. Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.				
[A.23]Manipulación de los equipos				I	3	48	C	1	48	C	X	DOMINIO_A11	OBJETIVO_A11_2	X	X	X		

'12	HARDWARE	Switch Cisco Switch HP (3)	[N1] Fuego	Desastres naturales. Exceso de frío o calor. Fallo eléctrico. Robo. Falta de mantenimiento	I	3	45	C	1	45	C	X	DOMINIO_A11	OBJETIVO_A11_2	X	X	X
				Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la						A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los		Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo					

[N2]Daños por agua	I	3	48	C	1	información no son los adecuados.	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	equipos con la desatendid confidencia os se les lidad, da integridad y protección disponibilid apropiada. ad de la informació n.			
												A11.2.8 Se debe Equipos aclarar y de usuario concientiza desatendid r a los o -- usuarios los Control: lineamiento Los s usuarios apropiados deben para el asegurarse manejo de los equipos cumpliendo con la confidencia lidad, integridad y disponibilid ad de la informació n.	X	X	X
												A11.2.8 Se debe Equipos aclarar y de usuario concientiza desatendid r a los o -- usuarios los Control: lineamiento Los s usuarios apropiados deben para el asegurarse manejo de	X	X	X
[I.3]Contaminación mecánica	I	3	48	C	1		48	C	X	DOMINIO _A11	OBJETIVO_ A11_2				

[I.5]Avería de origen físico o lógico	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	de que a los equipos desatendidos se les da protección apropiada.	los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.			
											A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
[I.6]Corte de suministro eléctrico	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados	X	X	X

[I.7]Condiciones inadecuadas de temperatura o humedad	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	deben para el asegurarse manejo de de que a los equipos los cumpliendo equipos con la desatendid confianza os se les lidad, da integridad y protección disponibilid apropiada. ad de la informació n.			
											A11.2.8 Se debe Equipos aclarar y de usuario concientiza desatendid r a los o -- usuarios los Control: lineamiento Los s usuarios apropiados deben para el asegurarse manejo de de que a los equipos los cumpliendo equipos con la desatendid confianza os se les lidad, da integridad y protección disponibilid apropiada. ad de la informació n.	X	X	X
											A11.2.8 Se debe Equipos aclarar y de usuario concientiza desatendid r a los o -- usuarios los Control: lineamiento	X	X	X
[E.23]Errores de mantenimiento/actualización de equipo	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2				

[E.25]Perdida de equipos	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Los usuarios apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.			
											A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
											A11.2.8 Equipos de usuario desatendidos	Se debe aclarar y concientizar a los	X	X	X
[A.23]Manipulación de los equipos	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2					

[N2]Daños por agua	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
											A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la	X	X	X
[I.3]Contaminación mecánica	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la	X	X	X

[I.5]Avería de origen físico o lógico	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	información.			
											Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
[I.6]Corte de suministro eléctrico	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.			
											Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad.	X	X	X

[I.7]Condiciones inadecuadas de temperatura o humedad	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	os se les da integridad y protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.			
											A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da integridad y protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
											A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo	X	X	X
[E.23]Errores de mantenimiento/actualización de equipo	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo	X	X	X

[E.25]Perdida de equipos	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2	equipos con la desatendid confidencia os se les lidad, da integridad y protección disponibilid apropiada. ad de la informació n.			
											A11.2.8 Se debe Equipos aclarar y de usuario concientiza desatendid r a los o -- usuarios los Control: lineamiento Los s usuarios apropiados deben para el asegurarse manejo de de que a los equipos los cumpliendo equipos con la desatendid confidencia os se les lidad, da integridad y protección disponibilid apropiada. ad de la informació n.	X	X	X
											A11.2.8 Se debe Equipos aclarar y de usuario concientiza desatendid r a los o -- usuarios los Control: lineamiento Los s usuarios apropiados deben para el asegurarse manejo de	X	X	X
[A.23]Manipulació n de los equipos	I	3	48	C	1	48	C	X	DOMINIO _A11	OBJETIVO_ A11_2				

[A.23]Manipulación de los equipos	I	2	22	C	1	22	C	X	DOMINIO_A11	OBJETIVO_A11_2	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Los usuarios apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.			
											A11.2.8 Equipos de usuario desatendidos o -- Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X

Nota. Elaborado por el autor del documento

Como se puede visualizar la Tabla 10 se relacionan con el dominio “A_11 Seguridad física y del entorno con los controles A.11.1.4 Protección contra amenazas externas y ambientales y A.11.2.8 Equipos de usuarios” en las medidas de protección de tipo Hardware.

Tabla 14.

Medidas de protección de los activos de información de tipo comunicaciones.

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual	Plan de Tratamiento										Requerimiento Legal	Obligación Contractual	Requerimiento de Negocio	Análisis de Riesgo	Exclusión
													Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control							
15	COMUNICACIONES	Internet	[A14] Interceptación de información (escucha)	Acceso no autorizado a la información sin alteración. Análisis de tráfico por intrusos. Alteración en el orden de la transmisión de mensajes.	I	3	75	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	75	C				X	DOMINIO_A13	OBJETIVO_A13_2	A13.2.1 Políticas y procedimientos de transferencia de información -Control: Se debe contar con políticas, procedimientos y controles de	Establecer la política de transferencia de información, garantizando la confidencialidad y disponibilidad de la información	X		X	X			

[A12] Análisis de trafico	I	3	75	C	1	75	C	X	DOMINIO_ A12	OBJETIVO_A1 2_4	transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicacio nes.							
											A12.4.1 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.				Establecer un correcto manejo al registro de eventos relacionando almacenamien to y consulta de los eventos	X	X	X
[A10] Alteración de secuencia	I	3	75	C	1	75	C	X	DOMINIO_ A8	OBJETIVO_A8 _2	A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar procedimient os para el manejo de activos, de acuerdo con	Se debe definir la política de confidencialid ad de la información que garantice la protección y el manejo óptimo de los activos	X	X	X			

[illegible]

[A10] Alteración de secuencia	I	3	75	C	1	75	C	X	DOMINIO_ A8	OBJETIVO_ A8_2	los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	
											A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización. Se debe definir la política de confidencialidad de la información que garantice la protección y el manejo óptimo de los activos	
												X X X

Nota. Elaborado por el autor del documento.

Como se puede visualizar la Tabla 11 se relacionan con el dominio “A_13 Seguridad de las comunicaciones y el control A.13.2.1 Políticas y procedimientos de transferencia de información” en las medidas de protección de tipo Comunicaciones.

Tabla 15.

Medidas de protección de los activos de información de tipo auxiliar.

No. De Amenazas y Vulnerabilidades		Activos de Información				Amenazas Metodología Magerit		Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual	Plan de Tratamiento										Requerimiento Legal	Obligación Contractual	Requerimiento de Negocio	Análisis de Riesgo	Exclusión
Indique el control a aplicar a partir de la norma ISO 27001:2013																	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control							
17	AUXILIAR	Rack de datos	[A7] Uso no previsto	Uso no adecuado para otros fines. Robo. Falta de mantenimiento. Falta de servicios dependientes de otros.	I	1	25	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	25	C				X	DOMINIO_A8	OBJETIVO_A8_2	A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Se debe definir la política de confidencialidad de la información que garantice la protección y el manejo óptimo de los activos	X		X	X							

[E25] Pérdida de equipos	I	1	25	C	1	25	C	X	DOMINIO_ A11	OBJETIVO_A1 1_2	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
[E23] Errores de mantenimiento/actualización de equipos	I	1	25	C	1	25	C	X	DOMINIO_ A11	OBJETIVO_A1 1_2	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
[I.9] Interrupción de otros servicios y suministro esenciales	I	1	25	C	1	25	C	X	DOMINIO_ A11	OBJETIVO_A1 1_2	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los	X	X	X

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

				[I.9] Interrupcion de otros servicios y suministro esenciales	I	2	30	C	1	30	C	X	DOMINIO_A11	OBJETIVO_A11_2	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
				[I.7] Condiciones inadecuadas de temperatura o humedad	I	2	30	C	1	30	C	X	DOMINIO_A11	OBJETIVO_A11_2	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
19	AUXILIAR	Cableado	[A7] Uso no previsto	Uso no adecuado para otros fines. Robo. Falta de mantenimiento. Falta de servicios dependientes de otros.	I	2	40	C	1	40	C	X	DOMINIO_A8	OBJETIVO_A8_2	A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar procedimientos para el	Se debe definir la política de confidencialidad de la información que garantice la protección y el manejo	X	X	X

[E25] Pérdida de equipos	I	2	40	C	1	40	C	X	DOMINIO_ A11	OBJETIVO_A1 1_2	manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	óptimo de los activos			
											A11.2.8 Equipos de usuario desatendido --Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.	X	X	X
											A11.2.8 Equipos de usuario desatendido --Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y	X	X	X
[E23] Errores de mantenimiento/actualización de equipos	I	2	40	C	1	40	C	X	DOMINIO_ A11	OBJETIVO_A1 1_2					

[illegible]

Nota. Elaborado por el autor del documento.

Como se puede visualizar la Tabla 12 se relacionan con el dominio “A_8 Gestión de los activos y como control el A.8.2.3 Manejo de activos para la definición de procesos y políticas que garanticen la protección y manejo de los activos de información” en las medidas de protección de tipo Auxiliar.

Tabla 16.

Medidas de protección de los activos de información de tipo instalaciones.

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Críticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Críticidad residual	Plan de Tratamiento										Requerimiento Legal	Obligación Contractual	Requerimiento de Negocio	Análisis de Riesgo	Exclusión
													Indique el control a aplicar a partir de la norma ISO 27001:2013														
													Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control							
20	INSTALACIONES	Oficina TIC Oficina Gerencia Distrital Oficina Gerencia Hospital Oficina Estadística	[N1]Fuego	Desastres naturales. Acceso no autorizado, provocando fuga, alteración y/o eliminación de la información. Vandalismo	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C			X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.8 Equipos de usuario desatendido --Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad	X	X	X					

																		y disponibilidad de la información.		
																		Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.		
[N2]Daños por agua	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C	X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.8 Equipos de usuario desatendido –Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.						X	X	X
[N.*]Desastres naturales	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C	X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.8 Equipos de usuario desatendido –Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.						X	X	X

[E15]Alteración accidental de la información	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C	X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.2 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.	Se debe proteger las áreas de información sensible implementando un sistema de control físico.	X	X	X
	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C	X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.2 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.	Se debe proteger las áreas de información sensible implementando un sistema de control físico.	X	X	X
	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C	X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.5 Trabajo en áreas seguras. -- Control: Se	Se debe contar con protección en las zonas seguras	X	X	X

[A18]Destrucción de información	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C		X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.5 Trabajo en áreas seguras. -- Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Se debe contar con protección en las zonas seguras implementando o procedimientos de seguridad desde la información almacenada y tratada como sensible.	X		X	X
	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C		X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.5 Trabajo en áreas seguras. -- Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Se debe contar con protección en las zonas seguras implementando o procedimientos de seguridad desde la información almacenada y tratada como sensible.	X		X	X
	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C		X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.5 Trabajo en áreas seguras. -- Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Se debe contar con protección en las zonas seguras implementando o procedimientos de seguridad desde la información almacenada y tratada como sensible.	X		X	X
	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C		X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.4 Protección contra amenazas externas y	Para protección de los activos se debe contar con el	X		X	X

[A27]Ocupación enemiga					adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.						ambientales. --Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	conocimiento pertinente para el manejo de los daños causados por el recurso humano o por desastres naturales.	
	I	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C	X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.3 Seguridad de oficinas, recintos e instalaciones. --Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones. Debido a la información que se maneja es importante tomar medidas de protección a las oficinas e instalaciones de la institución	X X X

Nota. Elaborado por el autor del documento.

Como se puede visualizar la Tabla 13 se relacionan con el dominio “A_11 Seguridad física y el entorno con el control A.11.2.8 Equipos de usuarios desatendido” en las medidas de protección de tipo Instalaciones.

Tabla 17.

Medidas de protección de los activos de información de tipo personal.

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Críticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Críticidad residual	Plan de Tratamiento										Requerimiento Legal	Obligación Contractual	Requerimiento de Negocio	Análisis de Riesgo	Exclusión
													Indique el control a aplicar a partir de la norma ISO 27001:2013														
													Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control							
21	PERSONAL	Total 6 personas Laura Sánchez Raúl Aguirre Margarita Torres Christian Gómez Luz Ochoa Davis Sánchez	[A29] Extorsión	Fuga de información. Amenazas. La no definición de roles y funciones. Absentismo laboral, huelgas, entre otros	1	3	60	C	1	Existe un control que no se implementa de adecuadamente, los procesos y procedimientos dedicados a proteger la información no son los adecuados.	60	C			X	DOMINIO_A13	OBJETIVO_A13_2	A13.2.4 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	Para asegurar la información se debe definir un acuerdo de confidencialidad a nivel interno para los empleados	X		X	X				

[A28] Indisponibilidad del personal	I	3	60	C	1	60	C	X	DOMINIO_A7	OBJETIVO_A7_1	protección de la información.				
											A7.1.2 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.	Se debe asegurar que todos los empleados acepten y cumplan las condiciones relacionadas con su cargo y seguridad de la información.	X	X	X
											A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Se debe definir la política de confidencialidad de la información que garantice la protección y el manejo óptimo de los activos	X	X	X
[E19] Fuga de información	I	3	60	C	1	60	C	X	DOMINIO_A8	OBJETIVO_A8_2					
[E17] Definición en la organización	I	3	60	C	1	60	C	X	DOMINIO_A8	OBJETIVO_A8_2	A8.2.3 Manejo de activos -- Control: Se deben desarrollar e implementar	Se debe definir la política de confidencialidad de la información	X	X	X

				procedimiento s para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	que garantice la protección y el manejo óptimo de los activos	
--	--	--	--	--	---	--

Nota. Elaborado por el autor del documento.

Como se puede visualizar la Tabla 14 se relacionan con el dominio “A_13 Seguridad de las comunicaciones y el control A.13.2.4 Acuerdos de confidencialidad o de no divulgación” en las medidas de protección de tipo Personal.

Tabla 18.

Resumen de medidas de protección a aplicar a las amenazas identificadas.

Salvaguardas por Dominio	Total Vulnerabilidades a aplicar
Dominio_A5 Políticas de seguridad de la información	14
Dominio_A7 Seguridad de los recursos humanos	1
Dominio_A8 Gestión de activos	13
Dominio_A9 Control de acceso	6
Dominio_A11 Seguridad física y del entorno	63
Dominio_A12 Seguridad de las operaciones	5
Dominio_A13 Seguridad de las comunicaciones	3
Total: 105 medidas de protección	

Nota. Elaborado por el autor del documento.

La tabla resume las medidas de protección de las amenazas identificadas en el departamento de TIC del Hospital Santa Teresita.

Se establecen medidas de protección según la norma ISO 27001:2013 para proteger los activos de información del departamento de TIC del Hospital Santa Teresita.

3.13 Políticas de seguridad de la información.

Después de haber identificado los activos de información, evaluado los riesgos asociados y definido las medidas de protección de acuerdo con el Anexo 1 de la norma ISO 27001:2013, se elaboran las políticas de seguridad de la información asegurándose de seguir las mejores prácticas y estándares establecidos en la norma ISO 27001:2013 para garantizar una gestión segura de la información.

Es imprescindible establecer políticas de seguridad específicas para el departamento de TIC del Hospital Santa Teresita, ya que carece de procedimientos formales y directrices para gestionar de forma correcta los activos de información. Además, es necesario contar con directrices claras sobre las mejores prácticas en materia de seguridad que el departamento debe seguir y cumplir, con el fin de asegurar que se aborden y reduzcan los riesgos de seguridad y asegurar la información del hospital.

Las políticas de seguridad se crean a partir de los controles indicados en el Anexo 1 de la norma ISO 27001:2013, que sirve como marco de referencia para seguir las prácticas recomendadas por la norma. Estas políticas son una herramienta valiosa para el departamento de Tecnología de la Información (TI), ya que establecen los requisitos que deben cumplirse en relación con los activos de información de la institución. Además, permiten identificar qué aspectos deben ser implementados o fortalecidos, y son compartidas con todos los empleados y proveedores de la institución.

Destaca la importancia de mencionar que las políticas de seguridad proporcionan directrices generales que sirven como punto de referencia para llevar a cabo procedimientos específicos adaptados a los procesos individuales.

Las políticas se encuentran claramente establecidas en dos documentos oficiales que han sido redactados con el propósito de brindar una guía específica y detallada sobre las normas y directrices a seguir.

Anexo 3. La Política de Seguridad de la Información dirigida a todos los empleados se enfoca en detallar cómo se deben cumplir y seguir las políticas y directrices de seguridad en toda la organización.

Anexo 4. Política de Seguridad para Empleados con Tareas y Responsabilidades Técnicas. Esta política detalla los lineamientos basados en la norma ISO 27001:2013 que deben seguirse, incluyendo controles sobre activos, accesos, seguridad, incidentes y cumplimiento.

3.14 Política de seguridad de la información para los empleados.

Política de uso permitido

- Los activos entregados por Hospital Santa Teresita deben usarse únicamente con fines laborales.
- El software debe ser utilizado solo para fines autorizados y no debe ser copiado, distribuido, instalado o eliminado sin permiso del departamento de TIC. Solo se instalará software aprobado por el Ministerio de Salud y el Hospital Santa Teresita en los dispositivos.
- Los datos deben usarse según lo autorizado, no se pueden modificar ni eliminar sin permiso.
- Los controles de seguridad relacionados con el uso de internet y correo electrónico, que han sido establecidos por el departamento de TIC, permanecerán invariables y no serán sujetos a modificaciones ni intentos por evadirlos.

- Los empleados deben interactuar de forma segura con la tecnología para evitar ataques de phishing. No compartir su contraseña de dominio en sitios web externos y tener cuidado al hacer clic en enlaces o descargar archivos adjuntos.
- No reenviar correos institucionales a cuentas personales.
- Los empleados no pueden reenviar automáticamente correos a otras cuentas.
- Los empleados deben cumplir con estándares de contraseña y manejar los datos confidenciales adecuadamente al usar dispositivos personales para acceder a la red del Hospital.
- Los empleados usarán el servidor de archivos para hacer copias de seguridad de datos. No se permiten copias de seguridad en dispositivos de almacenamiento personal o cuentas en la nube.
- Los empleados que deban usar medios extraíbles personales pueden pedir una excepción y esperar su aprobación.
- Los empleados deben informar los eventos/incidentes o cualquier evento sospechoso de seguridad al departamento de seguridad.
- Los empleados que necesiten conectarse de forma remota deberán usar VPN para trabajar de forma segura desde cualquier lugar.
- Los dispositivos de Hospital Santa Teresita no deben ser llevados por los empleados en viajes personales.
- Los empleados deben obtener aprobación escrita de la alta gerencia antes de llevar activos de trabajo fuera de la ciudad por motivos laborales.

Gestión de contraseñas

- Las contraseñas deben ser complejas. Las contraseñas deben tener un mínimo de ocho (8) caracteres de longitud y debe incluir caracteres especiales, mayúsculas, minúsculas y números.
- Las contraseñas deben actualizarse cada 90 días.
- Las contraseñas no deben incluir información personal o laboral del usuario.
- Las contraseñas no deben anotarse ni almacenarse electrónicamente en un archivo.
- Las contraseñas se guardan solo en aplicaciones de gestión de contraseñas aprobadas por el departamento de TIC.
- Las contraseñas son privadas e intransferibles y no se deben compartir.

Capacitación

La capacitación en seguridad ayuda a los empleados a identificar y evaluar las amenazas diarias. Cada usuario debe ser competente en la gestión del riesgo de la información para que la institución tenga éxito en sus operaciones.

- Todos los empleados deben completar la capacitación de seguridad en las fechas establecidas.
- La capacitación en seguridad comenzará pronto después de ser contratados. Se llevarán a cabo actividades de concientización y capacitación de forma constante para mantener un nivel estable de conciencia.
- El Hospital Santa Teresita debe proporcionar a los empleados información sobre la ubicación de los materiales de capacitación y políticas de seguridad.

3.15 Política de seguridad de la información a empleados con funciones y responsabilidades técnicas.

Manejo de Datos y Activos

- Establecer una política de control de acceso restringido.
- Encriptar datos en redes de transmisión.
- Evitar enviar información restringida y confidencial por mensajes instantáneos o Chat estarán prohibidos y se consideran una su falta grave de seguridad.
- La información confidencial no se puede almacenar en almacenamiento expandible.
- Los requisitos para el almacenamiento expandible deben aprobarse a través de solicitud de excepción y, si es aprobado, se debe usar encriptación.
- La copia de seguridad de la información restringida y confidencial debe estar encriptada.
- Eliminar de forma segura los sistemas y medios que contengan información restringida o confidencial.

Gestión de activos.

Es imperativo establecer y mantener un sistema de gestión de activos que permita la identificación de todos los dispositivos pertenecientes Hospital Santa Teresita.

Después de Realizar la compra o recibir una donación de equipamiento informático para usuarios finales, es necesario ingresar estos elementos en la base de datos correspondiente de gestión de activos. Se les deberá asignar la información mínima necesaria para su registro, que incluye el número de serie, el número de orden de compra, el número de factura, la fecha de

adquisición, la titularidad, el estado actual, la ubicación, el número de modelo y el identificador de etiqueta de activo.

3.16 Control de acceso.

Procedimiento de control de acceso

Desarrollar un documento detallado que establezca un protocolo de seguridad para regular el acceso a cada aplicación o sistema, detallando las medidas para mitigar los riesgos asociados con la gestión de las cuentas de usuario, el control de acceso, la aplicación y el cumplimiento de normas de separación de funciones, así como el acceso remoto.

Es importante tener en cuenta varios aspectos en relación a la seguridad del sistema o aplicación, como los requisitos de seguridad existentes, el tipo de datos que se almacenan en ellos, las obligaciones legales o contractuales sobre la restricción de accesos, la gestión de derechos y roles de control de acceso, la necesidad de autorizaciones formales para solicitudes de acceso y revisiones periódicas, la revocación de accesos, la identificación de roles con privilegios, así como la importancia de mantener un registro detallado de todas las actividades relevantes relacionadas con la gestión de identidades y niveles de autenticación.

Acceso de usuarios

- Implementar autenticación multifactor (MFA) para acceder a sistemas críticos.
- Requerir contraseñas fuertes, cambiarlas regularmente y evitar el uso de las mismas contraseñas en múltiples sistemas.
- Realizar revisiones periódicas para asegurar que los privilegios de acceso sean adecuados y necesarios.

- Otorgar el nivel mínimo de acceso necesario para que los empleados realicen sus tareas.
- Revisar y ajustar los privilegios de acceso regularmente.

Cuentas de identificaciones a usuarios

- Establecer procedimientos formales para la solicitud, aprobación y creación de cuentas de usuario.
- Asignar identificadores únicos a cada usuario para asegurar la individualidad de cada cuenta.
- Definir y asignar roles y privilegios apropiados según las funciones del usuario.
- Desactivar inmediatamente las cuentas de usuarios que ya no están autorizados (por ejemplo, empleados que dejan la institución).
- Retener cuentas desactivadas por un período determinado antes de eliminarlas permanentemente, según las políticas de retención de datos.
- Realizar auditorías periódicas de las cuentas de usuario para verificar la necesidad continua y la adecuación de los privilegios asignados.

Cuentas de identificaciones a sistemas

- Implementar un procedimiento formal para la creación de cuentas de sistema, que requiera la aprobación de un superior o administrador de sistemas.
- Asignar identificadores de usuario únicos para cada cuenta de sistema para asegurar la trazabilidad.
- Definir y asignar roles y permisos específicos basados en las necesidades del usuario y sus responsabilidades laborales.

- Llevar a cabo auditorías regulares para verificar el cumplimiento de las políticas de cuentas de sistemas.
- Desactivar inmediatamente las cuentas de usuarios que ya no necesiten acceso al sistema (por ejemplo, al finalizar un contrato o un proyecto).
- Mantener las cuentas desactivadas durante un período específico antes de eliminarlas permanentemente, según las políticas de retención de datos.

Privilegios de acceso

- Los privilegios de acceso deben otorgarse basándose en el principio de mínimos privilegios.
- Cada solicitud de aumento de privilegios debe ser aprobada por el supervisor inmediato y el administrador del sistema.
- Definir roles para todas las posiciones dentro de la institución y los permisos necesarios para cada rol.
- Asignar roles a los empleados según sus responsabilidades laborales y revisar estas asignaciones trimestralmente.
- Realizar auditorías de acceso cada seis meses para verificar que los privilegios de acceso sean apropiados y necesarios.
- Mantener un registro detallado de todas las solicitudes y aprobaciones de cambio de privilegios de acceso.
- Otorgar accesos temporales con privilegios limitados para proyectos específicos.
- Configurar accesos temporales para que expiren automáticamente después del tiempo determinado de 30 días.

Administrar los derechos de acceso privilegiado

- Los roles privilegiados deben estar claramente definidos y documentados.
- Los derechos de acceso privilegiado solo se otorgarán a los usuarios que los necesiten para cumplir con sus responsabilidades laborales.
- Todos los accesos privilegiados requieren autenticación multifactor (MFA).
- Los métodos de MFA incluyen aplicaciones de autenticación, tokens de hardware y biometría.
- Mantener registros detallados de todas las actividades realizadas con acceso privilegiado.
- Implementar herramientas de monitoreo continuo para detectar y alertar sobre actividades inusuales o no autorizadas.
- Realizar auditorías de acceso privilegiado cada seis meses.
- Revisar periódicamente los derechos de acceso privilegiado para asegurar que sean necesarios y apropiados.
- Informar a los usuarios sobre los riesgos asociados con el acceso privilegiado y cómo mitigarlos.

Revocación de derechos de acceso

- Todos los accesos de los empleados que dejan la institución deben ser revocados inmediatamente al finalizar su relación laboral.
- El equipo de TI debe recibir notificación de la terminación del empleado y completar la revocación de accesos dentro de las 24 horas siguientes.

- Realizar auditorías de acceso cada seis meses para identificar y revocar accesos innecesarios o inapropiados.
- La alta gerencia debe revisar y confirmar los permisos de acceso de sus subordinados directos trimestralmente.
- Configurar todos los accesos temporales con una fecha de expiración automática, no superior a 90 días.
- Revisar y renovar accesos temporales solo si es absolutamente necesario y documentar las razones para la renovación.
- Monitorear y detectar cuentas de usuario que han estado inactivas durante más de 30 días.
- Revisar y desactivar cuentas inactivas después de confirmar que no son necesarias.

Control de acceso a aplicaciones y sistemas

Procedimientos de inicio de sesión seguro

- Las contraseñas deben tener al menos 8 caracteres y contener al menos una letra mayúscula, una minúscula, un número y un carácter especial.
- Se debe cambiar la contraseña cada 90 días y no se pueden reutilizar las últimas cinco contraseñas.
- Todos los empleados deben usar autenticación multifactor para acceder a sistemas internos y aplicaciones sensibles.
- Los métodos aceptables de MFA incluyen aplicaciones de autenticación móvil y tokens de seguridad.
- Las sesiones deben cerrarse automáticamente después de 15 minutos de inactividad.

- Cada usuario puede tener una sola sesión activa a la vez y debe cerrar sesión en todos los dispositivos antes de iniciar una nueva sesión.
- Se debe mantener un registro detallado de todos los intentos de inicio de sesión exitosos y fallidos.
- El equipo de seguridad de la información debe revisar los registros de inicio de sesión diariamente para detectar intentos de acceso no autorizados.
- Las contraseñas nunca deben almacenarse en texto claro y deben ser encriptadas tanto en almacenamiento como en transmisión.
- Las credenciales de acceso solo deben transmitirse a través de conexiones seguras y cifradas.

Gestión de contraseñas

- Las contraseñas deben tener al menos 8 caracteres y contener al menos una letra mayúscula, una minúscula, un número y un carácter especial.
- Se debe cambiar la contraseña cada 90 días y no se pueden reutilizar las últimas cinco contraseñas.
- Las contraseñas deben almacenarse utilizando técnicas de hashing seguras y nunca en texto claro.
- Las credenciales de acceso solo deben transmitirse a través de conexiones seguras y cifradas.
- Todos los empleados deben usar autenticación multifactor para acceder a sistemas internos y aplicaciones sensibles.
- Los métodos aceptables de MFA incluyen aplicaciones de autenticación móvil y tokens de seguridad.

- Los empleados no deben compartir sus contraseñas con otros empleados, contratistas o terceros.
- Las contraseñas no deben escribirse en áreas accesibles o visibles para otros empleados.
- Se debe realizar una auditoría de contraseñas cada seis meses para asegurar el cumplimiento de las políticas de seguridad.
- Se debe monitorear continuamente el uso de contraseñas y el acceso a sistemas críticos para detectar posibles actividades maliciosas.

3.17 Uso de cifrado.

El cifrado asegura que solo los autorizados puedan leer la información. Al cifrar la información se protege la privacidad de los datos durante su transmisión o almacenamiento.

Y las políticas cruciales que se deberán implementar son las siguientes:

- Todos los datos sensibles, incluyendo información personal y financiera, deben ser cifrados durante la transmisión a través de redes públicas o no seguras y durante el almacenamiento en repositorios de datos.
- Se deben utilizar algoritmos de cifrado robustos como AES-256 para proteger los datos sensibles.
- Todas las claves de cifrado deben ser almacenadas de manera segura utilizando técnicas de protección fuertes como el almacenamiento en módulos de seguridad de hardware (HSM).
- Las claves de cifrado deben ser rotadas cada 90 días y en caso de sospecha de compromiso.

- Todos los correos electrónicos enviados fuera de la red interna deben ser cifrados utilizando cifrado de correo electrónico seguro.
- Todos los datos transmitidos a través de redes inalámbricas deben ser cifrados utilizando protocolos de cifrado como WPA2.
- Todos los dispositivos móviles que almacenen datos sensibles deben estar cifrados.
- Las unidades USB utilizadas para el almacenamiento de datos sensibles deben estar cifradas y protegidas con una contraseña segura.
- Realizar auditorías periódicas para verificar el cumplimiento de las políticas de cifrado y la efectividad de las medidas implementadas.
- Verificar regularmente la configuración de cifrado de los servidores y dispositivos de red para asegurar que estén configurados de acuerdo con las políticas de seguridad.

3.18 Seguridad de las Operaciones.

Procedimientos operativos documentados

Los procedimientos operativos documentados son esenciales para la seguridad de las operaciones en cualquier organización. Estos documentos detallan las tareas, procesos y responsabilidades específicas, proporcionando una guía clara y estandarizada para el personal. Su principal objetivo es asegurar que todas las actividades se realicen de manera consistente y segura, minimizando errores y riesgos.

Estos procedimientos ayudan a garantizar el cumplimiento de las políticas de seguridad y regulaciones aplicables, reduciendo la posibilidad de violaciones de seguridad. Al tener procedimientos claros, se facilita la capacitación de nuevos empleados y la transferencia de

conocimientos, asegurando que todos los miembros del equipo sigan las mejores prácticas y protocolos establecidos.

- Los procedimientos operativos deben ser creados por personal calificado y conocedor del proceso específico.
- Todo procedimiento debe ser revisado y aprobado por la alta dirección o un comité específico antes de su implementación.
- Los procedimientos deben seguir un formato estándar que incluya objetivos, alcance, responsabilidades, pasos detallados, y referencias.

Gestión de cambios

La gestión de cambios es crucial para asegurar que las modificaciones en sistemas, infraestructuras o procesos se realicen de manera controlada y sin impactos negativos en la seguridad y la operación de la institución.

Protección de malware

- Todos los parches de seguridad críticos deben ser revisados y aplicados dentro de los primeros 7 días de su publicación.
- Planificar mantenimientos regulares para asegurar que los sistemas estén actualizados con las últimas protecciones contra malware.
- Limitar los privilegios de instalación de software a usuarios autorizados y asegurar que el software provenga de fuentes confiables y verificadas.
- Establecer un proceso formal para la aprobación y instalación de nuevo software en sistemas críticos, asegurando que solo el software autorizado y seguro sea instalado.

- Implementar sistemas de monitoreo continuo para detectar actividad sospechosa o indicadores de compromiso relacionados con malware.
- Desarrollar procedimientos de respuesta a incidentes específicos para malware, incluyendo la cuarentena y eliminación de amenazas.

Copias de seguridad

- Implementar procedimiento de respaldo.
- Proteger los medios de copia de seguridad contra accesos no autorizados.
- Llevar un inventario de los medios de respaldo.

Gestión de Vulnerabilidades Técnicas

- Implementar herramientas de escaneo de vulnerabilidades que realicen revisiones automatizadas de los sistemas y aplicaciones en busca de vulnerabilidades.
- Evaluar el riesgo de cada vulnerabilidad identificada en términos de su impacto potencial y probabilidad de explotación, asignando una puntuación de riesgo.
- Todos los cambios propuestos para abordar vulnerabilidades deben ser documentados en un registro de cambios detallado.
- Desarrollar un plan de implementación detallado que incluya plazos y recursos necesarios para la remediación de cada vulnerabilidad.

Escaneo de vulnerabilidades

- Aborde de forma rápida las vulnerabilidades de seguridad con el fin de minimizar la exposición de la aplicación o el sistema.

- Es necesario llevar a cabo una evaluación de vulnerabilidades en las aplicaciones y bases de datos antes de proceder con la puesta en marcha del servicio.
- Es indispensable llevar a cabo un examen de vulnerabilidad de manera regular en todas las aplicaciones y sistemas.

3.19 Seguridad de la red.

Para asegurar que las redes protejan adecuadamente la información en los sistemas y aplicaciones, es crucial implementar políticas y controles que aborden varios objetivos clave de seguridad.

- Configurar los servidores web para que utilicen SSL/TLS, asegurando que todo el tráfico HTTP se redirija a HTTPS.
- Implementar una VPN corporativa que requiera autenticación multifactor (MFA) para el acceso remoto seguro de empleados.
- Configurar VLANs separadas para cada departamento (e.g., finanzas, recursos humanos, TI) y aplicar políticas de firewall para limitar el acceso entre VLANs.
- Implementar un sistema IDS/IPS que monitoree y analice el tráfico de red en busca de patrones de ataque conocidos, generando alertas y bloqueando tráfico sospechoso.

Configurar reglas de firewall que bloqueen puertos y protocolos no utilizados y limiten el acceso a servicios críticos solo a IPs autorizadas.

3.20 Seguridad de eliminación y reutilización de activos.

Es fundamental asegurarse de que los datos dentro de los sistemas o dispositivos sean eliminados de manera segura para poder reutilizar los activos de manera segura o deshacerse de ellos adecuadamente.

Estas políticas deben abarcar la eliminación física y lógica de datos, así como la preparación adecuada de los activos para su reutilización.

- Utilizar software de borrado seguro que sobrescriba los datos múltiples veces, siguiendo estándares como DoD 5220.22-M o NIST 800-88.
- Aplicar técnicas de desmagnetización a discos duros y cintas magnéticas para destruir la información almacenada.
- Realizar un formateo completo y seguro de discos duros antes de su reutilización en otros sistemas.
- Triturar discos duros y otros medios de almacenamiento utilizando una trituradora certificada que convierta los medios en partículas pequeñas e irrecuperables.
- Incinerar medios de almacenamiento en instalaciones certificadas para asegurar que los datos sean completamente destruidos.
- Mantener los activos en áreas seguras con acceso controlado hasta que se complete el proceso de eliminación.

3.21 Incidentes de seguridad.

El Equipo de Respuesta a Incidentes de Hospital Santa Teresita es el único equipo autorizado para gestionar incidentes de seguridad relacionados con los entornos informáticos de la institución. Este equipo es responsable de:

- Identificar, analizar y mitigar incidentes de seguridad.
- Coordinar la respuesta a incidentes con otras áreas relevantes.
- Realizar análisis forenses y recopilar evidencia.
- Restaurar datos y sistemas afectados.

3.22 Capacitación de concientización sobre seguridad.

El objetivo de la capacitación de concientización sobre seguridad es ayudar a los empleados del Hospital Santa Teresita a reconocer y evaluar las diversas amenazas a la seguridad de la información que enfrentamos diariamente. Esta política tiene como finalidad asegurar que todos los empleados estén conscientes de los riesgos de seguridad asociados con sus actividades y conozcan las políticas, estándares y procedimientos aplicables relacionados con la seguridad de los sistemas del hospital.

- Proporcionar sesiones de capacitación inicial a todos los empleados nuevos sobre los riesgos de seguridad relevantes.
- Realizar campañas periódicas de concientización sobre temas de seguridad específicos, como phishing, ingeniería social y protección de contraseñas.
- Distribuir materiales de concientización, como boletines, folletos y correos electrónicos informativos.

Para consultas o asistencia relacionada con la capacitación de concientización sobre seguridad, contactar al departamento de TIC del Hospital Santa Teresita a través de:

Correo Electrónico: soporte.tics@07d06.mspz7.gob.ec

3.23 Cumplimiento.

Cumplimiento de requisitos legales y contractuales

Esta política es asegurar que el Hospital Santa Teresita cumpla con todos los requisitos legales, estatutarios, reglamentarios y contractuales aplicables relacionados con la seguridad de la información y la tecnología de la información. Además, garantizar la protección de los datos contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, así como la protección de datos personales según lo exigen las legislaciones y regulaciones pertinentes.

- Asegurar el cumplimiento de todos los requisitos legales y contractuales relacionados con la seguridad de la información.
- Documentar todos los casos de incumplimiento y las acciones correctivas tomadas.
- Es necesario garantizar la protección de los datos evitando su pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, cumpliendo con los estándares legales, normativos y contractuales correspondientes.
- Según las leyes y regulaciones aplicables, es necesario asegurarse de proteger adecuadamente los datos personales y la información de identificación personal.

Consideraciones de auditoría del sistema de información

Las auditorías deben ser planificadas cuidadosamente con anticipación. Esto incluye definir el alcance de la auditoría, los objetivos, y los recursos necesarios.

- Es necesario establecer y seguir estrictamente protocolos de auditoría con el fin de asegurar que las tareas relacionadas con la revisión o auditoría se organicen de

manera meticulosa, a fin de reducir al máximo la posibilidad de que los servicios ofrecidos por el hospital se vean afectados por problemas o interrupciones imprevistas.

- Es necesario establecer medidas de seguridad específicas para evitar que personas no autorizadas accedan a información confidencial o cometan irregularidades en el proceso de auditoría.
- Los sistemas de información del Hospital Santa Teresita deben tener la capacidad de crear registros de auditoría que incluyan información detallada con el fin de determinar el tipo de incidencia que tuvo lugar, la fecha y ubicación exactas de la misma, el origen y las consecuencias del incidente, así como la identidad de todas las personas implicadas en el hecho.

3.24 Documentación mínima para establecer un SGSI.

La norma ISO 27001:2013 establece los requisitos para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI). Para cumplir con esta normativa, es necesario contar con cierta documentación mínima. A continuación se describe la documentación esencial que debe estar presente:

- Política de Seguridad de la Información
- Alcance del SGSI
- Evaluación de Riesgos y Tratamiento de Riesgos
- Declaración de Aplicabilidad
- Los objetivos de seguridad de la información
- Plan de Tratamiento de Riesgos
- Procedimientos y Controles Operacionales
- Roles y Responsabilidades de Seguridad de la Información

- Control de Documentos y Registros
- Políticas y Procedimientos Específicos
- Plan de Formación y Concienciación
- Informe de Auditorías Internas
- Revisión por la Dirección
- Acciones Correctivas y Preventivas
- Plan de Continuidad del Negocio
- Medición y Evaluación del Desempeño

Para el Hospital Santa Teresita y con base a los objetivos del diseño SGSI se reúne y produce los siguientes documentos:

- Política de Seguridad de la Información
- Alcance del SGSI
- Evaluación de Riesgos y Tratamiento de Riesgos
- Declaración de Aplicabilidad
- Los objetivos de seguridad de la información

A continuación, se evidenciar el documento que contiene el diseño del SGSI para el Hospital Santa Teresita, detallando los documentos esenciales necesarios según lo establecido en la normativa ISO 27001:2013.

3.25 Diseño del sistema de gestión de seguridad de la información para el Hospital Santa

Teresita

Alcance

El sistema de gestión de seguridad de la información del Hospital Santa Teresita se implementa de manera uniforme a todos los activos de información, sin dejar a ninguno por fuera, y se extiende de la misma forma a todos los colaboradores, incluyendo el personal hospitalario. Cada una de las unidades de la institución tiene la obligación de cumplir con sus responsabilidades de manera obligatoria.

Políticas de seguridad de la información

Su objetivo principal es establecer los principios y requisitos que deben seguirse para garantizar la protección de los sistemas de tecnología de la información pertenecientes al Hospital Santa Teresita, así como la salvaguarda de la información sensibles contenida en dichos sistemas. El departamento de Tecnologías de la Información y Comunicación ha establecido los principios y normativas de esta política con el fin de resguardar al Hospital Santa Teresita, a sus empleados y pacientes, de posibles perjuicios derivados de la incorrecta utilización de los recursos y la información del hospital. El uso inapropiado de estos activos abarca desde acciones intencionadas hasta aquellas que se realizan sin intención.

Para obtener información más detallada sobre las políticas de seguridad de la información, los interesados pueden consultar los contenidos específicos ubicados en los Anexos 3 y 4 que forman parte de este documento en particular.

Proceso de evaluación de riesgos para la seguridad de la información

Durante esta etapa, se emplea la metodología MAGERIT, la cual se fundamenta en los principios establecidos en el Libro I y II. Su objetivo es identificar con precisión los activos de información, especificando su respectivo tipo y valor. También se busca identificar las posibles amenazas, evaluando su impacto para determinar el grado de deterioro que podrían ocasionar en caso de que el riesgo se materialice en los activos identificados.

En la sección 3.10 sobre la Evaluación de Activos se explica minuciosamente cómo se aplicó la metodología para evaluar los riesgos, mientras que en el Anexo 1 de este informe se detalla la evaluación de riesgos para los activos de información de la Institución.

Proceso de tratamiento de riesgos de seguridad de la información

Se sigue utilizando el enfoque MAGERIT para gestionar los riesgos, considerando las medidas de seguridad y controles especificados en el Anexo 1 de la normativa ISO 27001:2013, con el propósito de reducir los impactos de todos los riesgos que han sido detectados.

Para obtener más información específica sobre cómo se aborda el tratamiento de riesgos, se puede consultar la sección 3.12 dedicada a las Medidas de Protección de Activos de Información. El Anexo 1 de la norma ISO 27001:2013 fue implementado y ahora se puede observar en el Anexo 2 de este documento cada una de las medidas de protección que se deben poner en práctica para mitigar los riesgos identificados.

Declaración de aplicabilidad

Después de haber identificado de manera exhaustiva todos los posibles riesgos de seguridad y haber determinado las medidas específicas destinadas a mitigarlos, se vuelve crucial y esencial

concluir con la creación de una declaración de aplicabilidad detallada que contenga los controles de seguridad correspondientes, con el objetivo de consolidar y fortalecer los procesos implementados para garantizar la máxima protección de la información sensible.

La declaración de aplicabilidad fue desarrollada tomando como referencia el Anexo 1 de la norma ISO 27001:2013, el cual detalla 14 áreas de enfoque y un total de 105 medidas de control asociadas a la seguridad de la información.

En el Hospital Santa Teresita se decidió que es necesario implementar los 105 controles específicos a raíz de los riesgos detectados y la carencia de directrices y normativas en materia de seguridad. Asimismo, se requieren para regular la contratación, la seguridad tanto física como digital, y la adhesión a las políticas y procedimientos establecidos.

La institución declara su aplicabilidad, lo cual está detallado en el Anexo 5 del documento.

Objetivos de seguridad de la información

- Garantizar la protección de los activos de información implica asegurarse de que únicamente el personal autorizado tenga la capacidad de acceder y manipular la información almacenada en los sistemas, lo cual se logra estableciendo categorías para los usuarios, roles específicos y permisos adecuados.
- Emplear técnicas de autenticación con el fin de prevenir la usurpación de identidad, partiendo de la implementación generalizada de credenciales de acceso y certificados digitales para incrementar la protección de la seguridad, así como las categorías de permisos y autorización.
- Establecer claramente los niveles de permisos que determinan quién puede acceder y operar los recursos de información, asegurando que se realicen revisiones regulares para

garantizar que únicamente los usuarios autorizados tengan acceso y manipulen los recursos, incluyendo la posibilidad de revocar los permisos de acceso.

- Garantizar que la información se mantenga segura y protegida en todo momento a través de procedimientos autorizados que cumplen con la integridad, confidencialidad y disponibilidad, asegurando que no haya modificaciones, alteraciones, divulgaciones o accesos no autorizados a los datos.
- Crear mecanismos de seguimiento y sistemas de alerta que tengan la función de supervisar y controlar las operaciones relacionadas con la seguridad, así como la identificación y documentación de cualquier incidente o situación sospechosa que pueda comprometer la seguridad y confidencialidad de la información.

Este apartado describe cómo se establece un Sistema de Gestión de la Seguridad de la Información (SGSI) de acuerdo con la normativa ISO 27001:2013 a través de la documentación mínima necesaria que el Hospital Santa Teresita debe proporcionar.

Conclusiones

El análisis de los objetivos previamente establecidos revela que la aplicación de la metodología MAGERIT permitió la evaluación exitosa de los recursos de información en el Hospital Santa Teresita. Este proceso facilitó la continua actualización del registro de activos de información y la identificación de posibles amenazas y vulnerabilidades que podrían poner en peligro dichos recursos.

Concluyendo, una vez que se ha evaluado el efecto de las amenazas en los activos de información, se procede a establecer un plan de acciones específicas para proteger estos activos, utilizando las medidas de seguridad descritas en el Anexo 1 de la norma ISO 27001:2013. Se incita al Hospital Santa Teresita a implementar estas medidas con el fin de reducir los riesgos, y al mismo tiempo se destaca la importancia de mantener actualizada la identificación de riesgos y el plan de tratamiento de forma continua.

El Hospital Santa Teresita ha verificado que la falta de conciencia, conocimiento e importancia sobre la seguridad de la información pone en riesgo sus activos de manera crítica y requiere atención inmediata. Esto subraya la importancia de establecer políticas de seguridad para dirigir y fomentar las buenas prácticas y estándares en la gestión segura de la información, en conformidad con la norma ISO 27001:2013.

Debido a lo mencionado previamente, se ha logrado establecer los elementos mínimos de documentación necesarios para que el Hospital Santa Teresita pueda desarrollar su SGSI de acuerdo con lo indicado en la normativa ISO 27001:2013. Esto impulsará a la institución a llevar a cabo la implementación del SGSI de manera efectiva, asegurando que genere la documentación requerida y exigida por la norma.

Recomendaciones

Implementar los controles y medidas de protección específicas establecidas de acuerdo con las directrices presentadas en el Anexo 1 de la normativa ISO 27001:2013.

Divulgar las políticas de seguridad a los empleados y al personal de salud de la institución es importante para asegurar que sean conscientes de ellas y las cumplan adecuadamente.

Fomentar la sensibilización sobre los asuntos relacionados con la seguridad y educar acerca de la relevancia y el significado de resguardar y preservar los activos de información de la institución.

Realizar inspecciones internas para garantizar que se cumplan las políticas y medidas de seguridad establecidas.

Es necesario seguir adelante con la creación de la documentación necesaria que aún no ha sido elaborada para cumplir con los estándares de la norma ISO 27001:2013, con el objetivo de lograr la correcta implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Contratar auditores externos para garantizar el cumplimiento de los requisitos legales de la norma ISO 27001:2013.

Es crucial que los profesionales especializados en seguridad de la información se mantengan continuamente actualizados en el ámbito de la seguridad para asegurar y supervisar de manera efectiva la protección de los activos de información.

Bibliografía

Alemán, N. & Helena, C. I. (2015). METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN SGSI EN LA FUNDACIÓN UNIVERSITARIA JUAN DE CASTELLANOS, BAJO LA NORMA ISO 27001:2005.

https://reunir.unir.net/bitstream/handle/123456789/3129/HelenaClaraIsabel_Aleman_Novoa.pdf?sequence=1&isAllowed=y

Antonio, J. M. A. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior.

Estudios Internacionales, 53(198), 169–197. <https://doi.org/10.5354/0719-3769.2021.57067>

Delgado, A. A. C. (2017). Fundamentos de seguridad informática. Areandina, 2, 98.

<https://digitk.areandina.edu.co/handle/areandina/1367>

Guerrero, Y. & Tabango, R. (2014). Sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO 27001 y 27002 para la unidad de Informática y Telecomunicaciones de la Universidad de Nariño.

Guzmán, A. (2015). Diseño de un sistema de gestión de la seguridad informática – SGSI, para empresas del área textil en la ciudad de Itagüí, Medellín y Bogotá D.C. a través de la auditoría. Colombia. UNAD. Escuela de Ciencias Básicas Tecnología e Ingeniería, 176.

Hernández, C. (2016). Seguridad Informática 1. Informática Aplicada MX.

James, D. (2023). Ransomware: 2023's top attacks and need-to-know stats | Egress.

<https://www.egress.com/blog/phishing/top-ransomware-attacks-statistics>

Markus, E. (2018). 7. Análisis de Riesgo | Gestión de Riesgo en la Seguridad Informática.

https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

Ministerio de Hacienda y Administraciones Públicas. (2012). PAe - MAGERIT v.3 :

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Moreno, C. & Otalora, N. (2020). Diseño de un sistema de gestión de seguridad de la

información para la empresa Sociedad Hotelera San Pablo basado en la norma ISO/IEC 270001: 2013.

Niño, M. N. R. (2019). Modelo de un sistema de gestión de seguridad de información – SGSI,

para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial

Lambayeque. <http://repositorio.unprg.edu.pe/handle/20.500.12893/5935>

Palacios, P. D. O. (2015). Diseño de un sistema de gestión de seguridad de la información

(SGSI) para el área de informática de la cooperativa del magisterio de Túquerres bajo la norma ISO 27001: 2013. Universidad Nacional Abierta y a Distancia UNAD.

<https://repository.unad.edu.co/handle/10596/3817>

Perdomo, R. M. A. & Mateus, A. F. S. (2018). Diseño de un sistema de gestión de seguridad

(SGSI) para la empresa Manufacturera Persianas Y Enrollables Safrá SAS basado en los estándares de la norma ISO 27001 - hdl:11349/14200.

<https://repository.udistrital.edu.co/handle/11349/14200>

Plaza, G. M. (2021). Análisis de un ataque Ransomware. Desarrollo del ransomware Gengar.

Treballs Finals de Grau (TFG) - Enginyeria Informàtica.

<https://diposit.ub.edu/dspace/handle/2445/182628>

Poveda, J. (2015). Modulo 7: Los activos de seguridad de la información.

[Http://Www.Worldvisioncapacitacion.Cl/Wp-](Http://Www.Worldvisioncapacitacion.Cl/Wp-Content/Uploads/Cursos_adjuntos/F52e0bd4c6c2c203413952826f916237.Pdf)

Content/Uploads/Cursos_adjuntos/F52e0bd4c6c2c203413952826f916237.Pdf.

Quiñones, R. (2021). Cyberwarfare o Ciberguerra. Comunicación: Estudios Venezolanos de

Comunicación, ISSN 0798-1856, N°. 196 (4º Trimestre), 2021 (Ejemplar Dedicado a:

Diseminados), Págs. 95-103, 196, 95–103.

<https://dialnet.unirioja.es/servlet/articulo?codigo=8255848&info=resumen&idioma=SPA>

Rojas, L. E. E. (2023). Diseño del sistema de seguridad de la información en la constructora

Galaxia SAC basado en la norma ISO/IEC 27001.

<http://repositorio.uncp.edu.pe/handle/20.500.12894/9215>

Ruiz, C. J. J. (2018). Modelo para la implementación de la ley de protección de datos personales basado en el SGSI de la norma ISO 27001.

<https://repository.unad.edu.co/handle/10596/18453>

Ruiz, D. J. (2016). Ciberamenazas: ¿el terrorismo del futuro? Bie3: Boletín IEEE, ISSN-e 2530-

125X, N° 3 (Julio - Septiembre), 2016, Págs. 541-561, 3, 541–561.

<https://dialnet.unirioja.es/servlet/articulo?codigo=6019490&info=resumen&idioma=ENG>

Ruiz, R. F. O. (2024). Diseño de un sistema de gestión de seguridad de la información al proceso de tic en la organización ortopédica alca plus s.a.s.

<https://repository.unad.edu.co/handle/10596/61633>

- Torres, L. M. J. (2024). Análisis de la seguridad de la red del Ministerio de Inclusión Económica y Social mediante técnicas de hacking ético para identificar vulnerabilidades y amenazas. <https://repositorio.upse.edu.ec/handle/46000/10937>
- Ulloa, M. L. (2023). Vista de Ataque cibernético al Hospital Ciudad Neily, Caja Costarricense Seguro Social, acciones realizadas, 31 de mayo-31 de agosto 2022. <https://revistas.uned.ac.cr/index.php/repertorio/article/view/4744/6544>
- Vargas, M. J. E. (2024). Diseño de un sistema de gestion de seguridad de la informacion sgsi para la emprea gotalk sas con base a la norma iso 27001:2013 Con Base A La Norma ISO 27001:2013. <https://repository.unad.edu.co/handle/10596/61544>
- Yanez, S. C. Del. (2007). Diseño de un sistema de gestión de seguridad de la información para el proceso soporte al usuario bajo la norma ISO/IEC 27001 en la empresa Copcil Consultora Profesional Cía. Ltda. <http://bibdigital.epn.edu.ec/handle/15000/8347>
- Yuver, P. P., Ancco, H., Información En, L. A., Municipalidad, L. A., De, D., Roberto, I. & Quispe, Q. (2018). Modelo de gestión de seguridad de la información con ISO/IEC 27001 para minimizar la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2018. Universidad Nacional José María Arguedas. <http://repositorio.unajma.edu.pe/handle/20.500.14168/487>

Anexos

Anexo 1. Evaluación de riesgos

[Vinculo de evaluación de riesgos](#)

Anexo 2. Tratamiento del Riesgo

[Vinculo de tratamiento del riesgo](#)

Anexo 5. Declaración de aplicabilidad

[Vinculo de declaración de aplicabilidad](#)

Anexo 3. Política de seguridad de la información para todos los empleados del hospital santa teresita



REPÚBLICA
DEL ECUADOR

Ministerio de Salud Pública

DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

POLITICA DE SEGURIDAD DE LA INFORMACION PARA TODOS LOS EMPLEADOS DEL HOSPITAL SANTA TERESITA

DECLARACIÓN Y PROPÓSITO

La finalidad de esta política es definir los principios y condiciones que deben seguirse para garantizar la seguridad de los sistemas de tecnología de la información pertenecientes al Hospital Santa Teresita, así como para proteger la información sensible que reside en dichos sistemas. El departamento de Tecnologías de la Información ha establecido claramente los fundamentos y condiciones de esta política con el objetivo de garantizar la protección del Hospital Santa Teresita, así como de sus empleados y pacientes, frente a posibles perjuicios generados por el inapropiado uso de los activos e información del Hospital Santa Teresita. El inadecuado manejo de estos activos abarca tanto las acciones intencionadas como las involuntarias.

APLICABILIDAD

Esta política se extiende a cada uno de los trabajadores del Hospital Santa Teresita, sin importar la posición jerárquica ni ninguna otra circunstancia que pueda surgir. Cada una de las áreas de la institución tiene la responsabilidad de cumplir obligatoriamente con esta política.

DEFINICIONES Y ALCANCE

Esta política incluye todos los sistemas de tecnología de la información del Hospital Santa Teresita y la información que contienen.

DECLARACIONES

Las implicaciones de utilizar inapropiadamente nuestros recursos pueden tener consecuencias serias y negativas. Los posibles daños están relacionados con una variedad de consecuencias, como la posibilidad de sufrir infecciones de malware (tales como virus informáticos), la disminución en la eficiencia laboral, menoscabo de las relaciones con el personal, y la posible afectación de la reputación y situación financiera debido a la exposición de datos confidenciales. En cualquier momento, el Hospital Santa Teresita tiene la capacidad de supervisar y rastrear el uso de sus recursos y obtener datos relacionados con dichos recursos. Esto puede abarcar información almacenada en los correos electrónicos, archivos y registros de actividad de cualquier empleado, relacionada con la utilización de los recursos del Hospital Santa Teresita.

POLÍTICA DE USO PERMITIDO

- Los activos entregados por Hospital Santa Teresita deben usarse únicamente con fines laborales.
- El software debe ser utilizado solo para fines autorizados y no debe ser copiado, distribuido, instalado o eliminado sin permiso del departamento de TIC. Solo se



DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

instalará software aprobado por el Ministerio de Salud y el Hospital Santa Teresita en los dispositivos.

- Los datos deben usarse según lo autorizado, no se pueden modificar ni eliminar sin permiso.
- Los controles de seguridad relacionados con el uso de internet y correo electrónico, que han sido establecidos por el departamento de TIC, permanecerán invariables y no serán sujetos a modificaciones ni intentos por evadirlos.
 - Los empleados deben interactuar de forma segura con la tecnología para evitar ataques de phishing. No compartir su contraseña de dominio en sitios web externos y tener cuidado al hacer clic en enlaces o descargar archivos adjuntos.
 - No reenviar correos institucionales a cuentas personales.
 - Los empleados no pueden reenviar automáticamente correos a otras cuentas.
- Los empleados deben cumplir con estándares de contraseña y manejar los datos confidenciales adecuadamente al usar dispositivos personales para acceder a la red del Hospital.
- Los empleados usarán el servidor de archivos para hacer copias de seguridad de datos. No se permiten copias de seguridad en dispositivos de almacenamiento personal o cuentas en la nube.
- Los empleados que deban usar medios extraíbles personales pueden pedir una excepción y esperar su aprobación.
- Los empleados deben informar los eventos/incidentes o cualquier evento sospechoso de seguridad al departamento de seguridad.
- Los empleados que necesiten conectarse de forma remota deberán usar VPN para trabajar de forma segura desde cualquier lugar.
- Los dispositivos de Hospital Santa Teresita no deben ser llevados por los empleados en viajes personales.
- Los empleados deben obtener aprobación escrita de la alta gerencia antes de llevar activos de trabajo fuera de la ciudad por motivos laborales.

GESTIÓN DE CONTRASEÑAS

- Las contraseñas deben ser complejas. Las contraseñas deben tener un mínimo de ocho (8) caracteres de longitud y debe incluir caracteres especiales, mayúsculas, minúsculas y números.
- Las contraseñas deben actualizarse cada 90 días.
- Las contraseñas no deben incluir información personal o laboral del usuario.
- Las contraseñas no deben anotarse ni almacenarse electrónicamente en un archivo.
- Las contraseñas se guardan solo en aplicaciones de gestión de contraseñas aprobadas por el departamento de TIC.
- Las contraseñas son privadas e intransferibles y no se deben compartir.

CAPACITACIÓN



DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

La capacitación en seguridad ayuda a los empleados a identificar y evaluar las amenazas diarias. Cada usuario debe ser competente en la gestión del riesgo de la información para que la empresa tenga éxito en sus operaciones.

- Todos los empleados deben completar la capacitación de seguridad en las fechas establecidas.
- La capacitación en seguridad comenzará pronto después de ser contratados. Se llevarán a cabo actividades de concientización y capacitación de forma constante para mantener un nivel estable de conciencia.
- El Hospital Santa Teresita debe proporcionar a los empleados información sobre la ubicación de los materiales de capacitación y políticas de seguridad.

Nombre de la política: Política de seguridad de la información a todos los empleados	
Versión: 1	Fecha creación: 23/05/2024
Aprobado por: director del Hospital y departamento de TIC.	Numero: SGSI-TICS-001

Anexo 4. Política de seguridad de la información empleados con funciones y responsabilidades técnicas declaración y propósito



REPÚBLICA
DEL ECUADOR

Ministerio de Salud Pública

DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

POLITICA DE SEGURIDAD DE LA INFORMACION EMPLEADOS CON FUNCIONES Y RESPONSABILIDADES TECNICAS DECLARACIÓN Y PROPÓSITO

La finalidad de esta política es definir los principios y condiciones que deben seguirse para garantizar la seguridad de los sistemas de tecnología de la información pertenecientes al Hospital Santa Teresita, así como para proteger la información sensible que reside en dichos sistemas. El departamento de Tecnologías de la Información ha establecido claramente los fundamentos y condiciones de esta política con el objetivo de garantizar la protección del Hospital Santa Teresita, así como de sus empleados y pacientes, frente a posibles perjuicios generados por el inapropiado uso de los activos e información del Hospital Santa Teresita. El inadecuado manejo de estos activos abarca tanto las acciones intencionadas como las involuntarias.

APLICABILIDAD

Esta política se extiende a cada uno de los trabajadores del Hospital Santa Teresita, sin importar la posición jerárquica ni ninguna otra circunstancia que pueda surgir. Cada una de las áreas de la institución tiene la responsabilidad de cumplir obligatoriamente con esta política.

DEFINICIONES Y ALCANCE

Esta política incluye todos los sistemas de tecnología de la información del Hospital Santa Teresita y la información que contienen.

DECLARACIONES

Manejo de Datos y Activos

- Establecer una política de control de acceso restringido.
- Encriptar datos en redes de transmisión.
- Evitar enviar información restringida y confidencial por mensajes instantáneos o Chat estarán prohibidos y se consideran una su falta grave de seguridad.
- La información confidencial no se puede almacenar en almacenamiento expandible.
- Los requisitos para el almacenamiento expandible deben aprobarse a través de solicitud de excepción y, si es aprobado, se debe usar encriptación.
- La copia de seguridad de la información restringida y confidencial debe estar encriptada.
- Eliminar de forma segura los sistemas y medios que contengan información restringida o confidencial.

Gestión de activos.

Es imperativo establecer y mantener un sistema de gestión de activos que permita la identificación de todos los dispositivos pertenecientes Hospital Santa Teresita.

Después de Realizar la compra o recibir una donación de equipamiento informático para usuarios finales, es necesario ingresar estos elementos en la base de datos correspondiente de gestión de activos. Se les deberá asignar la información mínima necesaria para su registro, que incluye el número de serie, el número de orden de compra, el número de factura, la fecha de adquisición, la titularidad, el estado actual, la ubicación, el número de modelo y el identificador de etiqueta de activo.

Control de acceso.

Procedimiento de control de acceso



REPÚBLICA
DEL ECUADOR

Ministerio de Salud Pública

DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

Desarrollar un documento detallado que establezca un protocolo de seguridad para regular el acceso a cada aplicación o sistema, detallando las medidas para mitigar los riesgos asociados con la gestión de las cuentas de usuario, el control de acceso, la aplicación y el cumplimiento de normas de separación de funciones, así como el acceso remoto.

Es importante tener en cuenta varios aspectos en relación a la seguridad del sistema o aplicación, como los requisitos de seguridad existentes, el tipo de datos que se almacenan en ellos, las obligaciones legales o contractuales sobre la restricción de accesos, la gestión de derechos y roles de control de acceso, la necesidad de autorizaciones formales para solicitudes de acceso y revisiones periódicas, la revocación de accesos, la identificación de roles con privilegios, así como la importancia de mantener un registro detallado de todas las actividades relevantes relacionadas con la gestión de identidades y niveles de autenticación.

Acceso de usuarios

- Implementar autenticación multifactor (MFA) para acceder a sistemas críticos.
- Requerir contraseñas fuertes, cambiarlas regularmente y evitar el uso de las mismas contraseñas en múltiples sistemas.
- Realizar revisiones periódicas para asegurar que los privilegios de acceso sean adecuados y necesarios.
- Otorgar el nivel mínimo de acceso necesario para que los empleados realicen sus tareas.
- Revisar y ajustar los privilegios de acceso regularmente.

Cuentas de identificaciones a usuarios

- Establecer procedimientos formales para la solicitud, aprobación y creación de cuentas de usuario.
- Asignar identificadores únicos a cada usuario para asegurar la individualidad de cada cuenta.
- Definir y asignar roles y privilegios apropiados según las funciones del usuario.
- Desactivar inmediatamente las cuentas de usuarios que ya no están autorizados (por ejemplo, empleados que dejan la institución).
- Retener cuentas desactivadas por un período determinado antes de eliminarlas permanentemente, según las políticas de retención de datos.
- Realizar auditorías periódicas de las cuentas de usuario para verificar la necesidad continua y la adecuación de los privilegios asignados.

Cuentas de identificaciones a sistemas

- Implementar un procedimiento formal para la creación de cuentas de sistema, que requiera la aprobación de un superior o administrador de sistemas.
- Asignar identificadores de usuario únicos para cada cuenta de sistema para asegurar la trazabilidad.
- Definir y asignar roles y permisos específicos basados en las necesidades del usuario y sus responsabilidades laborales.
- Llevar a cabo auditorías regulares para verificar el cumplimiento de las políticas de cuentas de sistemas.
- Desactivar inmediatamente las cuentas de usuarios que ya no necesiten acceso al sistema (por ejemplo, al finalizar un contrato o un proyecto).
- Mantener las cuentas desactivadas durante un período específico antes de eliminarlas permanentemente, según las políticas de retención de datos.

Privilegios de acceso



DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

- Los privilegios de acceso deben otorgarse basándose en el principio de mínimos privilegios.
- Cada solicitud de aumento de privilegios debe ser aprobada por el supervisor inmediato y el administrador del sistema.
- Definir roles para todas las posiciones dentro de la institución y los permisos necesarios para cada rol.
- Asignar roles a los empleados según sus responsabilidades laborales y revisar estas asignaciones trimestralmente.
- Realizar auditorías de acceso cada seis meses para verificar que los privilegios de acceso sean apropiados y necesarios.
- Mantener un registro detallado de todas las solicitudes y aprobaciones de cambio de privilegios de acceso.
- Otorgar accesos temporales con privilegios limitados para proyectos específicos.
- Configurar accesos temporales para que expiren automáticamente después del tiempo determinado de 30 días.

Administrar los derechos de acceso privilegiado

- Los roles privilegiados deben estar claramente definidos y documentados.
- Los derechos de acceso privilegiado solo se otorgarán a los usuarios que los necesiten para cumplir con sus responsabilidades laborales.
- Todos los accesos privilegiados requieren autenticación multifactor (MFA).
- Los métodos de MFA incluyen aplicaciones de autenticación, tokens de hardware y biometría.
- Mantener registros detallados de todas las actividades realizadas con acceso privilegiado.
- Implementar herramientas de monitoreo continuo para detectar y alertar sobre actividades inusuales o no autorizadas.
- Realizar auditorías de acceso privilegiado cada seis meses.
- Revisar periódicamente los derechos de acceso privilegiado para asegurar que sean necesarios y apropiados.
- Informar a los usuarios sobre los riesgos asociados con el acceso privilegiado y cómo mitigarlos.

Revocación de derechos de acceso

- Todos los accesos de los empleados que dejan la institución deben ser revocados inmediatamente al finalizar su relación laboral.
- El equipo de TI debe recibir notificación de la terminación del empleado y completar la revocación de accesos dentro de las 24 horas siguientes.
- Realizar auditorías de acceso cada seis meses para identificar y revocar accesos innecesarios o inapropiados.
- La alta gerencia debe revisar y confirmar los permisos de acceso de sus subordinados directos trimestralmente.
- Configurar todos los accesos temporales con una fecha de expiración automática, no superior a 90 días.
- Revisar y renovar accesos temporales solo si es absolutamente necesario y documentar las razones para la renovación.
- Monitorear y detectar cuentas de usuario que han estado inactivas durante más de 30 días.
- Revisar y desactivar cuentas inactivas después de confirmar que no son necesarias.

Control de acceso a aplicaciones y sistemas

Procedimientos de inicio de sesión seguro



DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

- Las contraseñas deben tener al menos 8 caracteres y contener al menos una letra mayúscula, una minúscula, un número y un carácter especial.
- Se debe cambiar la contraseña cada 90 días y no se pueden reutilizar las últimas cinco contraseñas.
- Todos los empleados deben usar autenticación multifactor para acceder a sistemas internos y aplicaciones sensibles.
- Los métodos aceptables de MFA incluyen aplicaciones de autenticación móvil y tokens de seguridad.
- Las sesiones deben cerrarse automáticamente después de 15 minutos de inactividad.
- Cada usuario puede tener una sola sesión activa a la vez y debe cerrar sesión en todos los dispositivos antes de iniciar una nueva sesión.
- Se debe mantener un registro detallado de todos los intentos de inicio de sesión exitosos y fallidos.
- El equipo de seguridad de la información debe revisar los registros de inicio de sesión diariamente para detectar intentos de acceso no autorizados.
- Las contraseñas nunca deben almacenarse en texto claro y deben ser encriptadas tanto en almacenamiento como en transmisión.
- Las credenciales de acceso solo deben transmitirse a través de conexiones seguras y cifradas.

Gestión de contraseñas

- Las contraseñas deben tener al menos 8 caracteres y contener al menos una letra mayúscula, una minúscula, un número y un carácter especial.
- Se debe cambiar la contraseña cada 90 días y no se pueden reutilizar las últimas cinco contraseñas.
- Las contraseñas deben almacenarse utilizando técnicas de hashing seguras y nunca en texto claro.
- Las credenciales de acceso solo deben transmitirse a través de conexiones seguras y cifradas.
- Todos los empleados deben usar autenticación multifactor para acceder a sistemas internos y aplicaciones sensibles.
- Los métodos aceptables de MFA incluyen aplicaciones de autenticación móvil y tokens de seguridad.
- Los empleados no deben compartir sus contraseñas con otros empleados, contratistas o terceros.
- Las contraseñas no deben escribirse en áreas accesibles o visibles para otros empleados.
- Se debe realizar una auditoría de contraseñas cada seis meses para asegurar el cumplimiento de las políticas de seguridad.
- Se debe monitorear continuamente el uso de contraseñas y el acceso a sistemas críticos para detectar posibles actividades maliciosas.

Uso de cifrado.

El cifrado asegura que solo los autorizados puedan leer la información. Al cifrar la información se protege la privacidad de los datos durante su transmisión o almacenamiento.

Y las políticas cruciales que se deberán implementar son las siguientes:

- Todos los datos sensibles, incluyendo información personal y financiera, deben ser cifrados durante la transmisión a través de redes públicas o no seguras y durante el almacenamiento en repositorios de datos.
- Se deben utilizar algoritmos de cifrado robustos como AES-256 para proteger los datos sensibles.

DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

- Todas las claves de cifrado deben ser almacenadas de manera segura utilizando técnicas de protección fuertes como el almacenamiento en módulos de seguridad de hardware (HSM).
- Las claves de cifrado deben ser rotadas cada 90 días y en caso de sospecha de compromiso.
- Todos los correos electrónicos enviados fuera de la red interna deben ser cifrados utilizando cifrado de correo electrónico seguro.
- Todos los datos transmitidos a través de redes inalámbricas deben ser cifrados utilizando protocolos de cifrado como WPA2.
- Todos los dispositivos móviles que almacenen datos sensibles deben estar cifrados.
- Las unidades USB utilizadas para el almacenamiento de datos sensibles deben estar cifradas y protegidas con una contraseña segura.
- Realizar auditorías periódicas para verificar el cumplimiento de las políticas de cifrado y la efectividad de las medidas implementadas.
- Verificar regularmente la configuración de cifrado de los servidores y dispositivos de red para asegurar que estén configurados de acuerdo con las políticas de seguridad.

Seguridad de las Operaciones.**Procedimientos operativos documentados**

Los procedimientos operativos documentados son esenciales para la seguridad de las operaciones en cualquier organización. Estos documentos detallan las tareas, procesos y responsabilidades específicas, proporcionando una guía clara y estandarizada para el personal. Su principal objetivo es asegurar que todas las actividades se realicen de manera consistente y segura, minimizando errores y riesgos.

Estos procedimientos ayudan a garantizar el cumplimiento de las políticas de seguridad y regulaciones aplicables, reduciendo la posibilidad de violaciones de seguridad. Al tener procedimientos claros, se facilita la capacitación de nuevos empleados y la transferencia de conocimientos, asegurando que todos los miembros del equipo sigan las mejores prácticas y protocolos establecidos.

- Los procedimientos operativos deben ser creados por personal calificado y conocedor del proceso específico.
- Todo procedimiento debe ser revisado y aprobado por la alta dirección o un comité específico antes de su implementación.
- Los procedimientos deben seguir un formato estándar que incluya objetivos, alcance, responsabilidades, pasos detallados, y referencias.

Gestión de cambios

La gestión de cambios es crucial para asegurar que las modificaciones en sistemas, infraestructuras o procesos se realicen de manera controlada y sin impactos negativos en la seguridad y la operación de la institución.

Protección de malware

- Todos los parches de seguridad críticos deben ser revisados y aplicados dentro de los primeros 7 días de su publicación.
- Planificar mantenimientos regulares para asegurar que los sistemas estén actualizados con las últimas protecciones contra malware.
- Limitar los privilegios de instalación de software a usuarios autorizados y asegurar que el software provenga de fuentes confiables y verificadas.
- Establecer un proceso formal para la aprobación y instalación de nuevo software en sistemas críticos, asegurando que solo el software autorizado y seguro sea instalado.



DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

- Implementar sistemas de monitoreo continuo para detectar actividad sospechosa o indicadores de compromiso relacionados con malware.
- Desarrollar procedimientos de respuesta a incidentes específicos para malware, incluyendo la cuarentena y eliminación de amenazas.

Copias de seguridad

- Implementar procedimiento de respaldo.
- Proteger los medios de copia de seguridad contra accesos no autorizados.
- Llevar un inventario de los medios de respaldo.

Gestión de Vulnerabilidades Técnicas

- Implementar herramientas de escaneo de vulnerabilidades que realicen revisiones automatizadas de los sistemas y aplicaciones en busca de vulnerabilidades.
- Evaluar el riesgo de cada vulnerabilidad identificada en términos de su impacto potencial y probabilidad de explotación, asignando una puntuación de riesgo.
- Todos los cambios propuestos para abordar vulnerabilidades deben ser documentados en un registro de cambios detallado.
- Desarrollar un plan de implementación detallado que incluya plazos y recursos necesarios para la remediación de cada vulnerabilidad.

Escaneo de vulnerabilidades

- Aborde de forma rápida las vulnerabilidades de seguridad con el fin de minimizar la exposición de la aplicación o el sistema.
- Es necesario llevar a cabo una evaluación de vulnerabilidades en las aplicaciones y bases de datos antes de proceder con la puesta en marcha del servicio.
- Es indispensable llevar a cabo un examen de vulnerabilidad de manera regular en todas las aplicaciones y sistemas.

Seguridad de la red.

Para asegurar que las redes protejan adecuadamente la información en los sistemas y aplicaciones, es crucial implementar políticas y controles que aborden varios objetivos clave de seguridad.

- Configurar los servidores web para que utilicen SSL/TLS, asegurando que todo el tráfico HTTP se redirija a HTTPS.
- Implementar una VPN corporativa que requiera autenticación multifactor (MFA) para el acceso remoto seguro de empleados.
- Configurar VLANs separadas para cada departamento (e.g., finanzas, recursos humanos, TI) y aplicar políticas de firewall para limitar el acceso entre VLANs.
- Implementar un sistema IDS/IPS que monitoree y analice el tráfico de red en busca de patrones de ataque conocidos, generando alertas y bloqueando tráfico sospechoso.

Configurar reglas de firewall que bloqueen puertos y protocolos no utilizados y limiten el acceso a servicios críticos solo a IPs autorizadas.

Seguridad de eliminación y reutilización de activos.

Es fundamental asegurarse de que los datos dentro de los sistemas o dispositivos sean eliminados de manera segura para poder reutilizar los activos de manera segura o deshacerse de ellos adecuadamente.



DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

Estas políticas deben abarcar la eliminación física y lógica de datos, así como la preparación adecuada de los activos para su reutilización.

- Utilizar software de borrado seguro que sobrescriba los datos múltiples veces, siguiendo estándares como DoD 5220.22-M o NIST 800-88.
- Aplicar técnicas de desmagnetización a discos duros y cintas magnéticas para destruir la información almacenada.
- Realizar un formateo completo y seguro de discos duros antes de su reutilización en otros sistemas.
- Triturar discos duros y otros medios de almacenamiento utilizando una trituradora certificada que convierta los medios en partículas pequeñas e irrecuperables.
- Incinerar medios de almacenamiento en instalaciones certificadas para asegurar que los datos sean completamente destruidos.
- Mantener los activos en áreas seguras con acceso controlado hasta que se complete el proceso de eliminación.

Incidentes de seguridad.

El Equipo de Respuesta a Incidentes de Hospital Santa Teresita es el único equipo autorizado para gestionar incidentes de seguridad relacionados con los entornos informáticos de la institución. Este equipo es responsable de:

- Identificar, analizar y mitigar incidentes de seguridad.
- Coordinar la respuesta a incidentes con otras áreas relevantes.
- Realizar análisis forenses y recopilar evidencia.
- Restaurar datos y sistemas afectados.

Capacitación de concientización sobre seguridad.

El objetivo de la capacitación de concientización sobre seguridad es ayudar a los empleados del Hospital Santa Teresita a reconocer y evaluar las diversas amenazas a la seguridad de la información que enfrentamos diariamente. Esta política tiene como finalidad asegurar que todos los empleados estén conscientes de los riesgos de seguridad asociados con sus actividades y conozcan las políticas, estándares y procedimientos aplicables relacionados con la seguridad de los sistemas del hospital.

- Proporcionar sesiones de capacitación inicial a todos los empleados nuevos sobre los riesgos de seguridad relevantes.
- Realizar campañas periódicas de concientización sobre temas de seguridad específicos, como phishing, ingeniería social y protección de contraseñas.
- Distribuir materiales de concientización, como boletines, folletos y correos electrónicos informativos.

Para consultas o asistencia relacionada con la capacitación de concientización sobre seguridad, contactar al departamento de TIC del Hospital Santa Teresita a través de:

Correo Electrónico: soporte.tics@07d06.mspz7.gob.ec

Cumplimiento.

Cumplimiento de requisitos legales y contractuales

Esta política es asegurar que el Hospital Santa Teresita cumpla con todos los requisitos legales, estatutarios, reglamentarios y contractuales aplicables relacionados con la seguridad de la información y la tecnología de la información. Además, garantizar la protección de los datos



DIRECCION DISTRITAL 07D06 – SANTA ROSA - SALUD

contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, así como la protección de datos personales según lo exigen las legislaciones y regulaciones pertinentes.

- Asegurar el cumplimiento de todos los requisitos legales y contractuales relacionados con la seguridad de la información.
- Documentar todos los casos de incumplimiento y las acciones correctivas tomadas.
- Es necesario garantizar la protección de los datos evitando su pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, cumpliendo con los estándares legales, normativos y contractuales correspondientes.
- Según las leyes y regulaciones aplicables, es necesario asegurarse de proteger adecuadamente los datos personales y la información de identificación personal.

Consideraciones de auditoría del sistema de información

Las auditorías deben ser planificadas cuidadosamente con anticipación. Esto incluye definir el alcance de la auditoría, los objetivos, y los recursos necesarios.

- Es necesario establecer y seguir estrictamente protocolos de auditoría con el fin de asegurar que las tareas relacionadas con la revisión o auditoría se organicen de manera metódica, a fin de reducir al máximo la posibilidad de que los servicios ofrecidos por el hospital se vean afectados por problemas o interrupciones imprevistas.
- Es necesario establecer medidas de seguridad específicas para evitar que personas no autorizadas accedan a información confidencial o cometan irregularidades en el proceso de auditoría.
- Los sistemas de información del Hospital Santa Teresita deben tener la capacidad de crear registros de auditoría que incluyan información detallada con el fin de determinar el tipo de incidencia que tuvo lugar, la fecha y ubicación exactas de la misma, el origen y las consecuencias del incidente, así como la identidad de todas las personas implicadas en el hecho.

Nombre de la política: Política de seguridad de la información a Empleados con funciones y responsabilidades técnicas	
Versión: 1	Fecha creación: 23/05/2024
Aprobado por: director del Hospital y departamento de TIC.	Numero: SGSI-TICS-002