AUDITORIA DE LA SEGURIDAD INFORMATICA BASADA EN LA NORMA ISO/IEC 27001 E ISO/IEC 27002 PARA LA E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO, POTOSI NARIÑO.

AURA MARIA GRANJA GARCÍA

JUAN CARLOS NARVAEZ BENAVIDES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERIA
PROGRAMA DE INGENIERIA DE SISTEMAS
SAN JUAN DE PASTO
2019

AUDITORIA DE LA SEGURIDAD INFORMATICA BASADA EN LA NORMA ISO/IEC 27001 E ISO/IEC 27002 PARA LA E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO, POTOSI NARIÑO

AURA MARIA GRANJA G.

JUAN CARLOS NARVAEZ B.

Proyecto de grado presentado como requisito parcial para optar el título de ingeniero de sistemas.

DIRECTOR:

I.S. Esp. FRANCISCO SOLARTE

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERIA
PROGRAMA DE INGENIERIA DE SISTEMAS
SAN JUAN DE PASTO
2019

NOTA DE RESPONSABILIDAD

“Las ideas y conclusiones aportadas en el trabajo de grado, son responsabilidad exclusiva de los autores”.

Artículo primero del acuerdo No. 324 de octubre 11 de 1966, emanado del Honorable Consejo Directivo de la Universidad de Nariño.

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor”.

Artículo 13, Acuerdo N. 005 de 2010 emanado del Honorable Consejo Académico.

Nota de aceptación

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

_____

Firma del asesor del proyecto

San Juan de Pasto, Marzo de 2019

DEDICATORIA

Dedico este trabajo a Dios por darme vida, salud, fortaleza, sabiduría y dedicación para culminar con éxito este proyecto.

A mi familia, mi madre Rosa Lourdes García Riascos, mi padre Jesús Eduardo Granja López y mi hermana Vanessa Nathaly Granja García; por brindarme todo su apoyo en cuanto a mi vida personal y profesional, por darme consejos sabios y llenos de amor para orientar mi futuro hacia un mejor camino. A ellos por ser la motivación, orgullo y felicidad de cada uno de mis días.

A mis compañeros y amigos, en especial a Oscar Padilla por su apoyo incondicional, tiempo, interés y preocupación por mi futuro; a Maribel Pérez por su ayuda, explicaciones y asesoramiento en el desarrollo de este trabajo y también a mi compañero Juan Carlos Narváez por permitirme trabajar con él en la realización de este proyecto.

Aura María Granja García

DEDICATORIA

Quiero dedicar este trabajo al gran Hacedor del universo al que le debemos toda la Honra y toda la Gloria por siempre, a Dios Todopoderoso por hacer presencia en mi vida.

A mi madre SUSANA ROSARIO BENAVIDES por ser ese ángel en la tierra, por su tenacidad, entrega y lucha, por estar batallando hombro a hombro y por ser siempre ese apoyo incondicional que no me dejaba desfallecer.

A mi padre GERARDO ANIBAL NARVAEZ porque a través de rígido carácter siempre ha querido para mí lo mejor y ha estado pendiente de mí, ayudándome a superarme y ser mejor ser humano.

Le dedico este trabajo al gran apoyo brindado por mi prima, que más que prima ha sido como una hermana MARYURI MUÑOZ NARVAEZ a su esposo ELMER RODRIGUEZ gracias por motivarme a seguir adelante, por cada palabra de aliento

A mi compañera Aura María por haber sido un apoyo incondicional y compartir con ella grandes momentos durante este trabajo de grado.

A la familia Telepasto en especial a su director LUIS ALFONSO C AICEDO, VIVIANA MONTUFAR, NESTOR DAVID PEREZ por su valiosa colaboración y por apoyarme durante este proceso

Le dedico este trabajo de grado a mi gran amiga JULIANA MORALES por ser esa persona que confía en mí y siempre estuvo ahí ayudándome a ser mejor persona.

Una dedicatoria especial para aquellos que físicamente ya no están que ahora gozan de la presencia del creador y desde arriba nos guían y cuidan en especial para mi tío JOSE ADAUCIO BENAVIDES El que fuera como un padre para mí.

Juan Carlos Narváez Benavides

AGRADECIMIENTOS

A nuestro asesor de proyecto de grado, ingeniero Francisco Solarte Solarte por su ayuda y colaboración para el satisfactorio desarrollo de nuestro proyecto.

Gerente Edgar Alberto Burbano Martínez de la E.S.E Centro Hospital Luis Antonio Montero de Potosí, Nariño y a todos sus empleados por permitirnos realizar el desarrollo de esta investigación, proporcionándonos los espacios, el tiempo y la información requerida.

Director del programa de ingeniería de sistemas, ingeniero Manuel Bolaños; por su colaboración y comprensión en la realización de este proyecto.

Mg. Gloria Amparo Thomé, secretaria Académica de la facultad de ingeniería por su dedicación, atención y colaboración al momento de corregir y orientar este proyecto mediante la estrategia egresado no graduado de la Universidad de Nariño.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE GRÁFICOS

pág.

LISTA DE ANEXOS

RESUMEN

La E.S.E Centro Hospital Luis Antonio Montero es una entidad prestadora de servicios de salud que se compromete a dar atención al usuario con calidad, oportunidad, seguridad, accesibilidad y pertenencia mediante la infraestructura física, tecnología y el personal idóneo que posee; para cumplir con esto se hace uso de información que es procesada y almacenada de diferentes maneras haciendo que sea parte fundamental para que se pueda obtener un correcto funcionamiento en la entidad. Por tal razón, es importante que todos los aspectos y elementos involucrados que permitan dar utilidad a la información sean protegidos de cualquier vulnerabilidad, riesgo o amenaza que pueda asecharlos.

Por tal razón el presente proyecto dio a conocer las recomendaciones y planes de mejoramiento que permitieron desarrollar en la entidad posteriormente las políticas de seguridad de la información de acuerdo a los resultados obtenidos de los hallazgos de esta investigación; utilizando como primera instancia la metodología MAGERIT para el análisis y gestión de riesgos, con los resultados de las amenazas, vulnerabilidades, impacto, probabilidad y riesgo encontrados se creó un plan de tratamiento de riesgos (PTR) que mitigo de alguna manera la materialización de una amenaza; a continuación, por medio de la familia de normas NTC ISO 27000 se hizo uso de las normas ISO/IEC 27001 e ISO/IEC 27002 para seleccionar los dominios, objetivos de control y controles aplicables sobre los activos de la entidad con los cuales se realizó preguntas a través de una lista de chequeo la que permitió determinar el nivel de cumplimiento de los dominios en el centro hospital y se creó una declaración de aplicabilidad con la cual se pueden determinar que controles se encuentran o no implementados. Al finalizar, de acuerdo a lo mencionado y con todos los hallazgos encontrados se realizó los planes de mejoramiento y recomendaciones correspondientes, esperando sean tenidos en cuenta por la E.S.E Centro Hospital Luis Antonio Montero para su beneficio y puedan resguardar de manera adecuada la información y todos los aspectos relacionados con ella.

Palabras clave: Auditoria. Auditoria de seguridad informática. Metodología MAGERIT. Norma ISO/IEC 27001. Norma ISO/IEC 27002. Plan de tratamiento de riesgos. Declaración de aplicabilidad.

ABSTRACT

The E.S.E Center Hospital Luis Antonio Montero is an entity providing health services that undertakes to give attention to the user with quality, opportunity, security, accessibility and membership by the physical infrastructure, technology and qualified personnel that possess; to comply with this is makes use of information that is processed and stored in different ways making it an essential part so that you can obtain a correct functioning of the entity. For this reason, it is important that all aspects and elements involved and that allow information to be useful are protected from any vulnerability, risk or threat that may be endangered.

For this reason, the present project aims to make known the recommendations and plans of improvement that allow to develop in the entity subsequently the policies of security of the information according to the results obtained from the findings of this research; Using as a first instance the MAGERIT methodology for the analysis and risk management, with the results of the threats, vulnerabilities, impact, probability and risk found a risk treatment plan (PTR) will be created that allows to mitigate of Some way the materialization of a threat; then, through the NTC ISO 27000 family of standards, ISO/IEC 27001 and ISO/IEC 27002 will be used to select the applicable domains, control objectives and controls over the assets of the entity with which they will be carried out. questions through a checklist which will allow to determine the level of compliance of the domains in the hospital center and a declaration of applicability will be created with which it can be determined which controls are or are not implemented. On having finished, in accordance with the mentioned and with all the opposing finds there are realized the plans of improvement and corresponding recommendations, waiting they are born in mind by the E.S.E Center Hospital Luis Antonio Montero for its benefit and be able to protect in a suitable way the information and all the aspects related to it.

Key words: Audit. Audit of computer security. Methodology MAGERIT. Standard ISO/IEC 27001. Standard ISO/IEC 27002. Risk treatment plan. Statement of Applicability.

INTRODUCCIÓN

De acuerdo al ensayo realizado por García Estudillo (2015) la importancia de la información en las empresas se encuentra contemplada de la siguiente manera:

> "La información es un recurso que no se puede palpar es por ello que muchas empresas han cometido el grave error de no darle a la información la importancia que merece. Quizás esto se deba a que sus rendimientos y resultados no sean manifiestos físicamente e individualmente, pero sin embargo la información contribuye en gran parte del éxito obtenido en la empresa y el grave error recae en que a la información la excluyen del éxito logrado en esta misma"[1].

Esto da una perspectiva sobre la importancia que en algunas de las entidades se da a la información, la cual no es la más adecuada y debería ser todo lo contrario; además hay que considerar que la información siempre tiene asociados diferentes factores que hacen que pueda ser útil como por ejemplo: el lugar donde se aloja, el personal que la manipula, las adversidades a las cuales puede estar expuesta ya sean de principio natural o humano; es por esto que deben también considerarse como prioridad para su resguardo.

Teniendo en cuenta el artículo Seguridad Informática ¿Qué hacer para proteger la información? publicado en la Revista Gerencia "la seguridad informática es una de las materias más amplias dentro del mercado de las Tecnologías de Información. Incluye desde el robo físico de documentos y archivos, hasta la copia de bases de datos y almacenamiento de información en dispositivos externos. Por eso, abordarla a nivel empresarial es una tarea compleja."[2]

Lo mencionado con anterioridad tuvo como propósito contextualizar por qué es importante la protección de la información contra ataques internos y externos como sabotajes informáticos que pueden causar daños en la parte de hardware y software del sistema, los ataques se pueden realizar de varias formas desde lo más simple

---

[1] GARCÍA ESTUDILLO, Victoriano. La información como recurso estratégico para las empresas. [en línea]. Gestiopolis. 13 de abril de 2015. [citado en 2016] Disponible en internet: http://www.gestiopolis.com/la-informacion-como-recurso-estrategico-para-las-empresas/

[2] REVISTA GERENCIA. Seguridad informática ¿Qué hacer para proteger la información? [en línea]. Gerencia. Noviembre de 2009. Disponible en internet: http://www.emb.cl/gerencia/articulo.mvc?xid=932

como desconectar el computador de su fuente de energía mientras se está trabajando, hasta las más complejas como el uso de programas lógicos destructivos aplicando para ello bombas lógicas, virus informáticos o contaminación de la información a través de gusanos.

Para realizar esta investigación fueron necesarias diversas normas que permiten detectar estas debilidades y ayudan a establecer controles que las contrarresten, una de ellas es la norma ISO/IEC 27001 y la norma ISO/IEC 27002 desarrolladas por la organización internacional de estándares ISO, que proporcionan un marco de gestión de la seguridad utilizable por cualquier organización pública o privada, sea grande, mediana o pequeña.

Las normas hacen referencia no solo a la seguridad informática en los sistemas de información usados para el procesamiento y manejo de la información, sino también de todos los activos de tecnologías de información usado en los procesos y servicios que se brinda a los usuarios y clientes finales de una organización.

En este orden de ideas fue necesario establecer controles de tipo preventivo, detectivo y correctivo que permitan asegurar la información buscando cumplir con las características de confidencialidad, integridad y disponibilidad para garantizar un óptimo nivel de servicios en sus procesos y procedimientos. Aquí fue necesario aplicar procesos de análisis y gestión de riesgos que permitieron establecer las vulnerabilidades y amenazas para hacer un diagnóstico previo, y posteriormente aplicar auditorías internas que permitan disminuir el impacto y la ocurrencia de fallas mediante planes de mejoramiento y controles.

Este proyecto se basó en la realización de una auditoria a la seguridad informática de la E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO, POTOSI NARIÑO; para ello se utilizó como apoyo las normas ISO/IEC 27001 e ISO/IEC 27002 las cuales fueron estudiadas y analizadas, posteriormente con estas bases se determinó de acuerdo a los activos encontrados en la entidad cuales eran los dominios a aplicar en esta auditoría; además se estableció que métricas, indicadores y escalas se tuvieron en cuenta en la realización del diseño de instrumentos de recolección de información, los cuales fueron aplicados en las respectivas áreas de la entidad de salud.

De acuerdo a los resultados obtenidos se procedió a su respectivo análisis del cual se determinaron los controles que pueden ayudar a mitigar los riesgos,

vulnerabilidades y amenazas encontrados y se realizó las respectivas recomendaciones y planes de mejoramiento.

Al culminar esta auditoria los beneficios que obtuvo la E.S.E Centro Hospital Luis Antonio Montero, Potosí Nariño son: que pueden adoptar los controles, planes de mejoramiento y recomendaciones brindados; para así poder mejorar significativamente la seguridad informática que se maneja en esta entidad.

Área de investigación

El proyecto se ubica dentro del área de investigación de Auditoria de Sistemas Computacionales definido por el comité curricular del Programa de Ingeniería de Sistemas de la Universidad de Nariño.

Línea de investigación

La línea de investigación a la cual pertenece el proyecto se denomina **Gestión, Seguridad y Control** porque ayuda a preservar la seguridad informática y de la información del Centro Hospital LUIS ANTONIO MONTERO, POTOSI NARIÑO.

Descripción del problema

Planteamiento del problema

El centro Hospital LUIS ANTONIO MONTERO cuenta con problemas de pérdida de información debido a la falta de integridad entre los diferentes componentes del sistema de información; además no se han realizado auditorias que permitan identificar los riegos, amenazas, y vulnerabilidades a los que se encuentran expuestos y no existen normas que garanticen la seguridad informática dentro de la entidad.

De acuerdo a Martínez de la Cruz (2009) “La información es un recurso vital para toda organización, y el buen manejo de esta puede significar la diferencia entre el éxito o el fracaso para todos los proyectos que se emprendan dentro de un

organismo que busca el crecimiento y el éxito"[3]. Por esta razón, según cómo se dé el tratamiento de esta depende que todo proceso que allí se realice sea eficiente, además es importante que las empresas inviertan en la seguridad informática y de la información y la tomen como un activo más del cual se pueden beneficiar ampliamente.

Según Erb (2009) "Desde el punto de vista de la entidad que maneja los datos, existen amenazas de origen externo como por ejemplo las agresiones técnicas, naturales o humanas, sino también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos"[4]; esto significa pérdidas para la organización porque la información representa un activo importante en la toma de decisiones.

Objetivo general

Auditar el sistema de información y activos informáticos de las diferentes dependencias de la E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO basándose en las normas ISO/IEC 27001 e ISO/IEC 27002; para recomendar la creación e implementación de políticas y controles que garanticen la integridad, confiabilidad, confidencialidad y seguridad de la información.

Objetivos específicos

- Analizar el sistema de información y activos informáticos que se va a auditar en la E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO mediante la realización de visitas a la entidad.

- Aplicar la metodología de gestión de riesgos seleccionada, MAGERIT; para poder determinar los riesgos asociados a los activos de la entidad y posteriormente realizar el plan de tratamiento de riesgos.

---

[3] MARTÍNEZ DE LA CRUZ, Sergio Alejandro. Importancia de los sistemas de información para las Pymes. [en línea]. Gestiopolis. 01 de noviembre de 2005. [citado en 2016] Disponible en internet: http://www.gestiopolis.com/importancia-sistemas-informacion-pymes/

[4] ERB, Markus. Amenazas y Vulnerabilidades. [en línea]. Disponible en internet: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/ [citado 2016]

- Determinar los dominios, objetivos de control y controles aplicables a los activos de la E.S.E Centro Hospital Luis Antonio Montero, según las normas ISO/IEC 27001 e ISO/IEC 27002 y según sus resultados, determinar la matriz de aplicabilidad correspondiente.

- Presentar los hallazgos encontrados en la entidad, además del informe de recomendaciones y planes de mejoramiento obtenidos de la auditoría realizada a la E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO.

Justificación

De acuerdo a Erb (2009) “En la seguridad de la información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación no autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo, existen más requisitos como por ejemplo la autenticidad entre otros”[5]; es por eso que es imprescindible tener controles que garanticen lo descrito anteriormente.

Realizar una valoración a la entidad en cuanto a este rubro permitió identificar los riesgos a los cuales está sometida su información y de acuerdo a esto se determinó los planes a seguir para minimizar el impacto que puede causar, esto permite que la organización proteja adecuadamente los datos y de esta manera tenga una firme continuidad de sus procesos.

La evaluación también permitió descubrir hallazgos, los cuales servirán al gerente para la toma de decisiones sobre las políticas de seguridad dentro de la empresa y además reforzar sus sistemas de información para así poder disipar todo ataque sobre estos.

El resultado de esta investigación proporcionado mediante el instrumento creado a partir de la Norma ISO/IEC 27001 e ISO/IEC 27002 ayudó en gran medida a

[5] ERB, Markus. Seguridad de la Información y Protección de Datos. [en línea]. Disponible en internet: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/ [citado 2016]

descubrir las vulnerabilidades, amenazas y riesgos en cuanto a seguridad informática en los sistemas de información de la entidad.

Este proyecto es de gran importancia para la E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO, porque se orientó a defender su seguridad informática y ayudar a preservar un activo tan importante como lo es la información, al llevar a cabo este proyecto se colabora a una mejor organización dentro de la entidad, a tener información confiable que será utilizada de la mejor manera para la toma de decisiones y con la seguridad de la información se garantiza que habrá un aumento en la confiablidad por parte de los usuarios.

El potencial beneficiario de esta propuesta fue dicha entidad de Salud, porque un buen diagnóstico desembocó en la realización de controles o soluciones apropiadas ante problemas de seguridad para así garantizar la preservación de la información.

Alcance y delimitación

Este proyecto se enfocó a auditar el sistema de información y activos informáticos existentes en el Centro Hospital Luis Antonio Montero y cubrió los siguientes aspectos: usuarios existentes, administradores del sistema, y los siguientes módulos del sistema:

- Módulo de administración del sistema.
- Módulo de Historias clínicas.
- Módulo de Control de Facturación.
- Módulo de Citas médicas.
- Módulo de Salidas y reportes.

Esta propuesta contempló los 9 de los 11 dominios de la norma ISO/IEC 27001 y los controles de la norma ISO/IEC 27002.

Marco referencial

Antecedentes

Para llevar a cabo el desarrollo de un proyecto de auditoria es necesario conocer proyectos que de una u otra forma tengan relación con este, para tener de cierta forma un precedente que ayude con su buena realización.

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO"[6].

El presente proyecto presentado por: ROBERT MARCELO TABANGO y YESID CAMILO GUERRERO está enfocado en un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 y 27002 para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño, ya que la información es un factor clave de éxito y por lo tanto su eficiente administración garantiza altos estándares de calidad y productividad.

El proyecto ayudará en la aplicación de la metodología de la norma ISO/IEC 27001 e ISO/IEC 27002.

"**AUDITORIA DEL MODULO DE HISTORIA CLINICA ELECTRONICA DEL SISTEMA DE INFORMACION DEL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO"[7].**

El presente proyecto realizado por: JENNY BURGOS GARCIA y MARIA CAROLINA DOMINGUEZ en el HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO el cual se basa en una auditoria al módulo de historia clínica electrónica del sistema

---

[6] TABANGO GOYES Marcelo, GUERRERO Camilo. Sistema de gestión de seguridad de la información basado en la norma ISO 27001 y 27002 para la unidad de informática y telecomunicaciones de la universidad de Nariño, San Juan De Pasto, 2014, 150h. Trabajo de Grado (ingeniero de sistemas). Universidad de Nariño. Facultad de Ingeniería

[7] BURGOS Jenny, DOMINGUEZ María Carolina, Auditoria del módulo de historia clínica electrónica del sistema de información del hospital universitario departamental de Nariño, San Juan de Pasto, 2008. 435h. Trabajo de Grado (ingeniero de sistemas). Universidad de Nariño. Facultad de Ingeniería

de información, ayudará a aplicar de una manera adecuada las fases de auditoria en un hospital; además de complementar la utilización de la norma ISO/IEC 27001.

“AUDITORIA AL MODULO DE INVENTARIO DEL SISTEMA DE INFORMACION EN EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO”[8].

El proyecto realizado por: DENIS ALFREDO COLUNGE BELALCAZAR y JORGE ALEXIS PORTILLA VARGAS en el HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO al igual que el proyecto anterior brindará la documentación necesaria para culminar con éxito la realización de una auditoria a la entidad de salud.

[8] COLUNGE Denis Alfredo, PORTILLA Jorge Alexis. Auditoria al módulo de inventario del sistema de información en el hospital universitario departamental de Nariño, San Juan de Pasto, 2013, 165h. Trabajo de Grado (ingeniero de sistemas). Universidad de Nariño. Facultad de Ingeniería

Marco teórico

Es importante para el desarrollo de esta investigación conocer los conceptos que se encuentran relacionados al presente proyecto, de acuerdo a esto se cuenta con el siguiente soporte teórico que ayuda a entender los procedimientos que se llevaron a cabo en el desarrollo de este trabajo, como son los siguientes temas.

Auditoria

Según Santillana González[9] el concepto de auditoría significa "verificar que la información financiera, administrativa y operacional de una entidad es confiable, veraz y oportuna".

En Iso 9000:2005[10] la auditoría es un "proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría".

De tal modo Muñoz Razo[11] define auditoría como la revisión independiente de actividades, funciones, resultados u operaciones de una entidad que es realizada por un profesional; el cual evalúa la correcta realización de estos procedimientos y de acuerdo al análisis obtenido emite opiniones para establecer el cumplimiento que se tiene de ellos.

De acuerdo a lo anterior la auditoría se basa en evaluar, revisar, verificar y confirmar si hay existencia de riesgos, vulnerabilidades o amenazas y la falta de existencia de controles internos para que de esta manera se pueda dar mitigación a los hallazgos encontrados.

---

[9] SANTILLANA GONZÁLEZ Juan Ramón. Auditoria Fundamentos: Thomson. 2004

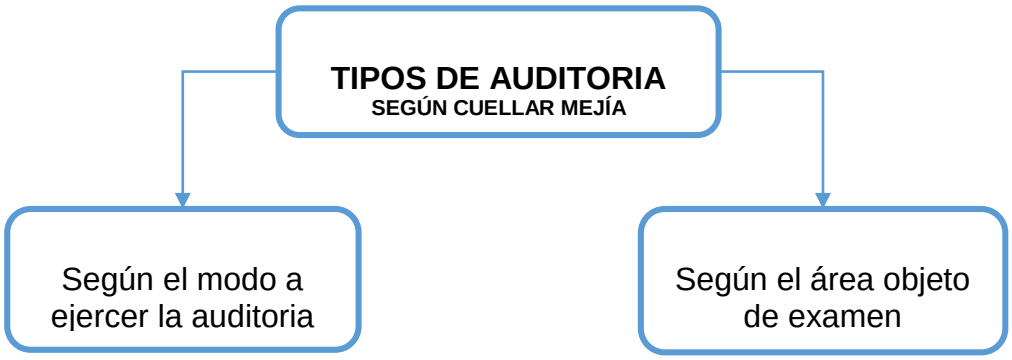
[10] Norma Técnica Colombiana. NTC ISO 9000:2005. Sistemas de Gestión de la Calidad. Fundamentos y Vocabulario. Bogotá, Colombia. ICONTEC.

[11] MUÑOZ RAZO Carlos, Auditoría en Sistemas Computacionales. Pearson Educación. México. ISBN 970-17-0405-3. Pág 11.

Tipos de auditoría

La auditoría se puede clasificar de la siguiente manera según Cuellar Mejía[12] de acuerdo al modo de ejercerla y el área objeto de examen.

Figura 1. Tipos de auditoria según Cuellar Mejía



Fuente: Autores del proyecto.

Por lo tanto, estas clasificaciones se subdividen así:

Según el modo de ejercer la auditoria:

- Auditoría Externa
- Auditoría Interna

Según el área objeto de examen:

- Auditoría Financiera
- Auditoría de Gestión
- Auditoría de Cumplimiento

[12] CUELLAR MEJIA, Guillermo Adolfo. Teoría General De La Auditoria y Revisoría Fiscal [en línea]. Septiembre de 2003. Disponible en internet: http://fccea.unicauca.edu.co/old/tgarf/marcos.html

- Auditoría de Control Interno
- Auditoría Integral
- Auditoría Informática
- Auditoría Gubernamental
- Auditoría Administrativa
- Auditoría Operacional
- Auditoría Social
- Auditoría de Recursos Humanos
- Auditoría Ambiental
- Auditoría Forense, Entre otras.

Técnicas de auditoria

Delgado Rojas[13] establece que las técnicas de auditoria tienen diferentes finalidades como la realización de pruebas a los sistemas, determinar su adecuado funcionamiento o la comprobación de datos, la realización de estas técnicas ayuda a corroborar que los procedimientos realizados en la organización cumplen de una manera satisfactoria con las necesidades que se han establecido inicialmente.

Según Muñoz Razo[14] las técnicas de auditoria se encuentran establecidas en tres grupos, las cuales son herramientas tradicionales y herramientas específicas que son aplicadas a los sistemas computacionales; se encuentran clasificadas de la siguiente manera:

Instrumentos de recopilación de datos

- Entrevistas
- Cuestionarios
- Encuestas

[13] DELGADO ROJAS, Xiomar. Auditoria Informática. [en línea] Euned. P 29. Disponible en internet: https://vdocuments.site/auditoria-informatica-xiomar-delgado-rojas-uned.html

[14] MUÑOZ RAZO Carlos, Auditoría en Sistemas Computacionales. Pearson Educación. México. ISBN 970-17-0405-3. Pág 47.

- Observación
- Inventarios
- Muestreo
- Experimentación

Técnicas de evaluación

- Examen
- Inspección
- Confirmación
- Comparación
- Revisión documental

Técnicas especiales para la auditoria de sistemas computacionales

- Guías de evaluación
- Ponderación
- Simulación
- Evaluación
- Diagrama del círculo de sistemas
- Matriz de evaluación
- Programas de verificación
- Seguimiento de programación

De acuerdo a las técnicas mencionadas anteriormente el presente trabajo tomo en cuenta algunas de ellas para llevar a cabo la realización de una buena auditoria que permita tener el desempeño adecuado a lo largo del proceso y ayude a la obtención de los resultados precisos que se necesitan para dar un informe satisfactorio acerca del estado actual que ayude a mantener y mejorar los objetivos que la organización ha planteado.

Auditoria informática

Según Echenique[15] lo define como el "proceso de recolección y evaluación de evidencias para establecer cuándo son salvaguardados los activos de los sistemas computarizados", cómo se mantiene la integridad de los datos, cómo se logran los objetivos que se encuentran establecidos en la organización de una manera eficaz y si se usan los recursos que se consumen de una manera eficiente.

De acuerdo a Delgado Rojas[16], la auditoria informática se basa en realizar la evaluación de los controles que existen sobre la administración de los recursos informáticos y también sobre los recursos que se encuentran alrededor de estos, para que de esta manera el logro de los objetivos que se establece en la organización sean alcanzados.

Muñoz Razo[17] define que es la "revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información que se utilizan en una empresa, sean individuales, compartidos y/o redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Esta revisión también se realiza a la gestión informática, aprovechamiento de recursos, medidas de seguridad y bienes de consumo que ayudan al correcto funcionamiento del centro de cómputo".

De acuerdo a los aportes de los anteriores autores se entiende que la auditoria informática se orienta a la realización de evaluaciones de los recursos informáticos y de todo lo que complementa la utilización de estos para posteriormente generar un análisis de los hallazgos. De esta manera se puede mejorar los objetivos que se encuentran establecidos en la empresa para su adecuado funcionamiento.

---

[15] ECHENIQUE GARCÍA, José Antonio. Auditoria Informática. Edición 2. McGraw-Hill Interamericana. 2001. 300 p. ISBN 9789701033562.

[16] DELGADO ROJAS, Xiomar. Auditoria Informática. [en línea] Euned. Disponible en internet: https://vdocuments.site/auditoria-informatica-xiomar-delgado-rojas-uned.html

[17] MUÑOZ RAZO Carlos, Auditoría en Sistemas Computacionales. Pearson Educación. México. ISBN 970-17-0405-3. Pág 19.

Seguridad de la información

Según Cano [18] la seguridad de la información es la "disciplina que habla de los riesgos, amenazas, análisis de escenarios, buenas prácticas y esquemas normativos, que exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información".

Para Misfud[19] la seguridad de la información indica que la información tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger, es así que la Seguridad de la Información se puede definir como "conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información".

Seguridad informática

Según Cano [20] la seguridad informática "es la distinción táctica y operacional de la seguridad. Es la forma como se detallan las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que, articulados con prácticas de tecnología de la información, establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo".

---

[18] CANO, Jeimy. La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes [en línea], 2011, vol. 5. Disponible en internet: https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx.

[19] MISFUD Elvira, Introducción a la seguridad informática. Ministerio de educación, cultura y deporte España, 26 de marzo de 2012. Disponible en internet: http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

[20] CANO, Jeimy. La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes [en línea], 2011, vol. 5. Disponible en internet: https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx

Para Villalón[21], La seguridad informática "consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio".

Sistema de gestión de la seguridad de la información (SGSI)

Según la ISO-IEC 27001[22], el SGSI es definido como "parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos".

Como requisito general, la organización debe establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta.

El establecimiento y gestión del SGSI se compone de:

- Definir el alcance y límites del SGSI de acuerdo a las características y especificaciones del negocio.
- Definir una política de SGSI de acuerdo a las características y especificaciones del negocio.
- Definir el enfoque organizacional para la valoración del riesgo.
- Identificar los riesgos.
- Analizar y evaluar los riesgos.
- Identificar y evaluar las opciones para el tratamiento de los riesgos.
- Seleccionar los objetivos de control para el tratamiento de los riesgos.

[21] VILLALÓN HUERTA Antonio, Seguridad de los sistemas de información. Octubre 2007

[22] Norma NTC ISO/IEC 27001. Sistema de gestión de la información, establecimiento y gestión del SGSI. Pág 4 – 6

- Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.
- Obtener autorización de la dirección para implementar y operar el SGSI.
- Elaborar una declaración de aplicabilidad

Todos estos elementos son importantes para llevar a cabo un adecuado establecimiento y gestión del SGSI para la empresa.

Norma ISO/IEC 27001

De acuerdo a lo establecido en la norma NTC ISO/IEC 27001[23], "esta norma se ha elaborado con el fin de brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI)". Esta norma además se puede usar para evaluar la conformidad por las partes interesadas, tanto internas como externas.

En la norma se promueve la adopción de un enfoque basado en procesos, para la gestión de la seguridad de la información, el cual hace énfasis en la importancia de:

a) comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información;

b) implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización;

c) el seguimiento y revisión del desempeño y eficacia del SGSI, y

d) la mejora continua basada en la medición de objetivos.

[23]Norma NTC ISO/IEC 27001. Generalidades. Pág I

Para el enfoque basado en procesos establecido anteriormente se adopta el modelo de procesos PHVA “Planificar-Hacer-Verificar-Actuar” el cual permite estructurar los procesos del SGSI tales como:

- Planificar (Establecer el SGSI): Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.

- Hacer (Implementar y operar el SGSI): Implementar y operar la política, los controles, procesos y procedimientos del SGSI.

- Verificar (hacer seguimiento y revisar el SGSI): Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad, reportar los resultados a la dirección, para su revisión.

- Actuar (mantener y mejorar el SGSI): Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

Figura 2. Ciclo PHVA

Fuente: PHVA: Safet YA. Procedimiento lógico y por etapas para la mejora continua. Disponible en internet: https://safetya.co/phva-procedimiento-logico-y-por-etapas/

En cuanto a la compatibilidad de la norma con otros sistemas de gestión, se encuentra alineada con la NTC-ISO 9001:2000 y la NTC-ISO 14001:2004, esto es con el fin de apoyar la implementación y operación consistentes e integradas con sistemas de gestión relacionados.

Norma ISO/IEC 27002

Según lo determinado en la norma ISO/IEC 27002[24], esta norma establece directrices para la seguridad de la información en las organizaciones y prácticas de gestión de la seguridad de la información incluyendo la selección, la implantación, y la gestión de los controles teniendo en consideración el entorno de riesgos de seguridad de la información de la organización.

Esta norma está diseñada para ser utilizada en organizaciones que pretendan:

a) Seleccionar controles en el proceso de implantación de un SGSI sistema de gestión de la seguridad basado en la Norma ISO/IEC 27001.

b) Implantar controles de seguridad de la información comúnmente aceptados.

c) Desarrollar sus propias directrices de seguridad de la información.

Análisis de riesgos

El análisis de riesgos según Sosa[25] puede ser cuantitativo o cualitativo:

Análisis de riesgos cuantitativo: este análisis se basa en asignar números reales y significativos a todos los elementos de los procesos que se relacionen con

[24] Extracto del documento UNE-EN ISO/IEC 27002, Objeto y campo de aplicación.

[25] SOSA, Johana. Análisis de Riesgos. [en línea]. 27 de enero de 2012. Disponible en internet: http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

controles, valor de los activos, amenaza y frecuencia de esta. Los pasos principales de este análisis son:

- Asignar un valor al activo
- Estimar la perdida potencial por amenaza
- Realizar un análisis de las amenazas
- Deducir el potencial total de pérdidas anuales por amenaza
- Reducir, transferir, evitar, o aceptar el riesgo.

Análisis de riesgos cualitativo: este proceso consiste en priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando la probabilidad de ocurrencia y combinándola con el impacto de dichos riesgos. El resultado de este análisis sirve de guía para definir la respuesta a los riesgos.

Evaluación de Riesgo

Según Ferrer[26] la evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Los dos puntos importantes a considerar son:

- La probabilidad de una amenaza.
- La magnitud del impacto sobre el sistema, la cual se mide por el nivel de degradación de uno o combinación de alguno de los siguientes elementos: confidencialidad, disponibilidad, integridad.

[26] FERRER, Rodrigo, Metodología de análisis de riesgo, Bogotá Colombia. 7 h. en línea]. Disponible en internet: http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_DE_ANALISIS_DE_RIESGO.pdf

Magerit

Magerit[27] significa Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las administraciones públicas. Esta, hace referencia al "Proceso de Gestión de los Riesgos", implementa este proceso dentro de un marco de trabajo para que se tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Esta metodología, persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

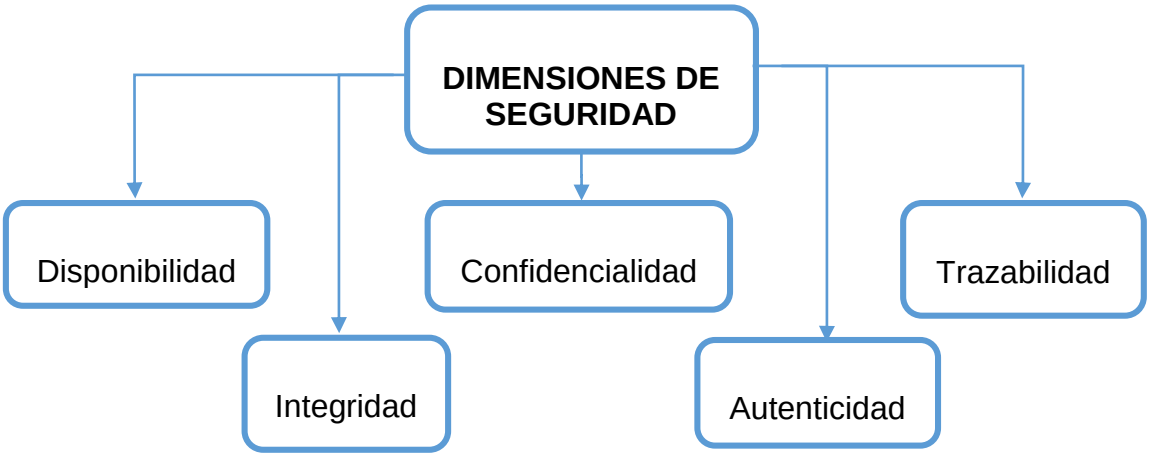
Magerit cuenta con las siguientes dimensiones de seguridad:

- Disponibilidad
- Integridad
- Confidencialidad
- Autenticidad

[27] MAGERIT, Introducción. En: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos: Libro I – Método. Madrid, octubre de 2012. Pág 7-8.

- Trazabilidad

Figura 3. Dimensiones de seguridad



Fuente: Autores del proyecto.

Octave [28]

Una evaluación efectiva de riesgos en la seguridad de la información considera tanto los temas organizacionales como los técnicos, examina cómo la gente emplea la infraestructura en forma diaria. La evaluación es de vital importancia para cualquier iniciativa de mejora en seguridad, porque genera una visión a lo ancho de la organización de los riesgos de seguridad de la información, proveyéndonos de una base para mejorar a partir de allí.

Para que una empresa comprenda cuáles son las necesidades de seguridad de la información, OCTAVE es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo.

[28] DUQUE OCHOA, Blanca Rubiela, Metodologías de Gestión de Riesgos 24h, Trabajo Final de auditoria, Universidad de Caldas, Facultad de Ingeniería [en línea]. Disponible en internet: http://docplayer.es/23365963-Metodologias-de-gestion-de-riesgos-octave-magerit-dafp-blanca-rubiela-duque-ochoa-codigo-auditoria-carlos-hernan-gomez.html

En contra de la típica consultoría focalizada en tecnología, que tiene como objetivo los riesgos tecnológicos y el foco en los temas tácticos, el objetivo de OCTAVE es el riesgo organizacional y el foco son los temas relativos a la estrategia y a la práctica.

Cuando se aplica OCTAVE, un pequeño equipo de gente desde los sectores operativos o de negocios hasta los departamentos de tecnología de la información (IT) trabajan juntos dirigidos a las necesidades de seguridad, balanceando tres aspectos: Riesgos Operativos, Prácticas de seguridad Y Tecnología.

Historia y evolución

OCTAVE apunta a dos aspectos diferentes: riesgos operativos y prácticas de seguridad. La tecnología es examinada en relación a las prácticas de seguridad, permitiendo a las compañías tomar decisiones de protección de información basados en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados a la información crítica.

El método OCTAVE permite la comprensión del manejo de los recursos, identificación y evaluación de riesgos que afectan la seguridad dentro de una organización.

Exige llevar la evaluación de la organización y del personal de la tecnología de la información por parte del equipo de análisis mediante el apoyo de un patrocinador interesado en la seguridad.

El método OCTAVE se enfoca en tres fases para examinar los problemas organizacionales y tecnológicos:

- Identificación de la información a nivel gerencial.
- Identificación de la información a nivel operacional.
- Identificación de la información a nivel de usuario final.

Estos tres pasos dan lugar a otros 5 procesos para completar los 8 puntos de los que consta OCTAVE:

Consolidación de la información y creación de perfiles de amenazas.

- Identificación de componentes claves.
- Evaluación de componentes seleccionados.

- Análisis de riesgos de los recursos críticos.
- Desarrollo de estrategias de protección.

Descripción general de Octave

Hay tres métodos OCTAVE:

Los métodos de OCTAVE se basan en los criterios del estándar con un enfoque en la práctica y evaluación de la seguridad basada en la información de riesgo. Estos criterios establecen los principios fundamentales y los atributos de gestión de riesgos que son utilizados por los métodos de OCTAVE.

El método fue desarrollado teniendo en cuenta grandes organizaciones de 300 ó más empleados, pero el tamaño no fue la única consideración. Por ejemplo, las grandes organizaciones suelen tener una jerarquía de múltiples capas y es probable que mantengan su propia infraestructura informática, junto con la capacidad interna para ejecutar herramientas de evaluación de la vulnerabilidad e interpretar los resultados en relación a los activos críticos.

El método utiliza una ejecución en tres fases que examina las cuestiones organizacionales y tecnológicas, monta una visión clara de la organización y sus necesidades de información y seguridad de la misma. Se compone de una serie de talleres, facilitados o llevados a cabo por un equipo de análisis interdisciplinario de tres a cinco personas de la propia organización. El método aprovecha el conocimiento de múltiples niveles de la organización, centrándose en:

- Identificar los elementos críticos y las amenazas a esos activos.
- La identificación de las vulnerabilidades, tanto organizativas y tecnológicas, que exponen a las amenazas, creando un riesgo a la organización.
- El desarrollo de una estrategia basada en la protección de prácticas y planes de mitigación de riesgos para apoyar la misión de la organización y las prioridades.

Estas actividades son apoyadas por un catálogo de buenas prácticas, así como encuestas y hojas de cálculo que se puede utilizar para obtener y captar información durante los debates y la solución de sesiones-problema.

DAFP

El tema de la Administración de Riesgos ya no es un tema nuevo para las entidades públicas, en virtud de que el Estado colombiano mediante el Decreto 1537 de 2001 estableció que todas las entidades de la Administración Pública deben contar con una política de Administración de Riesgos tendiente a darles un manejo adecuado a los riesgos, con el fin de lograr de la manera más eficiente el cumplimiento de sus objetivos y estar preparados para enfrentar cualquier contingencia que se pueda presentar.

En este sentido, las entidades de la Administración Pública no pueden ser ajenas al tema de los riesgos y deben buscar cómo manejarlos y controlarlos, partiendo de la base de su razón de ser y de su compromiso con la sociedad; por esto se debe tener en cuenta que los riesgos no solo son de carácter económico y están directamente relacionados con entidades financieras o con lo que se ha denominado riesgos profesionales, sino que hacen parte de cualquier gestión que se realice.

Historia y evolución

A través del Decreto 1599 del 20 de mayo del 2005 se adoptó el Modelo Estándar de Control Interno para todas las entidades del Estado de las que habla el artículo 5º de la Ley 87 de 1993; este modelo presenta tres Subsistemas de Control: el Estratégico, el de Gestión y el de Evaluación. La Administración del Riesgo ha sido contemplada como uno de los componentes del Subsistema de Control Estratégico y ha sido definida en el Anexo Técnico “como el conjunto de Elementos de Control que, al interrelacionarse, permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública auto controlar aquellos eventos que pueden afectar el cumplimiento de sus objetivos”.

Objetivos de DAFP

General

Fortalecer la implementación y desarrollo de la política de la administración del riesgo a través del adecuado tratamiento de los riesgos para garantizar el

cumplimiento de la misión y objetivos institucionales de las entidades de la Administración Pública.

Específicos

- Generar una visión sistémica acerca de la administración y evaluación de riesgos, consolidada en un Ambiente de Control adecuado a la entidad y un Direccionamiento Estratégico que fije la orientación clara y planeada de la gestión dando las bases para el adecuado desarrollo de las Actividades de Control.

- Proteger los recursos del Estado, resguardándolos contra la materialización de los riesgos.

- Introducir dentro de los procesos y procedimientos las acciones de mitigación resultado de la administración del riesgo.

- Involucrar y comprometer a todos los servidores de las entidades de la Administración Pública en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.

- Propender a que cada entidad interactúe con otras para fortalecer su desarrollo y mantener la buena imagen y las buenas relaciones.

- Asegurar el cumplimiento de normas, leyes y regulaciones.

Pruebas de penetración[29]

Metodología del test de penetración. La metodología utilizada está basada en un test del tipo Black-Box, el cual consiste en que partiendo únicamente de la información pública de la empresa se intenta realizar una intrusión mediante los servicios externos. Los métodos utilizados son los siguientes:

Reconocimiento Pasivo: Se utilizan técnicas de footprinting para obtener información sobre la empresa, tecnologías utilizadas y servicios publicados. El objetivo en esta etapa además de recopilar información para realizar el ataque es

[29] Coppola y García. Test de Intrusión. [en línea]. Montevideo. Disponible en internet: http://www.cyg.com.uy/documentos/test_de_intrusion.pdf

demostrar a la organización que tipo de información se puede obtener públicamente acerca de la empresa en sí, sus sistemas y tecnologías, ya que generalmente se obtiene información detallada que habitualmente subestimada.

Reconocimiento Activo: Se utilizan técnicas de escaneos de puerto, servicios y sistemas operativos para obtener información sobre dispositivos utilizados y que servicios/aplicaciones se encuentran. Llegado a este punto hacemos un mapa de red con los dispositivos y servicios detectados que luego vamos a adjuntar en el reporte para que 6 la organización sea consciente de la información con la que cuenta un atacante

Escaneo de Vulnerabilidades: En base a la información obtenida anteriormente se procede a buscar vulnerabilidades en los sistemas detectados. Luego cada una de estas vulnerabilidades serán especificadas en el reporte detallando una explicación, gravedad de las mismas y posibles soluciones.

Explotación de Vulnerabilidades: Se procede a explotar las vulnerabilidades encontradas con el objetivo de obtener acceso y elevar privilegios en los sistemas objetivos y/o obtener información confidencial. El objetivo es que la organización conozca que metodología puede utilizar un atacante para penetrar las defensas, que datos puede obtener y que daño es capaz de hacer a la organización.

Expansión del Acceso: A partir de un sistema comprometido se intentan acceder a otros sistemas dentro de la red mediante técnicas de pivoting y nuevos escaneos internos. El objetivo en este paso es que una vez encontrada una brecha que nos permita estar dentro de un sistema vulnerable, evaluar qué posibilidades de acceder desde dicho 7 sistema hacía otros sistemas dentro de la red que generalmente son más críticos e importantes para la organización que el sistema vulnerado. De esto modo además de los sistemas de borde podemos evaluar la seguridad perimetral y relevar que importancia puede tener asegurar todos los sistemas de la red y no solo los más críticos.

Mantenimiento de acceso: Una vez obtenido el acceso a los sistemas o red en general se intenta crear una vía de acceso permanente, de modo de volver periódicamente a conectarse a dichos sistemas sin ser detectado y sin explotar las vulnerabilidades nuevamente. Desde modo podemos evaluar las facilidades que puede tener una atacante para entrar y salir de la organización una vez comprometido el sistema de modo de poder implementar políticas que dificulten esta tarea. 7. Borrado de huellas: Se intenta eliminar los registros para que no queden rastros de la intrusión. El objetivo en este paso es el de probar la capacidad de los sistemas para mantener logs y registros de accesos no autorizados.

Pruebas de redes[30]

Análisis de vulnerabilidades con UpGuard: UpGuard es un escáner web que permite identificar vulnerabilidades a aplicaciones web realizando pruebas de pishing, presencia de malware, falsa autenticación directamente en la aplicación y en las comunicaciones como registro de servidores DNS, puertos, servicios, etc.

Análisis de vulnerabilidades con Nessus: Nessus scanner es una herramienta de la empresa Tenable Network Security, que permite identificar y analizar vulnerabilidades mediante varias opciones evaluando cada infraestructura de red. Entre sus opciones se encuentran escaneos para encontrar vulnerabilidades a redes, escaneos a host y aplicaciones web, como también escaneos a servicios en la nube.

Pruebas a base de datos[31]

Dentro de la seguridad informática, la disponibilidad es un factor muy importante que normalmente se le suele menospreciar. Entendemos por disponibilidad, a la garantía de que los usuarios autorizados puedan acceder a la información y recursos de red, cuando los necesiten. La disponibilidad es un factor imprescindible un servidor de bases de datos.

Dbstress: es una herramienta de stress test y rendimiento de base de datos de código abierto escrita en Scala y Akka. Esta herramienta, ejecuta una consulta de base de datos (utilizando un controlador JDBC específico de la base de datos) cierto número de veces en paralelo (posiblemente en varios hosts de bases de datos) y genera un archivo CSV con resultados resumidos.

Elemento de configuración de nivel superior: es un escenario, que consiste en al menos una unidad. Una unidad representa una operación de base de datos particular, junto con su configuración. Todas las unidades configuradas dentro de un escenario se ejecutan en paralelo, independientemente unas de otras y sus resultados también se informan por separado. A menos que se necesite hacer algunas pruebas más avanzadas, como conectarse a la base de datos con

[30] CORTES CAMACHO Jesús German. Auditoria a la seguridad de la red de datos de la empresa panavias s.a, San Juan De Pasto,2016, 197h, Trabajo de grado, Universidad Abierta Y Distancia “Unad”, Facultad De Ciencias Básicas e Ingeniería

[31] Herramienta para Stress test de base de datos, [en línea]. Noticias Seguridad. 7 de diciembre de 2017. [citado en 2018]. Disponible en internet: http://noticiasseguridad.com/seguridad-informatica/herramienta-para-stress-test-de-bases-de-datos-2/

diferentes usuarios a diferentes esquemas, está bien tener un escenario con una sola unidad.

La configuración de la unidad consiste en:

- Nombre de la unidad: debe ser una cadena alfanumérica.
- Descripción (opcional).
- Consulta de base.
- URI de conexión.
- Nombre de clase de controlador JDBC: opcional, solo se especifica si no se puede detectar automáticamente
- Nombre de usuario.
- Contraseña de la base de datos: opcional si se proporciona en la línea de comando
- Número de conexiones de bases de datos paralelas: más conocido como “PAR”.
- Cuántas veces se debe repetir la consulta, más conocido como “REP”.
- Tiempo de espera de inicialización de la conexión (opcional).

La ejecución de la prueba consta de dos fases básicas: fase de inicialización de la conexión y fase de ejecución de la consulta. En la fase de inicialización de la conexión, cada unidad genera una llamada unidad de ejecución (PAR). Cada ejecución de unidad abre una conexión de base de datos. En la fase de ejecución de consultas, cada ejecución de unidad envía la consulta configurada (REP) secuencialmente a la base de datos. Por lo tanto, cada unidad envía la consulta a la base de datos es el resultado de PAR*REP.

Varios tipos de errores pueden ocurrir durante la ejecución del escenario, dos categorías más importantes de errores son los errores de inicialización de conexión y de consulta. Cuando falla la inicialización de una conexión (debido a una excepción o a exceder el tiempo de espera), dbstress no procede a la fase de ejecución de la consulta y finaliza inmediatamente. Los errores de consulta, por otro lado, no detienen el escenario, pero se informan como fallas en el CSV resultante.

Marco conceptual

A continuación, se definen algunos términos que serán utilizados y nombrados en el desarrollo del proyecto.

Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Vulnerabilidad: toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Las amenazas pueden ser: de origen natural, de entorno (de origen industrial), defectos de las aplicaciones, causadas por las personas de forma accidental, causadas por las personas de forma deliberada.

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro.

Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

Confidencialidad: la información debe llegar solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

Integridad: mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Disponibilidad: es la disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Trazabilidad: aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

Marco legal

El presente proyecto esta soportado en un contexto legal, ya que cada vez que se hable de seguridad de la información, toda organización debe seguir un estricto uso y cumplimiento de las leyes, normas y decretos aplicables a proyectos de este tipo.

Entre las principales leyes que el presente trabajo debe cumplir están toda ley que vele por el cumplimiento de la protección de datos personales, delitos informáticos y protección de la información y la ley de derecho de autor.

Decreto 1377 de 2013: "Protección de Datos, decreto por el cual se reglamenta parcialmente la ley 1581 de 2012**".**

Ley estatutaria 1581 de 2012: "Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional"

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

- Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

- Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

- Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben

presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

- Crea una especial protección a los datos de menores de edad.

- Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

- Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

- Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

- Crea el Registro Nacional de Bases de Datos.

- Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

Decreto 2693 de 2012: "Por el cual se establecen los lineamientos generales de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones"

Ley 1341 del 30 de julio de 2009: "Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"

Ley estatutaria 1266 del 31 de diciembre de 2008: "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"

Ley 603 de 2000: “Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales”

Ley 1273 del 2009. Esta Ley planteo nuevos tipos penales en relación con los delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “De la Protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. El sentido de esta ley está en que al mismo tiempo que crecen los avances tecnológicos a su vez aumenta los bienes de aquellos que se apropian de forma ilegal del patrimonio de otros por medio de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para hacer posible las transferencias electrónicas de fondos mediante la manipulación de programas y afectación de los cajeros automáticos. No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

Esta adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

Para el presente trabajo esta ley deja claro que en cada avance tecnológico que se dé habrá un ataque para el mismo, y que llegado el momento es comprensible tener presente en una auditoria todos los hallazgos que se encuentren y que de cierta forma no sean agradables para terceros estos pueden ser violados pero que a su vez una acción de este tipo tiene su penalización correspondiente.

Para el presente trabajo esta ley deja claro que en cada avance tecnológico que se dé habrá un ataque para el mismo, y que llegado el momento es comprensible tener

presente en una auditoria todos los hallazgos que se encuentren y que de cierta forma no sean agradables para terceros estos pueden ser violados pero que a su vez una acción de este tipo tiene su penalización correspondiente.

Ley de derechos de autor. Determina que todo autor desde el momento de la creación, dispone de unos derechos patrimoniales. Esto significa que todo creador o quien lo haya contratado o quien sea que haya adquirido derechos de explotación sobre una obra, dispone del derecho exclusivo de autorizar o prohibir cualquier forma de explotación. Mientras alguien sea titular o propietario de unos derechos, puede administrar y explotar su obra como a bien tenga. El problema es que pesar de que esto en teoría es viable, en la práctica y ante diversas formas de explotación, le queda absolutamente imposible a un creador titular de sus derechos, hacer esa gestión individual.

Respetar el trabajo de otros haciendo mención de ellos en caso de necesitarlo es una forma de respeto por quien hizo el trabajo y aun para el que pretende hacer algo nuevo o una mejora.

Marco contextual

La ***E.S.E. Centro Hospital Luis Antonio Montero*** se encuentra ubicada en el barrio La Unión del municipio de Potosí al sur del departamento de Nariño. Dista a 140 kilómetros de la capital de San Juan de Pasto y a 9 kilómetros de la ciudad de Ipiales, con una superficie de 397 kilómetros cuadrados situada a 2.796 metros sobre el nivel del mar, presenta dos pisos térmicos: frío y páramo con una temperatura de 12 grados centígrados promedio.

El municipio de Potosí se encuentra políticamente dividido en: 3 corregimientos, 20 veredas y diez barrios; cuenta con una población total de 12.137 y en la zona urbana de 2151 habitantes.

Figura 4. Ubicación municipio de Potosí, Nariño

Fuente: Página E.S.E Centro Hospital Luis Antonio Montero, Acerca de la entidad, Donde estamos. Disponible en internet: http://www.eseluisantoniomonteropotosi.gov.co/es/acerca-de-la-entidad/donde-estamos

Misión

Somos una Empresa Social del Estado, que presta servicios de salud del primer nivel de atención, con calidad, calidez y eficiencia, de acuerdo a las necesidades de los usuarios, y de las Familias Potositanas, contando con la tecnología, sostenibilidad económica y Social y un equipo humano idóneo para garantizar el bienestar y satisfacción de los usuarios y contribuir al desarrollo de Nuestra Región.

Visión

Seremos una empresa prestadora de servicios de salud de primer nivel de atención que aporte al mejoramiento del Bienestar y calidad de vida de la poblAción, reconocida en el ámbito local y regional, por la calidad en la atención en salud, su gestión administrativa, financiera, y el mejoramiento continuo de procesos, convirtiéndola en una entidad modelo entre los prestadores de salud.

Objetivos y funciones

Los Principios Corporativos reafirman el compromiso y orientan los valores éticos de los funcionarios de la E.S.E., Centro Hospital Luis Antonio Montero con el fin de brindar confianza a todos sus grupos de interés, externos e internos, de tal forma que se garantice el cumplimiento de los principios generales de Ética y Buen Gobierno dentro de la Institución.

Universalidad: El Centro Hospital Luis Antonio Montero E.S.E. reconoce que el ciudadano siempre constituirá su razón de ser, por tanto prestara sus servicios, sin ninguna discriminación y en todas las etapas de la vida.

Integralidad: Se reconocerá la prioridad en la atención continua y oportuna a las familias y a las personas, en su contexto Biopsicosocial, con servicios de óptima calidad humana, científica y técnica conforme a criterios de necesidad verificables.

Eficiencia: El manejo óptimo y transparente de sus recursos tecnológicos, financieros y del talento humano, tendrá en cuenta la relación entre los beneficios y los costos generados.

Eficacia: La solución de aquellos problemas de salud de la población Usuaria, que correspondan a sus principales necesidades y expectativas, será nuestra prioridad.

Efectividad: mediante la combinación de la eficacia y eficiencia lograr un impacto

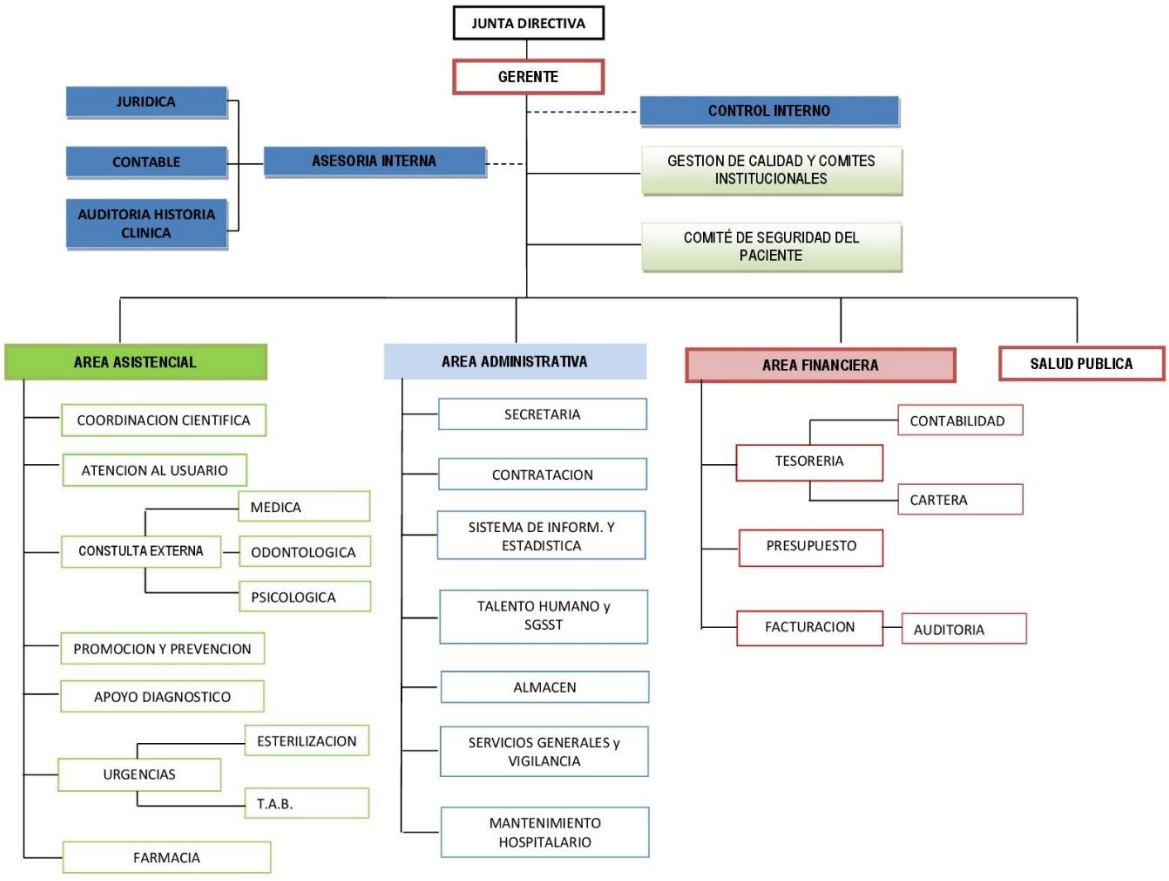
positivo en el estado de salud de la Comunidad Potositana.

Calidad Humana: Atender y servir a nuestros usuarios, con humanismo y atención personalizada.

Equidad: Entendido como la virtud de dar a cada uno lo que le corresponde en la E.S.E. Centro Hospital Luis Antonio Montero atendiendo a las personas y grupos de la población expuestos a mayores riesgos para su Salud, con el fin de brindarles aquella protección especial que esté a nuestro alcance.

La E.S.E. Centro Hospital Luis Antonio Montero posee el siguiente organigrama:

Figura 5. Organigrama Ese Centro Hospital Luis Antonio Montero



Fuente: Página E.S.E Centro Hospital Luis Antonio Montero, Acerca de la entidad, Estructura organizacional. Disponible en internet: http://www.eseluisantoniomonteropotosi.gov.co/es/acerca-de-la-entidad/estructura-organizacional

Metodología

Tipo de investigación

El tipo de investigación del proyecto es descriptivo, ya que precisa las características más importantes de la seguridad informática y se obtuvo datos completos y exactos; por lo tanto, el proyecto de investigación tomó las medidas necesarias para la protección contra errores y vulnerabilidades de la seguridad informática, teniendo en cuenta cada fase del proceso.

La investigación descriptiva según Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010, p. 80) "Busca especificar las propiedades, características y los perfiles de personas, grupos, comunidades, procesos, objetos, o cualquier otro fenómeno que se someta a un análisis"[32].

Paradigma

Según los autores Tesch y Krippendorff (1992) "consideran el análisis cuantitativo como una descripción objetiva y sistemática del contenido manifiesto de la información, con el propósito de realizar inferencias válidas y replicables"[33]. De acuerdo a lo anterior el paradigma de investigación del proyecto fue de tipo cuantitativo porque gracias a las escalas de medición, las técnicas estadísticas y el análisis de datos; se determinó el grado de confidencialidad, confiabilidad e integridad de la información. Para obtener un conocimiento lo más objetivo posible del estado de la seguridad de informática de la entidad de salud.

---

[32] HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA LUCIO, Pilar. Metodología de la investigación: McGraw-Hill Interamericana; México, 2010. p.80

[33] TESCH, R. Qualitative research: analysis types and software tolos: The Falm Press; New York, 1992

KRIPPENDORFF, K. Content analysis. An introduction to its methodology: Sage; Beverly Hills, 1980

Enfoque

El enfoque para esta investigación es el empírico analítico, según Restrepo (1999. p. 8)[34] Empírico se refiere a la denominada investigación científica clásica, que consiste en plantear situaciones problemáticas a partir de hipótesis de trabajo para demostrarlas, además busca el dominio y conocimiento a través de la experiencia y se interesa por controlar y predecir los hechos que se estudian para ser modificados.

Y, analítico ya que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Fue necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método permitió conocer más del objeto de estudio, con lo cual se pudo: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías.

De acuerdo a esto se tomó en cuenta las experiencias propias de los usuarios en el manejo de los diferentes activos informáticos presentes en la entidad de salud y el análisis de los procedimientos que se llevan a cabo por parte de los usuarios del sistema con el fin establecer las vulnerabilidades, amenazas y riesgos a los que se encuentra expuesto el sistema de información de la E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO de POTOSI NARIÑO.

[34] RESTREPO, María Consuelo. Producción de textos educativos. [en línea]. Ediciones Bogotá D.C; Colombia. Pág 8. ISBN: 978-958-20-0850-4. Disponible en internet: http://biblioteca.salamandra.edu.co/libros/Produccion%20de%20textos%20educativos.pdf

Población

La población para este proyecto fueron todos los usuarios que interactúan con el sistema de información de la E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO de acuerdo a los módulos siguientes:

- Módulo de administración del sistema.
- Módulo de Historias clínicas.
- Módulo de Control de Facturación.
- Módulo de Citas médicas.
- Módulo de Salidas y reportes.

De acuerdo a los módulos planteados anteriormente, se cuenta con la siguiente relación de usuarios del sistema.

Cuadro 1. Población

Talento humano	Vinculados
Ingeniero de sistemas	1
Médicos generales	6
Jefes de Enfermería	4
Auxiliares de Enfermería	26
Bacteriólogas	2
Regentes	3
Odontólogos	2
Higienistas	2
Auxiliares de Odontología	2
Psicología	2
Ingeniero Biomédico	1
Total, asistencial	51

Fuente: Esta investigación.

Muestra

La investigación usó un muestreo intencional ya que permite realizar una selección de usuarios de acuerdo al grado de experiencia y conocimiento en la entidad, para así obtener una información veraz y precisa.

Según Glass y Stanley (1996) "El muestreo intencional es un procedimiento que permite seleccionar los casos característicos de la población limitando la muestra a estos casos. Se utiliza en situaciones en las que la población es muy variable y consecuentemente la muestra es muy pequeña"[35].

Instrumentos de recolección de información

Para el proyecto se usó diferentes instrumentos de recolección de información, mediante los cuales se obtuvo un estado actual del hospital y además permitió realizar el análisis de riesgos que permitió definir las medidas y controles necesarios; para el desarrollo de esta investigación se utilizaron los siguientes:

Observación directa: Según Tamayo (2001) la observación directa "es aquella en la cual el investigador puede observar y recoger datos mediante su propia observación"[36].

Por otra parte, de acuerdo con Méndez (2001) "la observación directa es el proceso mediante el cual se perciben deliberadamente ciertos rasgos existentes en la realidad por medio de un esquema conceptual previo y con base en ciertos propósitos definidos generalmente por una conjetura que se quiere investigar"[37].

---

[35] GLASS, G y STANLEY, J.S. Métodos Estadísticos Aplicados a las ciencias sociales: Prentice-Hall; México, 1996

[36] TAMAYO, Mario. El Proceso de la investigación científica: Limusa; México, 2001

[37] MÉNDEZ, C. Metodología, Diseño y Desarrollo del Proceso de Investigación: Mc Graw-Hill; Caracas, 2001

Haciendo uso de este instrumento se observan características, condiciones, conductas y actividades en la entidad. En el centro hospital se implementó esta técnica para colocarse en contacto con los sistemas de información existentes, y con las personas responsables de la información.

Entrevistas: De acuerdo con Barrera (2008) **"**la técnica de la entrevista es la información que se recoge solicitándola a otra. El investigador no puede tener la experiencia directa del evento; es otro quien la tiene, la información se obtiene dialogando"[38].

En el proyecto fue valioso ya que se pudo entablar conversaciones, obteniendo información desde el punto de vista de cada funcionario sobre su área de trabajo.

Check-List: Según Bichachi (2013) "Se entiende por lista de chequeo (check-list) a un listado de preguntas, en forma de cuestionario que sirve para verificar el grado de cumplimiento de determinadas reglas establecidas a priori con un fin determinado"[39]. En el proyecto se utilizó este instrumento como técnica de verificación de conformidades y no conformidades en el manejo de la seguridad de la información en las áreas del hospital.

[38] BARRERA Hurtado de, Jacqueline. El Proyecto de Investigación: Sypal; Caracas, 2008.

[39] BICHACHI, Diana Susana. El uso de las Listas de Chequeo (CheskList) como herramienta para controlar la calidad de la ley. [en línea]. Disponible en internet: http://www.claudiabernazza.com.ar/ssgp/html/pdf/check_list.pdf

1. RESULTADOS DE LA INVESTIGACIÓN

1.1 Inventario de activos

Los activos son recursos necesarios e importantes que permiten que la E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO desarrolle y cumpla con las actividades, metas y objetivos propuestos en la entidad de una manera adecuada; por esta razón se encuentró la necesidad de protegerlos de riesgos y amenazas para que se dé una continuidad del negocio estable; de esta manera resguardar los activos de estos sucesos fue necesario realizar un inventario de todos los activos con los que cuenta la entidad. Es por esto que con la ayuda de la metodología Magerit se han clasificado en los siguientes grupos:

- Datos / información **[D]**
- Servicios **[S]**
- Software **[SW]**
- Equipos informáticos **[HW]**
- Redes de comunicación **[COM]**
- Soportes de información (almacenamiento electrónico y no electrónico) **[MEDIA]**
- Equipamiento auxiliar **[AUX]**
- Instalaciones **[L]**
- Personal **[P]**

La clasificación de cada activo de la entidad se realizó basándose en parámetros establecidos en la metodología, como son los siguientes:

- Determinar el grupo al que pertenece el activo.
- Determinar el código y nombre del activo.

Independientemente a lo mencionado, se asignó un código que detalle el activo identificado y se da una breve descripción del uso que posee en la empresa.

En el siguiente cuadro se describe los activos encontrados en la E.S.E CENTRO HOSPITAL LUIS ANTONIO MONTERO, de acuerdo a lo especificado anteriormente.

Cuadro 2. Clasificación de activos MAGERIT

ACTIVOS MAGERIT				
Grupo de activos	**Código de activo MAGERIT**	**Nombre de activo MAGERIT**	**Código activo**	**Activo de acuerdo a la entidad**
[D] Datos / Información	[backup]	Copias de Respaldo	[copias_seguridad]	Archivo de Copias de seguridad de la información
	[password]	Credenciales	[pass_empleados]	Contraseñas de acceso de funcionarios
[S] Servicios	[ipm]	Gestión de privilegios	[gest_privilegios]	Manejo de privilegios de acuerdo a los roles dentro de la entidad.
[SW] Software	[office]	Ofimática	[oficce]	Paquete de Office versión 2016
	[av]	Antivirus	[antivirus]	Antivirus Eset NOD32, Avast
	[os]	Sistema operativo	[os_servidor]	Sistema operativo servidor
	[os]	Sistema operativo	[os_Pcs]	Sistemas operativos de los usuarios
	[browser]	Navegador web	[navegador]	Navegador web Google Chrome, Mozilla Firefox
	[App]	Aplicación	[info_salud]	Aplicación para la gestión de información de la entidad
[HW] Equipos Informáticos	[mid]	Equipos de trabajo conectados a través de red	[pc_trabajadores]	Equipos de escritorio
	[print]	Equipos de impresión	[impresoras]	Impresoras
	[router]	Enrutadores	[router]	Router
	[switch]	Switch	[switch]	Switch
	[data]	Servidor	[servidor]	Servidor
[COM] Redes de Comunicaciones	[wifi]	Red inalámbrica	[r_wifi]	Red Inalámbrica
	[LAN]	Red local	[r_Local]	Red de área local
	[Internet]	Internet	[internet]	Internet

Fuente: Esta investigación.

Cuadro 2. (Continuación)

ACTIVOS MAGERIT				
Grupo de activos	**Código de activo MAGERIT**	**Nombre de activo MAGERIT**	**Código activo**	**Activo de acuerdo a la entidad**
[MEDIA] Soportes de Información (Almacenamiento Electrónico)	[disk]	Discos	[media_dd]	Almacenamientos en Disco Duro
[MEDIA] Soportes de Información (Almacenamiento No Electrónico)	[printed]	Material impreso	[media_hclinicas]	Carpetas que contienen información de soporte, sobre el historial clínico de los pacientes
[AUX] Equipamiento Auxiliar	[ups]	Sistemas de alimentación ininterrumpida	[ups]	UPS computadores
	[gen]	Generadores eléctricos	[gen_electricos]	Planta de energía
	[cabling]	Cableado estructurado	[cab_estructurado]	Cableado estructurado
[L] Instalaciones	[building]	Edificio	[edf_entidad]	Instalación física de la entidad (Hospital Luis Antonio Montero)
[P] Personal	[ui]	Usuarios internos	[funcionarios]	Funcionarios de recepción, área técnica, administrativa y archivo
	[adm]	Administradores de sistemas	[admin_sist]	Administrador de sistemas

Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO A. Documento unificado Magerit, hoja Activos Magerit.**

1.2 Valoración cualitativa de los activos

De acuerdo a los activos que se encuentran en la entidad fue evidente que cada uno de ellos tienen más o menos importancia y que de acuerdo a algún imprevisto que se pueda presentar estos pueden llegar a tener una consecuencia diferente; es por esto que se realizó una valoración cualitativa a cada uno de ellos en cuanto a las dimensiones de seguridad mencionadas en la metodología MAGERIT, las cuales son:

- Autenticidad
- Confiabilidad
- Integridad
- Disponibilidad
- Trazabilidad

La metodología proporciona los siguientes interrogantes ligados a cada dimensión y establece un ejemplo sobre a qué tipo de activo puede hacer referencia. La respuesta a cada una de estas preguntas permitió realizar una valoración apropiada a cada uno de los activos.

Autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

(Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar))

Confidencialidad: ¿qué daño causaría que lo conociera quien no debe? (Esta valoración es típica de datos)

Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? (Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos)

Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? (Esta valoración es típica de los servicios)

Trazabilidad del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

Trazabilidad del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Además de lo mencionado, los criterios de valoración establecidos para calificar cada dimensión han sido simplificados de la tabla original de los criterios de valoración de la metodología MAGERIT, los cuales son los siguientes.

Cuadro 3. Criterios de valoración.

Valor		Criterio
MA	Muy alto	Daño muy grave
A	Alto	Daño grave
M	Medio	Daño importante
B	Bajo	Daño menor
MB	Muy bajo	Irrelevante a efectos prácticos

Fuente: Adaptación de MAGERIT versión 3, libro 2 catálogos de elementos. Página 19

A fin de dar un ejemplo de cómo se realiza este proceso, se obtiene la valoración cualitativa del activo Copias de seguridad, que se encontró en el grupo de activos de Datos e Información [D], para cada dimensión se estableció los siguientes argumentos que determinan las calificaciones otorgadas a continuación.

- **Autenticidad** Valoración: MA
  Es importante tener en cuenta que en la copia de respaldo los datos no deben ser manipulados (deben ser igual a su origen) y que quien acceda a los datos para la realización de las copias debe ser la persona autorizada.

- **Confidencialidad** Valoración: MA
  El acceso y uso de la copia de respaldo solo deben tener las personas autorizadas, de lo contrario puede haber fugas de información.

- **Integridad** Valoración: MA

Es importante que la información que se encuentra contenida en las copias de seguridad no se encuentre manipulada, dañada o incompleta; ya que afectaría los procesos de la entidad en caso de ser necesaria.

- **Disponibilidad** Valoración: MA
  Las copias de seguridad deben estar disponibles en cualquier momento ya que son quienes ayudan en caso de pérdida o daño de la información primaria.

- **Trazabilidad** Valoración: MA
  Es importante determinar en qué momento y quien realiza las copias de seguridad, además de quien puede acceder a ellas; ya que esto permite identificar incidentes y de acuerdo a esto vigilar personas que intervengan en ello o también dar posibles soluciones o mejoras a los procesos que relacionen al activo.

En la siguiente tabla se realiza la valoración cualitativa de los activos establecidos para la ESE Centro Hospital Luis Antonio Montero de acuerdo a cada una de las dimensiones.

Cuadro 4. Valoración cualitativa de activos MAGERIT

VALORACIÓN CUALITATIVA DE ACTIVOS MAGERIT				**Dimensión de Seguridad**				
Grupo de Activos	**Código grupo de activo MAGERIT**	**Nombre grupo de activo MAGERIT**	**Código Activo**	**Autenticidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Trazabilidad**
[D] Datos / Información	[backup]	Copias de Respaldo	[copias_seguridad]	MA	MA	MA	MA	MA
	[password]	Credenciales	[pass_empleados]	A	MA	A	A	A
[S] Servicios	[ipm]	Gestión de privilegios	[gest_privilegios]	A	A	A	A	A

Fuente: Esta investigación.

Cuadro 4. (Continuación)

VALORACIÓN CUALITATIVA DE ACTIVOS MAGERIT				Dimensión de Seguridad				
Grupo de Activos	**Código grupo de activo MAGERIT**	**Nombre grupo de activo MAGERIT**	**Código Activo**	**Autenticidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Trazabilidad**
[SW] Software	[Oficce]	Ofimática	[oficce]	B	B	B	B	B
	[av]	Antivirus	[antivirus]	M	B	A	A	B
	[os]	Sistema operativo	[os_servidor]	MA	MA	MA	MA	A
	[os]	Sistema operativo	[os_Pcs]	M	B	A	A	B
	[browser]	Navegador web	[navegador]	B	B	MB	B	MB
	[App]	Aplicación	[info_salud]	MA	MA	MA	MA	MA
[HW] Equipos Informáticos	[mid]	Equipos de trabajo conectados a través de red	[pc_trabajadores]	B	B	M	A	B
	[print]	Equipos de impresión	[impresoras]	B	B	M	A	B
	[router]	Enrutadores	[router]	B	B	A	A	B
	[switch]	Switch	[switch]	B	B	A	A	B
	[data]	Servidor	[servidor]	A	A	MA	MA	A
[COM] Redes de Comunicaciones	[wifi]	Red inalámbrica	[r_wifi]	M	A	M	A	B
	[LAN]	Red local	[r_Local]	M	A	M	A	B
	[Internet]	Internet	[internet]	B	B	M	A	B
[MEDIA] Soportes de Información (Alm. Electrónico)	[disk]	Discos	[media_dd]	M	A	A	A	M

Fuente: Esta investigación.

Cuadro 4. (Continuación)

VALORACIÓN CUALITATIVA DE ACTIVOS MAGERIT				Dimensión de Seguridad				
Grupo de Activos	**Código grupo de activo MAGERIT**	**Nombre grupo de activo MAGERIT**	**Código Activo**	**Autenticidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Trazabilidad**
[MEDIA] Soportes de Información (Alm. No Electrónico)	[printed]	Material impreso	[media_hclinicas]	A	A	A	A	M
[AUX] Equipamiento Auxiliar	[ups]	Sistemas de alimentación ininterrumpida	[ups]	MB	MB	M	M	B
	[gen]	Generadores eléctricos	[gen_electricos]	MB	MB	M	M	B
	[cabling]	Cableado estructurado	[cab_estructurado]	B	MB	A	A	B
[L] Instalaciones	[building]	Edificio	[edf_entidad]	MB	MB	A	A	B
[P] Personal	[ui]	Usuarios internos	[funcionarios]	A	B	A	M	M
	[adm]	Administradores de sistemas	[admin_sist]	A	B	A	MA	A

Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO A. Documento unificado Magerit, hoja Valoración Cualitativa.**

1.3 Valoración cuantitativa de los activos

La valoración cuantitativa de los activos es un valor equivalente numérico acorde a la valoración cualitativa asignada anteriormente. Para esto se debió tener en cuenta el siguiente cuadro adaptado de la tabla de MAGERIT.

Cuadro 5. Escala de valoración cuantitativa

Valor		Calificación activo
MA	5	Critico
A	4	Importante
M	3	Apreciable
B	2	Bajo
MB	1	Despreciable

Fuente: Adaptación de MAGERIT versión 3, libro 2 catálogos de elementos. Página 19

Basándose en las escalas de valoración mencionadas; por cada dimensión y valoración cualitativa dada a cada uno de los activos se debe asignar el valor numérico correspondiente, posteriormente se debió promediar las valoraciones y de acuerdo al valor obtenido se determina la relevancia que tiene el activo en la E.S.E Centro Hospital Luis Antonio Montero.

Como ejemplo de lo explicado anteriormente se toma el activo copias de seguridad, del cual ya se había identificado las valoraciones cualitativas para cada dimensión las cuales tenían un valor de MA (Muy alto) por lo tanto, se procedió a asignar la valoración cuantitativa de acuerdo a su equivalente numérico que sería 5, de los valores obtenidos se saca el promedio y su respectiva calificación; como se muestra a continuación.

Cuadro 6. Valoración cuantitativa del activo copias de seguridad

Activo Copias de seguridad	**Autenticidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Trazabilidad**	**Promedio**	**Calificación**	
Valoración cualitativa	MA	MA	MA	MA	MA			
Valoración Cuantitativa	5	5	5	5	5	5	MA	Crítico

Fuente: Esta investigación.

Al finalizar la valoración del activo copias de seguridad, se obtuvo una calificación de MA que corresponde a Crítico y por lo tanto, se pudo determinar que este activo es de vital importancia para la E.S.E Centro Hospital Luis Antonio Montero y debe ser tenido en cuenta para su protección y preservación de manera adecuada.

A continuación, se presenta el cuadro con la valoración cuantitativa realizada a cada uno de los activos presentes de la entidad.

Cuadro 7. Valoración cuantitativa de los activos MAGERIT

VALORACIÓN CUANTITATIVA DE ACTIVOS MAGERIT			**Dimensión de Seguridad**					**Resultados**		
Grupo de Activos	**Código grupo de activo MAGERIT**	**Código Activo**	**Autenticidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Trazabilidad**	**Promedio**	**Calificación**	
[D] Datos / Información	[backup]	[copias_seguridad]	5	5	5	5	5	5	MA	Crítico
	[password]	[pass_empleados]	4	5	4	4	4	4	A	Importante

Fuente: Esta investigación.

Cuadro 7. (Continuación)

VALORACIÓN CUANTITATIVA DE ACTIVOS MAGERIT			Dimensión de Seguridad					Resultados		
Grupo de Activos	Código grupo de activo MAGERIT	Código Activo	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Trazabilidad	Promedio	Calificación	
[S] Servicios	[ipm]	[gest_privilegios]	4	4	4	4	4	4	A	Importante
[SW] Software	[Oficce]	[oficce]	2	2	2	2	2	2	B	Bajo
	[av]	[antivirus]	3	2	4	4	2	3	M	Apreciable
	[os]	[os_servidor]	5	5	5	5	4	5	MA	Crítico
	[os]	[os_Pcs]	3	2	4	4	2	3	M	Apreciable
	[browser]	[navegador]	2	2	1	2	1	2	B	Bajo
	[App]	[info_salud]	5	5	5	5	5	5	MA	Crítico
[HW] Equipos Informáticos	[mid]	[pc_trabajadores]	2	2	3	4	2	3	M	Apreciable
	[print]	[impresoras]	2	2	3	4	2	3	M	Apreciable
	[router]	[router]	2	2	4	4	2	3	M	Apreciable
	[switch]	[switch]	2	2	4	4	2	3	M	Apreciable
	[data]	[servidor]	4	4	5	5	4	4	A	Importante
[COM] Redes de Comunicaciones	[wifi]	[r_wifi]	3	4	3	4	2	3	M	Apreciable
	[LAN]	[r_Local]	3	4	3	4	2	3	M	Apreciable
	[Internet]	[internet]	2	2	3	4	2	3	M	Apreciable
[MEDIA] Soportes de Información (Almacenamiento Electrónico)	[disk]	[media_dd]	3	4	4	4	3	4	A	Importante
[MEDIA] Soportes de Información (Almacenamiento No Electrónico)	[printed]	[media_hclinicas]	4	4	4	4	3	4	A	Importante

Fuente: Esta investigación.

Cuadro7. (Continuación)

VALORACIÓN CUANTITATIVA DE ACTIVOS MAGERIT			Dimensión de Seguridad					Resultados		
Grupo de Activos	**Código grupo de activo MAGERIT**	**Código Activo**	**Autenticidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Trazabilidad**	**Promedio**	**Calificación**	
[AUX] Equipamiento Auxiliar	[ups]	[ups]	1	1	3	3	2	2	B	Bajo
	[gen]	[gen_electricos]	1	1	3	3	2	2	B	Bajo
	[cabling]	[cab_estructurado]	2	1	4	4	2	3	M	Apreciable
[L] Instalaciones	[building]	[edf_entidad]	1	1	4	4	2	2	B	Bajo
[P] Personal	[ui]	[funcionarios]	4	2	4	3	3	3	M	Apreciable
	[adm]	[admin_sist]	4	2	4	5	4	4	A	Importante

Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO A. Documento unificado Magerit, hoja Valoración Cuantitativa.**

1.4 Análisis de seguridad técnico y físico de la entidad

En este análisis se llevó a cabo dos procesos que permitieron identificar vulnerabilidades y amenazas sobre los activos de la entidad:

- Análisis técnico de seguridad: este permite recolectar información sobre la forma en que los activos han sido configurados, como se encuentra establecida la estructura de la red de comunicación y la forma en que son administrados.

- Análisis de seguridad física: como su nombre lo indica permite identificar el entorno físico del cual se encuentran rodeados los activos.

En estos análisis se encuentra relacionado el factor humano, el cual se encarga de la manipulación y uso de la información, el acceso físico a los activos y el correcto uso de ellos.

Para poder determinar de manera adecuada las amenazas y vulnerabilidades que se pueden presentar sobre los activos de la E.S.E Centro Hospital Luis Antonio Montero, se han desarrollado pruebas que permitan determinar a qué se encuentran expuestos. Algunas de estas se han podido determinar mediante visitas a la entidad, observación directa y operación sobre algunos computadores de los cuales se obtuvo permiso de la Gerencia y la dependencia de sistemas para ser evaluados y poder determinar los resultados, más no para la muestra de evidencias obtenidas como fotos, capturas de imagen, o documentos facilitados por la entidad; además, no se obtuvo acceso para evaluaciones sobre bases de datos y servidor de la entidad.

Algunas de las evaluaciones presentadas a continuación, se realizaron de acuerdo a la selección de una muestra de equipos por cada dependencia, descrita a continuación.

Cuadro 8. Muestra de equipos por dependencia.

Dependencia	Número de equipos	Muestra
Urgencias	3	2
Sala era	1	1
Consultorio urgencias	1	1
Consulta externa	8	4
Atención al usuario	3	1
Facturación	4	2
Salud pública	4	2
Almacén	1	1
Farmacia	2	1
Odontología	2	0
Higiene oral	1	1
Administración	3	2
Tesorería	3	2
Estadística	1	0
Archivo	2	1
Total	39	21

Fuente: Esta investigación.

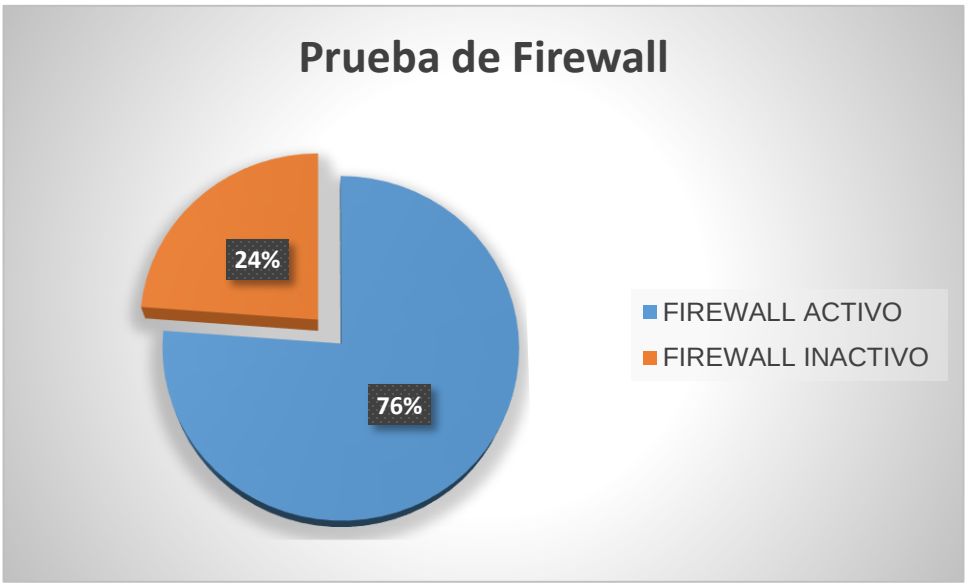
En los siguientes cuadros, se muestra los aspectos a los cuales se realizó la evaluación, el objetivo de esta, una breve descripción de lo que es y los resultados obtenidos del análisis.

Cuadro 9. Evaluación al firewall del sistema

EVALUACIÓN AL FIREWALL DEL SISTEMA	
OBJETIVO	Determinar el nivel de protección del sistema.
DESCRIPCIÓN	Por medio de esta prueba se va a determinar el estado del firewall en diferentes equipos de cómputo del centro de salud con el fin de verificar si se encuentra activo o no. En el equipo seleccionado se ingresa al Panel de control > Sistema y seguridad > Firewall de Windows > Activar o desactivar el firewall de Windows. A continuación, se revisa el estado del firewall en el equipo ya sea activo o inactivo.
RESULTADOS OBTENIDOS	
De acuerdo a la revisión realizada en la muestra de los equipos establecida anteriormente, se obtuvieron los siguientes resultados:	

Fuente: Esta investigación.

Cuadro 9. (Continuación)

1. EVALUACIÓN AL FIREWALL DEL SISTEMA
• Número total de la muestra: 21 • Número de equipos con el firewall activo: 16 • Número de equipos con el firewall inactivo: 5 Los resultados obtenidos en esta prueba evidencian que la mayoría (76%) de equipos están protegidos mediante el firewall del equipo, lo que ayuda a evitar conexiones no deseadas a los computadores; pero es importante tener en cuenta que en los computadores restantes en la entidad (24%) se debe verificar que esta configuración se encuentre realizada de manera adecuada y corregir en caso de que no esté activa. A continuación, se muestra la siguiente grafica de resultados que soportan lo dicho anteriormente. **Gráfico 1. Resultados evaluación de Firewall del sistema**      **Fuente:** Esta investigación.

Fuente: Esta investigación.

Cuadro 10. Evaluación de los puertos del sistema

EVALUACIÓN DE LOS PUERTOS DEL SISTEMA	
OBJETIVO	Determinar el nivel de vulnerabilidad de los puertos del sistema.
DESCRIPCIÓN	• Mediante el uso de la herramienta de línea de comandos Netstat podemos determinar las conexiones y los puertos que están abiertos en los computadores. • Mediante la interfaz de línea de comandos CMD del equipo, se ejecuta el comando netstat –an para poder observar los puertos y el estado de las conexiones existentes.
RESULTADOS OBTENIDOS	
La utilidad Netstat permite determinar el tráfico en el equipo de cómputo. Esta prueba fue realizada en una muestra de 21 equipos en los cuales se aplicó el procedimiento anteriormente mencionado. Al analizar los resultados podemos darnos cuenta que todos los equipos tienen una conexión establecida con el servidor que aparece con dirección IP 10.242.11.67 y diferentes dependencias de la entidad. Los equipos poseen diferentes puertos en escucha y con conexiones establecidas. Al investigar sobre las funciones y problemas de ellos se encontró lo siguiente: • **Puerto 135:** al recibir una conexión con este puerto, se dirige el tráfico hasta el Epmap (Asignador de puntos finales) quien recibe las conexiones Rpc (Llamada a procedimiento remoto) y redirecciona el tráfico hacia los demás puertos asignados para aplicaciones integradas con RPC. **Problema:** El Epmap (Asignador de puntos finales) es aprovechado por virus. Las conexiones repetitivas al puerto 135 pueden provocar la sobrecarga de una computadora, lo cual podría ser un ataque de denegación de servicio. El virus "Blaster" ataca el puerto 135. • **Puerto 139:** El puerto 139 es un dispositivo de programación en red. Es una dirección para una aplicación que se ejecuta en una computadora remota. Es asignado a NetBIOS, Network Basic Input / Output System; los puertos NetBIOS son utilizados por el intercambio de archivos y aplicaciones de uso compartido de impresoras.	

Fuente: Esta investigación.

Cuadro 10. (Continuación)

EVALUACIÓN DE LOS PUERTOS DEL SISTEMA
Problema: Los piratas informáticos utilizan este puerto para intentar ingresar a los servidores; algunos de los malware que atacan por medio de este puerto son virus Chode, el Gusano Mensaje de Dios, Msinit, Netlog, Red, Qaz sadmind y SMB Relay. • **Puerto 445:** este puerto es fundamental para compartir archivos a través de una red TCP/IP Windows. **Problema:** este puerto puede permitir a un atacante remoto obtener información confidencial del sistema y dependiendo del ataque realizado propagarse a través de la red para afectar a más equipos con esta vulnerabilidad. Algunos de los malware que se aprovechan este puerto son los gusanos Sasser, Nimda y Wanna Cry. De acuerdo a las descripciones y problemas descritos anteriormente, es importante tener en cuenta que se debe verificar para qué tanto es útil utilizar cada uno de ellos en la entidad, ya sea para compartir recursos o ejecutar aplicaciones; de lo contrario es necesario que se cierren los puertos abiertos que no se están usando puesto que el malware y los piratas informáticos hacen uso de ellos para vulnerar a las entidades y obtener sus propios beneficios, afectando de manera significativa el correcto funcionamiento de los procesos.

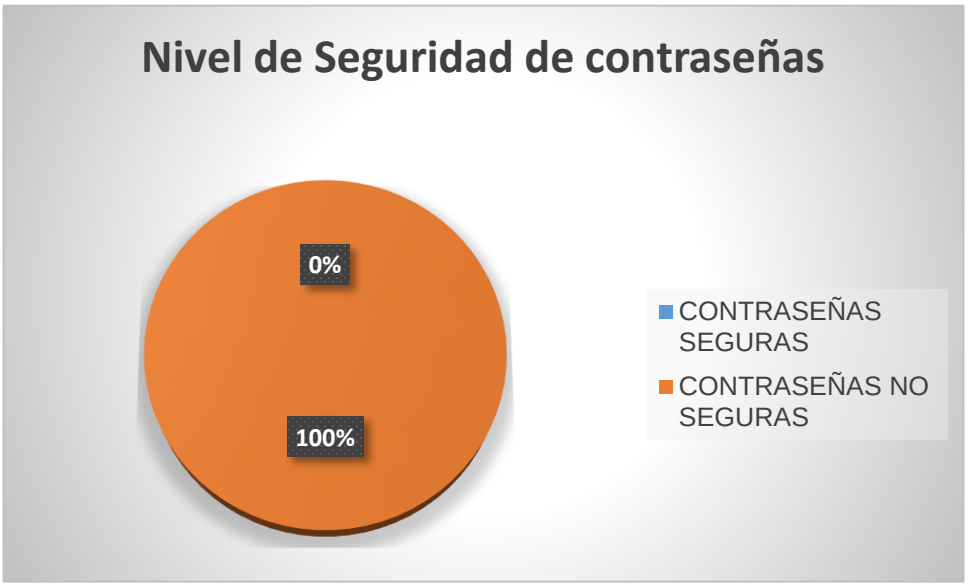
Fuente: Esta investigación.

Cuadro 11. Evaluación del nivel de seguridad de las contraseñas

3. EVALUACIÓN DEL NIVEL DE SEGURIDAD DE LAS CONTRASEÑAS	
OBJETIVO	Determinar el grado de seguridad de las contraseñas en los principales equipos de cómputo del centro de salud.
DESCRIPCIÓN	Para esta prueba se hace uso de la herramienta en línea comprobador de contraseñas. En el siguiente enlace, se puede someter una contraseña a una prueba de nivel de seguridad. https://password.es/comprobador/ Mediante el análisis que nos arroja este sitio se puede determinar el porcentaje de seguridad de la contraseña. Además, se realiza una revisión de cuentas de usuario, determinando si poseen roles establecidos con inicios de sesión seguros protegidos mediante contraseñas.
RESULTADOS OBTENIDOS	
Para cada equipo de trabajo se procedió a realizar la metodología antes planteada de los cuales se obtuvo los siguientes resultados. • Numero de muestra: 21 • Contraseñas seguras: 0 • Contraseñas inseguras: 21 El resultado de esta prueba es negativo, se evidenció que el ingreso al sistema operativo, como al sistema Infosalud tiene un nivel de seguridad en cuanto a contraseñas muy bajo (100%); ya que se utilizan contraseñas débiles, su extensión es máximo de 5 dígitos y no se hace uso de combinaciones de números, letras (mayúsculas – minúsculas) y caracteres especiales. Además, no existe una política que aborde el uso de contraseñas seguras y contengan una periodicidad para ser cambiadas, inclusive en algunos equipos se encontró que no tenían una configuración de rol de usuario con asignación de contraseña, lo que hace fácil el acceso a cualquier usuario sobre el sistema, sus aplicativos y la información contenida en ellos. A continuación, se presenta el gráfico en donde se puede observar el porcentaje de contraseñas inseguras que se manejan en la entidad contando con un 100%.	

Fuente: Esta investigación.

Cuadro 11. (Continuación)

3. EVALUACIÓN DEL NIVEL DE SEGURIDAD DE LAS CONTRASEÑAS
Gráfico 2. Resultados nivel de seguridad de contraseñas  Fuente: Esta investigación.

Fuente: Esta investigación.

Cuadro 12. Recolección de información sobre la red eléctrica, red de datos y cuarto de comunicaciones

<table>
<tr><th colspan="2">4. RECOLECCIÓN DE INFORMACIÓN SOBRE LA RED ELECTRICA, RED DE DATOS Y CUARTO DE COMUNICACIONES</th></tr>
<tr><td>OBJETIVO</td><td>Recolectar información de la red Eléctrica del centro hospital.</td></tr>
<tr><td>DESCRIPCIÓN</td><td>Realizar una verificación sobre las instalaciones eléctricas del centro hospital revisando conexiones, toma eléctrica, etc.
Realizar una verificación del cableado estructurado que se encuentra en las instalaciones de la entidad.
Revisar el acceso y estado del cuarto de comunicaciones y de los elementos contenidos en él.</td></tr>
<tr><td colspan="2">RESULTADOS OBTENIDOS</td></tr>
<tr><td colspan="2">Revisión instalaciones eléctricas
Se hizo una revisión detallada en cuanto a instalaciones eléctricas dentro de cada puesto de trabajo en donde se encontraron algunas irregularidades en cuanto a conexiones eléctricas ya que algunas de estas presentan daños por uso y tiempo de exposición.
Existen equipos de cómputo que no están conectados a fuentes de regulación de energía.
Existen conexiones eléctricas defectuosas en las instalaciones.
El incumplimiento del reglamento establecido para las instalaciones eléctricas RETIE, puede hacer que se presenten fallos y pérdidas de equipos e instalaciones, como también afectar vidas humanas.
Revisión estructura de red del centro hospital
No existe una topología definida.
Puntos de conexión de red obsoletos o en desuso.
En el área de salud pública existen puntos de conexión a red que no están restringidos, es decir, cualquier usuario puede tener acceso a ellos y establecer conexión con la red del centro de salud.
Desorganización en cuanto a conexión de switch.
Canaletas del cable de red dañadas.
Dispositivos de red inseguros, se encuentran al alcance de cualquier usuario.
Algunas partes de las instalaciones del centro de salud presentan humedad.
Revisión del cuarto de comunicaciones
El cuarto de comunicaciones se encuentra en un lugar de fácil acceso; además, no cuenta con una puerta adecuada sino, con una reja la cual no está bajo llave.</td></tr>
</table>

Fuente: Esta investigación.

Cuadro 12. (Continuación)

4. RECOLECCIÓN DE INFORMACIÓN SOBRE LA RED ELECTRICA, RED DE DATOS Y CUARTO DE COMUNICACIONES
RESULTADOS OBTENIDOS
• El gabinete que contiene el switch tiene puesta en la puerta la llave y permite que cualquier persona pueda acceder a los elementos que se encuentran dentro de él. • El cableado troncal que llega al cuarto de comunicaciones se encuentra expuesto, no tiene una canaleta adecuada que lo proteja. • Los cables de red no se encuentran etiquetados. En cuanto al cableado estructurado y el cuarto de comunicaciones hace falta hacer uso de las normas ANSI/TIA/EIA 568A Y 568B, que son quienes establecen como debería estar instalado el cableado (tipo de canaletas y cable de red de acuerdo a los recorridos por donde pase, lugares por donde puede o no pasar el cableado, distancias permitidas en caso de inundaciones, distancias permitidas entre cableado de red y eléctrico, entre otras). Además, estas normas establecen parámetros específicos para el cuarto de comunicaciones sobre su acceso, ubicación, ventilación, material del cuarto, seguridad, entre otras. Al presentar incumplimiento de las normas, en el cuarto de comunicaciones y cableado estructurado en la entidad, se puede presentar perdida de equipos, daños en la red de carácter intencionado o no, ruido e interferencia y efectos en las instalaciones físicas del cableado por humedad e inundaciones.

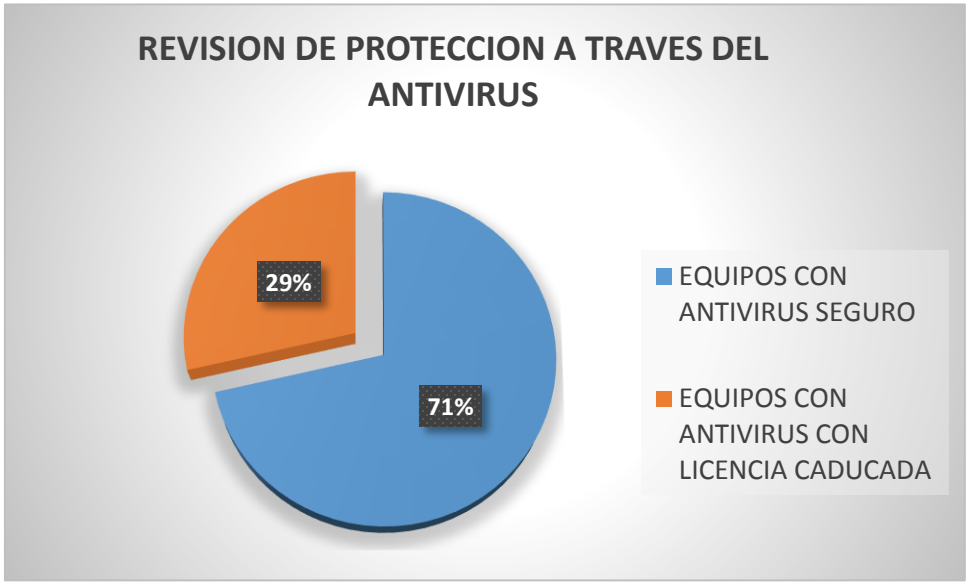
Fuente: Esta investigación.

Cuadro 13. Revisión de protección del sistema a través del antivirus

5. REVISIÓN DE PROTECCIÓN DEL SISTEMA A TRAVES DEL ANTIVIRUS	
OBJETIVO	Determinar el nivel de protección a través del antivirus de los equipos de cómputo de las dependencias del centro hospital.
DESCRIPCIÓN	Se realiza la verificación de la existencia de un antivirus en los equipos de cómputo. Se procede a verificar la configuración del antivirus instalado. Se realiza la verificación de la actualización del antivirus instalado en los equipos de cómputo.
RESULTADOS OBTENIDOS	
Total, muestra: 21 equipos de cómputo En todos los equipos se encuentra instalado algún tipo de antivirus. Equipos de cómputo seguros con antivirus con licencia vigente: 15 Equipos de cómputo con licencias caducadas: 6 A pesar de que existen equipos con licencia vigente; según lo informado por el administrador de sistemas, él no es quien se encarga de realizar la compra y activación de licencias para los antivirus instalados en los computadores. Esto causa que no se tenga en cuenta la importancia de tener un antivirus activo y licenciado que reste problemas de infección de malware; ya que los usuarios de manera intencionada o no, pueden infectar los equipos y por lo tanto llevar a pérdida de información en la entidad. A continuación, se presenta el grafico en donde se puede evidenciar los equipos que se encuentran con y sin antivirus licenciados.	

Fuente: Esta investigación.

Cuadro 13. (Continuación)

5. REVISIÓN DE PROTECCIÓN DEL SISTEMA A TRAVES DEL ANTIVIRUS
Gráfico 3. Resultados protección del sistema con antivirus    **Fuente:** Esta investigación.

Fuente: Esta investigación.

Debido a que no se podía realizar pruebas de stress de disco sobre la base de datos, se planteó una prueba adicional de manera opcional esperando sea tenida en cuenta por la E.S.E Centro Hospital Luis Antonio Montero para que se pudieran observar los resultados reales de lo sugerido a continuación y tengan una idea de cómo se encuentra este aspecto en la entidad.

Cuadro 14. Pruebas de stress de disco sobre base de datos para SQL Server

PRUEBAS DE STRESS DE DISCO SOBRE BASE DE DATOS PARA SQL SERVER	
OBJETIVO	Hacer una prueba de stress sobre sistemas de discos para así poder determinar la capacidad de IOPS (cantidad de operaciones de entrada / salida por segundo que procesa un disco) para SQL Server
DESCRIPCIÓN	La siguiente prueba fue diseñada pensando en el sistema de base de datos que se maneja en el software Infosalud y como sugerencia a ser aplicada, ya que por razones de seguridad y de confidencialidad no se permitió el acceso a dichas bases de datos. **Herramienta a utilizar (DiskSpd)** Microsoft hace varios años proporciona distintas herramientas para poder realizar esta tarea, hasta hace un tiempo se usaba SQLIO,SQLIOSIM o SQLIOStress pero hace unos dos años fueron reemplazadas por Diskspd la cual se sugiere utilizar para realizar esta prueba. Esta herramienta corre desde la línea de comandos y no necesita tener instalado nada adicional al servidor, por lo que lo primero que se hace es descargar la herramienta, descomprimir el archivo y seguir las instrucciones de instalación. Lo que se busca es poder estresar al sistema de almacenamiento para así poder determinar cuál es su capacidad de IOPS (cantidad de operaciones de entrada / salida por segundo que procesa un disco). **Parámetros de Diskspd** Esta herramienta tiene un número importante de parámetros para realizar diferentes funciones, pero para la realización de la prueba sugerida se usa los siguientes: -d: Duración de la prueba medida en segundos (se usará 300 segundos para todas las pruebas) -c: Tamaño del archivo (se usa 512GB para este caso)

Fuente: Esta investigación.

Cuadro 14. (Continuación)

PRUEBAS DE STRESS DE DISCO SOBRE BASE DE DATOS PARA SQL SERVER	
DESCRIPCIÓN	-r: Lecturas Random -w20: Escritura 20% y 80% lectura -t: Cantidad de thread (ideal usar misma cantidad de cores) -o: Request de I/O (carga: se irá aumentando este valor para buscar la carga máxima del Storage) -b8k: quiere decir que se usara bloques de 8k -h: se deshabilita el cache de software & Hardware -L: se obtiene los valores de latencia Nota: Para poder ejecutar diskspd debemos abrir una consola CMD con privilegios de administrador. Con los parámetros anteriormente mencionados se arma las siguientes ejecuciones las cuales pueden ser ejecutadas sobre cualquier unidad de disco, para dar un ejemplo se coloca la letra g suponiendo se esté realizando la prueba sobre esta unidad. **DiskSpd.exe -d300 -c512G -r -w20 -t4 -o1 -b8k -h -L g:\test.dat > oltp_o1.txt** **DiskSpd.exe -d300 -c512G -r -w20 -t4 -o2 -b8k -h -L g:\test.dat > oltp_o2.txt** **DiskSpd.exe -d300 -c512G -r -w20 –mt4 -o4 -b8k -h -L g:\test.dat > oltp_o4.txt** **DiskSpd.exe -d300 -c512G -r -w20 -t4 -o8 -b8k -h -L g:\test.dat > oltp_o8.txt**

Fuente: Esta investigación.

Cuadro 14. (Continuación)

PRUEBAS DE STRESS DE DISCO SOBRE BASE DE DATOS PARA SQL SERVER
RESULTADOS ESPERADOS
Si se realiza esta prueba en el servidor de la E.S.E Centro Hospital Luis Antonio Montero, los resultados detallados que se podrían obtener por cada ejecución del programa diskspd pueden ser guardados en archivos planos para su posterior análisis y compresión. De esta manera se podría observar que, si la base de datos no presenta ningún inconveniente en la realización de las pruebas, la carga máxima de IOPS (cantidad de operaciones de entrada / salida por segundo que procesa un disco) podría variar y tomar valores entre 500 IOPS y 1000 IOPS lo cual sería normal en la base de datos analizada de lo contrario el nivel de funcionamiento del disco estaría saturado. Además, si todo se presenta con normalidad se apreciaría un promedio de latencia que variaría de 7.95 seg en una ejecución a 63 seg en una octava ejecución.

Fuente: Esta investigación.

1.5 Identificación de amenazas y vulnerabilidades

Cada activo identificado en la E.S.E Centro Hospital Luis Antonio Montero se encuentra expuesto a una o varias amenazas, las cuales se pudieron materializar de acuerdo a ciertas vulnerabilidades encontradas en la entidad. Por este motivo es necesario evaluar y determinar a qué amenazas se encuentran expuestos estos activos haciendo uso de la metodología MAGERIT, en ella se plantea diferentes tipos de amenazas y se asocian a cada grupo de activos que puedan afectar.

De acuerdo a las amenazas identificadas según la metodología, se determinó las vulnerabilidades que pueden hacer que se materialicen y causen fallos o daños en la vida útil del activo.

Para continuar analizando el activo copias de seguridad perteneciente al grupo [D] Datos / Información que se ha mencionado en ejemplos anteriores, se realizó el análisis de las amenazas asociadas a él y sus vulnerabilidades. De acuerdo a las amenazas que se pueden referir a este grupo de activos y en específico para el activo planteado, se ha seleccionado la siguiente de la metodología y de acuerdo a esto su respectiva vulnerabilidad como se muestra a continuación.

Cuadro 15. Ejemplo Identificación de amenazas y vulnerabilidades activo copias de seguridad.

Grupo de Activo	Activo	Grupo de amenaza	Amenaza	Vulnerabilidad
[D] Datos / Información	Copias de seguridad	[E] Errores y fallos no intencionados	[E.2] Errores del administrador	Fallo en la creación de copias de seguridad

Fuente: Esta investigación.

De acuerdo a esto se ha realizado el análisis de amenazas y vulnerabilidades para cada uno de los activos de la entidad como se muestra en el siguiente cuadro.

Cuadro 16. Identificación de amenazas y vulnerabilidades de los activos de la entidad

Grupo de activos	Nombre activo MAGERIT	Código activo	Amenazas	Vulnerabilidades
[D] Datos / Información	Copias de Respaldo	[copias_seguridad]	[E.2] Errores del administrador	Fallo en la creación de copias de seguridad
	Credenciales	[Pass_empleados]	[E.2] Errores del administrador	Falta de control sobre contraseñas inseguras
			[E.19] Fugas de información	Contraseñas inseguras
			[A.11] Acceso no autorizado	Contraseñas inseguras
[S] Servicios	Gestión de privilegios	[gest_privilegios]	[E.2] Errores del administrador	Asignación de privilegios inadecuados a usuarios
			[A.19] Divulgación de información	Acceso a información confidencial
[SW] Software	Ofimática	[oficce]	[E.1] Errores de los usuarios	Personal no capacitado
	Antivirus	[antivirus]	[E.1] Errores de los usuarios	Personal no capacitado
			[E.2] Errores del administrador	Instalación de software no licenciado
			[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de actualización de firmas de virus
	Sistema operativo	[os_servidor]	[E.2] Errores del administrador	Configuraciones inadecuadas
			[E.15] Alteración accidental de la información	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones
			[E.20] Vulnerabilidades de los programas (software)	Falta de parches y actualizaciones en el software
			[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de parches y actualizaciones en el software

Fuente: Esta investigación.

Cuadro 16. (Continuación)

Grupo de activos	Nombre activo MAGERIT	Código activo	Amenazas	Vulnerabilidades
[SW] Software	Sistema operativo	[os_servidor]	[A.5] Suplantación de la identidad del usuario	Contraseñas inseguras
			[A.8] Difusión de software dañino	Falta de antivirus licenciados y actualizados, puertos abiertos
			A.11] Acceso no autorizado	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones
			[A.15] Modificación deliberada de la información	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones y contraseñas inseguras en el sistema
	Sistema operativo	[os_Pcs]	[E.2] Errores del administrador	Instalación de software no licenciado
			[E.8] Difusión de software dañino	Propagación de virus por falta de antivirus licenciado.
			[E.21] Errores de mantenimiento / actualización de programas	Falta de actualizaciones importantes del sistema.
			[A.7] Uso no previsto	Instalación de software no licenciado
			[A.11] Acceso no autorizado	Falta de cuentas de usuario con contraseñas seguras
	Navegador web	[navegador]	[E.8] Difusión de software dañino	Descarga de malware
			[A.7] Uso no previsto	Uso inadecuado por parte del personal
	Aplicación	[info_salud]	[A.5] Suplantación de la identidad del usuario	Contraseñas inseguras
			[A.11] Acceso no autorizado	Contraseñas inseguras
			[A.15] Modificación deliberada de la información	Contraseñas inseguras
			[A.24] Denegación de servicio	Recursos del servidor insuficientes para las necesidades del sistema.

Fuente: Esta investigación.

Cuadro 16. (Continuación)

Grupo de activos	Nombre activo MAGERIT	Código activo	Amenazas	Vulnerabilidades
[HW] Equipos Informáticos	Equipos de trabajo conectados a través de red	[pc_trabajadores]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos
			[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Inadecuada planeación y realización de mantenimientos preventivos.
	Equipos de impresión	[impresoras]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos
			[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.
	Enrutadores	[router]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.
	Switch	[switch]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.
			[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.
	Servidor	[servidor]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.
			[E.24] Caída del sistema por agotamiento de recursos	Recursos del equipo insuficientes para las necesidades del sistema.
			[A.11] Acceso no autorizado	Falta de control de acceso
			[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.

Fuente: Esta investigación.

Cuadro 16. (Continuación)

Grupo de activos	Nombre activo MAGERIT	Código activo	Amenazas	Vulnerabilidades
[COM] Redes de Comunicaciones	Red inalámbrica	[r_wifi]	[I.8] Fallo de servicios de comunicaciones	Facilidad de acceso a los access point.
			[A.7] Uso no previsto	Acceso de los empleados a la red inalámbrica
			[A.14] Interceptación de información (escucha)	Red inalámbrica insegura
	Red local	[r_Local]	[I.8] Fallo de servicios de comunicaciones	Saturación de tráfico en la red
			[E.2] Errores del administrador	Desorganización en la asignación de direcciones IP a los equipos
			[A.11] Acceso no autorizado	Puntos de red accesibles fácilmente
	Internet	[internet]	[I.8] Fallo de servicios de comunicaciones	Inadecuado servicio de banda ancha
[MEDIA] Soportes de Información (Almacenamiento Electrónico)	Discos	[media_dd]	[I.10] Degradación de los soportes de almacenamiento de la información	Daño en los equipos por tiempo de uso y lugar de exposición.
			[E.2] Errores del administrador	Inadecuada manipulación de los discos duros.
			[A.7] Uso no previsto	Almacenamiento de datos personales.
[MEDIA] Soportes de Información (Almacenamiento No Electrónico)	Material impreso	[media_hclinicas]	[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.
			[E.19] Fugas de información	Extracción de información confidencial

Fuente: Esta investigación.

Cuadro 16. (Continuación)

Grupo de activos	Nombre activo MAGERIT	Código activo	Amenazas	Vulnerabilidades
[AUX] Equipamiento Auxiliar	Sistemas de Alimentación ininterrumpida	[ups]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos
			[I.6] Corte del suministro eléctrico	Daño por variaciones de energía eléctrica.
			[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.
	Generadores eléctricos	[gen_electricos]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos
			[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.
	Cableado estructurado	[cab_estructurado]	[N.1] Fuego	Instalaciones eléctricas inadecuadas
			[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.
[L] Instalaciones	Edificio	[edf_entidad]	[N.7] Desastres naturales. Fenómeno sísmico.	Temblores o terremotos.
[P] Personal	Usuarios internos	[funcionarios]	[E.19] Fugas de información	Extracción de información confidencial
			[A.30] Ingeniería social (picaresca)	Ingenuidad por parte del personal.
	Administradores de sistemas	[admin_sist]	[E.7] Deficiencias en la organización	Inadecuada asignación de funciones al administrador.
			[E.28] Indisponibilidad del personal	Ausencia laboral por enfermedad.

Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO A. Documento unificado Magerit, hoja Amenazas y vulnerabilidades.**

1.6 Estimación de probabilidad y degradación del activo

De acuerdo a las amenazas y vulnerabilidades identificadas que pueden afectar a los activos de la E.S.E Centro Hospital Luis Antonio Montero, se debió realizar una valoración de la influencia de estas, en cuanto a los siguientes aspectos:

- **Probabilidad:** qué tan probable es que se materialice la amenaza.
- **Degradación:** qué tan perjudicado resultaría el activo (mide el daño causado por un incidente en el supuesto de que ocurriera).

La valoración que se utilizó para calificar la probabilidad se basó en el siguiente cuadro adaptado de las escalas cualitativas de la metodología Magerit.

Cuadro 17. Valoración cualitativa de la probabilidad

Valoración Cualitativa		Descripción
MA	Muy alta	Prácticamente seguro
A	Alta	Probable
M	Media	Posible
B	Baja	Poco probable
MB	Muy baja	Muy raro

Fuente: Adaptación de MAGERIT versión 3, libro 3 Guía de técnicas. Página 7.

Para determinar la valoración otorgada a la degradación se tomó en cuenta la siguiente escala teniendo en cuenta tres porcentajes, en cuanto a qué tan perjudicado resultaría el activo; teniendo que:

Cuadro 18. Valoración de la degradación del activo

Valoración	Descripción
100%	Degradación alta del activo
10%	Degradación media del activo
1%	Degradación baja del activo

Fuente: Adaptación de MAGERIT versión 3, libro 1 Método. Página 28.

Como ejemplo de estas valoraciones se tiene el activo copias de seguridad, al cual de acuerdo a la amenaza y la vulnerabilidad asociada se ha determinado las siguientes calificaciones.

Cuadro 19. Ejemplo valoración de probabilidad y degradación activo copias de seguridad

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Probabilidad	Degradación %
[D] Datos / Información	[copias_seguridad]	[E.2] Errores del administrador	Fallo en la creación de copias de seguridad	M	100

Fuente: Esta investigación.

- **Probabilidad** Valoración: M (Media)
  Se determina esta valoración la cual significa que es **posible** que la vulnerabilidad: fallo en la creación de copias de seguridad, permita materializar la amenaza de errores del administrador. Es posible que en la creación de las copias de seguridad de la entidad el administrador encargado genere una copia errónea o con fallas que pueda afectar a este activo y por lo tanto a la entidad, ya que estas copias son de gran ayuda en caso de pérdida o daño de información y es indispensable tenerlas realizadas de manera adecuada.

- **Degradación** Valoración: 100%
  La degradación sobre el activo de copias de seguridad en caso de que se materialice la amenaza sería en un 100% ya que, el activo resultaría altamente afectado y por lo tanto perjudicaría el normal desarrollo de los procesos que se desarrollan en la entidad en caso de llegarlo a necesitar.

A continuación, se realizó la correspondiente valoración en cuanto a probabilidad y degradación para cada activo de la entidad como se muestra a continuación.

Cuadro 20. Valoración de probabilidad y degradación de los activos de la entidad

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Probabilidad	Degradación %
[D] Datos / Información	[copias_seguridad]	[E.2] Errores del administrador	Fallo en la creación de copias de seguridad	M	100
	[Pass_empleados]	[E.2] Errores del administrador	Falta de control sobre contraseñas inseguras	A	10
		[E.19] Fugas de información	Contraseñas inseguras	A	10
		[A.11] Acceso no autorizado	Contraseñas inseguras	MA	10
[S] Servicios	[gest_privilegios]	[E.2] Errores del administrador	Asignación de privilegios inadecuados a usuarios	MB	100
		[A.19] Divulgación de información	Acceso a información confidencial	MB	10
[SW] Software	[oficce]	[E.1] Errores de los usuarios	Personal no capacitado	M	1
	[antivirus]	[E.1] Errores de los usuarios	Personal no capacitado	A	1
		[E.2] Errores del administrador	Instalación de software no licenciado	MA	10
		[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de actualización de firmas de virus.	A	10

Fuente: Esta investigación.

Cuadro 20. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Probabilidad	Degradación %
[SW] Software	[os_servidor]	[E.2] Errores del administrador	Configuraciones inadecuadas	M	10
		[E.15] Alteración accidental de la información	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones	A	10
		[E.20] Vulnerabilidades de los programas (software)	Falta de parches y actualizaciones en el software	B	10
		[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de parches y actualizaciones en el software	B	10
		[A.5] Suplantación de la identidad del usuario	Contraseñas inseguras	A	10
		[A.8] Difusión de software dañino	Falta de antivirus licenciados y actualizados, puertos abiertos	M	100
		A.11] Acceso no autorizado	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones	A	10

Fuente: Esta investigación.

Cuadro 20. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Probabilidad	Degradación %
[SW] Software	[os_servidor]	[A.15] Modificación deliberada de la información	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones y contraseñas inseguras en el sistema	A	10
	[os_Pcs]	[E.2] Errores del administrador	Instalación de software no licenciado	M	10
		[E.8] Difusión de software dañino	Propagación de virus por falta de antivirus licenciado.	A	100
		[E.21] Errores de mantenimiento / actualización de programas	Falta de actualizaciones importantes del sistema.	B	10
		[A.7] Uso no previsto	Instalación de software no licenciado	M	1
		[A.11] Acceso no autorizado	Falta de cuentas de usuario con contraseñas seguras	A	10
	[navegador]	[E.8] Difusión de software dañino	Descarga de malware	A	100
		[A.7] Uso no previsto	Uso inadecuado por parte del personal	A	10

Fuente: Esta investigación.

Cuadro 20. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Probabilidad	Degradación %
[SW] Software	[info_salud]	[A.5] Suplantación de la identidad del usuario	Contraseñas inseguras	A	100
		[A.11] Acceso no autorizado	Contraseñas inseguras	A	100
		[A.15] Modificación deliberada de la información	Contraseñas inseguras	M	100
		[A.24] Denegación de servicio	Recursos del servidor insuficientes para las necesidades del sistema.	M	10
[HW] Equipos Informáticos	[pc_trabajadores]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	B	1
		[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	B	10
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Inadecuada planeación y realización de mantenimientos preventivos.	B	10
	[impresoras]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	B	1
		[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	B	1

Fuente: Esta investigación.

Cuadro 20. (Continuación)

Grupo de Activos	Código Activo	Amenazas	Vulnerabilidades	Probabilidad	Degradación %
[HW] Equipos Informáticos	[router]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	B	10
	[switch]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	B	10
		[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	M	10
	[servidor]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	B	10
		[E.24] Caída del sistema por agotamiento de recursos	Recursos del equipo insuficientes para las necesidades del sistema.	B	10
		[A.11] Acceso no autorizado	Falta de control de acceso	M	100
		[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	M	100

Fuente: Esta investigación.

Cuadro 20. (Continuación)

Grupo de Activos	Código Activo	Amenazas	Vulnerabilidades	Probabilidad	Degradación %
[COM] Redes de Comunicaciones	[r_wifi]	[I.8] Fallo de servicios de comunicaciones	Facilidad de acceso a los access point.	M	10
		[A.7] Uso no previsto	Acceso de los empleados a la red inalámbrica	A	10
		[A.14] Interceptación de información (escucha)	Red inalámbrica insegura	M	10
	[r_Local]	[I.8] Fallo de servicios de comunicaciones	Saturación de tráfico en la red	B	10
		[E.2] Errores del administrador	Desorganización en la asignación de direcciones IP a los equipos	M	10
		[A.11] Acceso no autorizado	Puntos de red accesibles fácilmente	M	10
	[internet]	[I.8] Fallo de servicios de comunicaciones	Inadecuado servicio de banda ancha	M	10
[MEDIA] Soportes de Información (Electrónico)	[media_dd]	[I.10] Degradación de los soportes de almacenamiento de la información	Daño en los equipos por tiempo de uso y lugar de exposición.	B	100
		[E.2] Errores del administrador	Inadecuada manipulación de los discos duros.	B	10

Fuente: Esta investigación.

Cuadro 20. (Continuación)

Grupo de Activos	Código Activo	Amenazas	Vulnerabilidades	Probabilidad	Degradación %
[MEDIA] Soportes de Información (Electrónico)	[media_dd]	[A.7] Uso no previsto	Almacenamiento de datos personales.	M	1
[MEDIA] Soportes de Información (No Electrónico)	[media_hclinicas]	[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	M	10
		[E.19] Fugas de información	Extracción de información confidencial	B	10
[AUX] Equipamiento Auxiliar	[ups]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	M	10
		[I.6] Corte del suministro eléctrico	Daño por variaciones de energía eléctrica.	B	100
		[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	A	100
	[gen_electricos]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	M	10
		[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	M	10
	[cab_estructurado]	[N.1] Fuego	Instalaciones eléctricas inadecuadas	M	100
		[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	M	100

Fuente: Esta investigación.

Cuadro 20. (Continuación)

Grupo de Activos	Código Activo	Amenazas	Vulnerabilidades	Probabilidad	Degradación %
[L] Instalaciones	[edf_entidad]	[N.7] Desastres naturales. Fenómeno sísmico.	Temblores o terremotos.	B	100
[P] Personal	[funcionarios]	[E.19] Fugas de información	Extracción de información confidencial	B	10
		[A.30] Ingeniería social (picaresca)	Ingenuidad por parte del personal.	M	10
	[admin_sist]	[E.7] Deficiencias en la organización	Inadecuada asignación de funciones al administrador.	M	10
		[E.28] Indisponibilidad del personal	Ausencia laboral por enfermedad.	B	10

Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO A. Documento unificado Magerit, hoja Amenazas y vulnerabilidades** o específicamente en la **hoja Probabilidad y Degradación.**

1.7 Estimación del impacto

El impacto es la medida del daño sobre un activo de acuerdo a la materialización de una amenaza. Para poder determinar la estimación del impacto sobre los activos de la E.S.E Centro Hospital Luis Antonio Montero fue necesario tener en cuenta la siguiente tabla, en la cual se cruza el resultado de la calificación dada al activo en la valoración cuantitativa y la valoración de la degradación.

Cuadro 21. Estimación del impacto

Impacto		**Degradación**		
		1%	**10%**	**100%**
Calificación valoración cuantitativa	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Adaptación de MAGERIT versión 3, libro 3 Guía de técnicas. Página 6.

De acuerdo al anterior cuadro, se procede a realizar la valoración de ejemplo para el activo copias de seguridad, en el cual se obtuvo las siguientes valoraciones.

- **Calificación valoración cuantitativa** Valoración: MA (Muy alto)
- **Degradación** Valoración: 100%

Al cruzar estas dos variables en el siguiente cuadro, se obtuvo una valoración de MA (Muy alto) para el impacto, lo cual podría hacer que se materialice la amenaza mediante la vulnerabilidad encontrada sobre el activo copias de seguridad, por tanto, el activo debe ser tenido en cuenta para una atención inmediata.

Cuadro 22. Ejemplo valoración del impacto activo copias de seguridad

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Calificación valoración cuantitativa	Degradación %	Impacto
[D] Datos / Información	[copias_seguridad]	[E.2] Errores del administrador	Fallo en la creación de copias de seguridad	MA	100	MA

Fuente: Esta investigación.

En el siguiente cuadro se obtuvieron los resultados del impacto por cada activo de acuerdo a la calificación de valoración cuantitativa y la degradación obtenida para cada uno de ellos.

Cuadro 23. Valoración del impacto de los activos de la entidad

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Valoración cuantitativa	Degradación %	Impacto
[D] Datos / Información	[copias_seguridad]	[E.2] Errores del administrador	Fallo en la creación de copias de seguridad	MA	100	MA
	[Pass_empleados]	[E.2] Errores del administrador	Falta de control sobre contraseñas inseguras	A	10	M
		[E.19] Fugas de información	Contraseñas inseguras	A	10	M
		[A.11] Acceso no autorizado	Contraseñas inseguras	A	10	M

Fuente: Esta investigación.

Cuadro 23. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Valoración cuantitativa	Degradación %	Impacto
[S] Servicios	[gest_privilegios]	[E.2] Errores del administrador	Asignación de privilegios inadecuados a usuarios	A	100	A
		[A.19] Divulgación de información	Acceso a información confidencial	A	10	M
[SW] Software	[oficce]	[E.1] Errores de los usuarios	Personal no capacitado	B	1	MB
	[antivirus]	[E.1] Errores de los usuarios	Personal no capacitado	M	1	MB
		[E.2] Errores del administrador	Instalación de software no licenciado	M	10	B
		[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de actualización de firmas de virus.	M	10	B
	[os_servidor]	[E.2] Errores del administrador	Configuraciones inadecuadas	MA	10	A
		[E.15] Alteración accidental de la información	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones	MA	10	A
		[E.20] Vulnerabilidades de los programas (software)	Falta de parches y actualizaciones en el software	MA	10	A
		[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de parches y actualizaciones en el software	MA	10	A

Fuente: Esta investigación.

Cuadro 23. (Continuación)

Grupo de Activos	Código Activo	Amenazas	Vulnerabilidades	Valoración cuantitativa	Degradación %	Impacto
[SW] Software	[os_servidor]	[A.5] Suplantación de la identidad del usuario	Contraseñas inseguras	MA	10	A
		[A.8] Difusión de software dañino	Falta de antivirus licenciados y actualizados, puertos abiertos	MA	100	MA
		A.11] Acceso no autorizado	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones	MA	10	A
		[A.15] Modificación deliberada de la información	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones y contraseñas inseguras en el sistema	MA	10	A
	[os_Pcs]	[E.2] Errores del administrador	Instalación de software no licenciado	M	10	B
		[E.8] Difusión de software dañino	Propagación de virus por falta de antivirus licenciado.	M	100	M
		[E.21] Errores de mantenimiento / actualización de programas	Falta de actualizaciones importantes del sistema.	M	10	B
		[A.7] Uso no previsto	Instalación de software no licenciado	M	1	MB
		[A.11] Acceso no autorizado	Falta de cuentas de usuario con contraseñas seguras	M	10	B

Fuente: Esta investigación.

Cuadro 23. (Continuación)

Grupo de Activos	Código Activo	Amenazas	Vulnerabilidades	Valoración cuantitativa	Degradación %	Impacto
[SW] Software	[navegador]	[E.8] Difusión de software dañino	Descarga de malware	B	100	B
		[A.7] Uso no previsto	Uso inadecuado por parte del personal	B	10	MB
	[info_salud]	[A.5] Suplantación de la identidad del usuario	Contraseñas inseguras	MA	100	A
		[A.11] Acceso no autorizado	Contraseñas inseguras	MA	100	A
		[A.15] Modificación deliberada de la información	Contraseñas inseguras	MA	100	A
		[A.24] Denegación de servicio	Recursos del servidor insuficientes para las necesidades del sistema.	MA	10	M
[HW] Equipos Iinformáticos	[pc_trabajadores]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	M	1	MB
		[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	M	10	B
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Inadecuada planeación y realización de mantenimientos preventivos.	M	10	B

Fuente: Esta investigación.

Cuadro 23. (Continuación)

Grupo de Activos	Código Activo	Amenazas	Vulnerabilidades	Valoración cuantitativa	Degradación %	Impacto
[HW] Equipos Informáticos	[impresoras]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	M	1	MB
		[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	M	1	MB
	[router]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	M	10	B
	[switch]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	M	10	B
		[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	M	10	B
	[servidor]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	A	10	M
		[E.24] Caída del sistema por agotamiento de recursos	Recursos del equipo insuficientes para las necesidades del sistema.	A	10	M
		[A.11] Acceso no autorizado	Falta de control de acceso	A	100	A

Fuente: Esta investigación.

Cuadro 23. (Continuación)

Grupo de Activos	Código Activo	Amenazas	Vulnerabilidades	Valoración cuantitativa	Degradación %	Impacto
[HW] Equipos Informáticos	[servidor]	[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	A	100	A
[COM] Redes de Comunicaciones	[r_wifi]	[I.8] Fallo de servicios de comunicaciones	Facilidad de acceso a los access point.	M	10	B
		[A.7] Uso no previsto	Acceso de los empleados a la red inalámbrica	M	10	B
		[A.14] Interceptación de información (escucha)	Red inalámbrica insegura	M	10	B
	[r_Local]	[I.8] Fallo de servicios de comunicaciones	Saturación de tráfico en la red	M	10	B
		[E.2] Errores del administrador	Desorganización en la asignación de direcciones IP a los equipos	M	10	B
		[A.11] Acceso no autorizado	Puntos de red accesibles fácilmente	M	10	B
	[internet]	[I.8] Fallo de servicios de comunicaciones	Inadecuado servicio de banda ancha	M	10	B
[MEDIA] Soportes de Información (Electrónico)	[media_dd]	[I.10] Degradación de los soportes de almacenamiento de la información	Daño en los equipos por tiempo de uso y lugar de exposición.	A	100	A
[MEDIA] Soportes de Información (Electrónico)	[media_dd]	[E.2] Errores del administrador	Inadecuada manipulación de los discos duros.	A	10	M

Fuente: Esta investigación.

Cuadro 23. (Continuación)

Grupo de Activos	Código Activo	Amenazas	Vulnerabilidades	Valoración cuantitativa	Degradación %	Impacto
[MEDIA] Soportes de Información (Electrónico)	[media_dd]	[A.7] Uso no previsto	Almacenamiento de datos personales.	A	1	B
[MEDIA] Soportes de Información (No Electrónico)	[media_hclinicas]	[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	A	10	M
		[E.19] Fugas de información	Extracción de información confidencial	A	10	M
[AUX] Equipamiento Auxiliar	[ups]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	B	10	MB
		[I.6] Corte del suministro eléctrico	Daño por variaciones de energía eléctrica.	B	100	B
		[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	B	100	B
	[gen_electricos]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	B	10	MB
		[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	B	10	MB
	[cab_estructurado]	[N.1] Fuego	Instalaciones eléctricas inadecuadas	M	100	M

Fuente: Esta investigación.

Cuadro 23. (Continuación)

Grupo de Activos	Código Activo	Amenazas	Vulnerabilidades	Valoración cuantitativa	Degradación %	Impacto
[AUX] Equipamiento Auxiliar	[cab_estructurado]	[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	M	100	M
[L] Instalaciones	[edf_entidad]	[N.7] Desastres naturales. Fenómeno sísmico.	Temblores o terremotos.	B	100	B
[P] Personal	[funcionarios]	[E.19] Fugas de información	Extracción de información confidencial	M	10	B
		[A.30] Ingeniería social (picaresca)	Ingenuidad por parte del personal.	M	10	B
	[admin_sist]	[E.7] Deficiencias en la organización	Inadecuada asignación de funciones al administrador.	A	10	M
		[E.28] Indisponibilidad del personal	Ausencia laboral por enfermedad.	A	10	M

Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO A. Documento unificado Magerit, hoja Amenazas y vulnerabilidades** o específicamente en la **hoja Impacto.**

1.8 Estimación del riesgo

La estimación del riesgo mide el grado de exposición a que una amenaza se materialice sobre los activos causando daños o perjuicios en la entidad. La estimación del riesgo se pudo calcular mediante los resultados obtenidos en la siguiente tabla en donde se cruza la valoración del impacto y la probabilidad.

Cuadro 24. Estimación del riesgo.

Riesgo		Probabilidad					Escala Cualitativa	
		MB	**B**	**M**	**A**	**MA**	**Valor**	**Escala**
Impacto	**MA**	A	MA	MA	MA	MA	MA	Crítico
	A	M	A	A	MA	MA	A	Importante
	M	B	M	M	A	A	M	Apreciable
	B	MB	B	B	M	M	B	Bajo
	MB	MB	MB	MB	B	B	MB	Despreciable

Fuente: Adaptación de MAGERIT versión 3, libro 3 Guía de técnicas. Página 7.

Para determinar la valoración del riesgo en el activo copias de seguridad se tuvo en cuenta la referencia a las siguientes valoraciones según lo mencionado anteriormente, las cuales son:

- **Impacto** Valoración: MA
- **Probabilidad** Valoración: M

De acuerdo a esto y basándose en la tabla se pudo determinar que la estimación del riesgo para el activo es de MA lo cual significa que es Crítico; por lo tanto, se debe tener en cuenta a activos como este que cuenten con una escala de crítico, importante y apreciable; ya que ellos son los que tienen un grado de exposición alto

a que la amenaza se materialice y se presenten daños en la E.S.E Centro Hospital Luis Antonio Montero.

Cuadro 25. Ejemplo valoración del riesgo activo copias de seguridad

Grupo de Activos	Código activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgo	
[D] Datos / Información	[copias_seguridad]	[E.2] Errores del administrador	Fallo en la creación de copias de seguridad	MA	M	MA	Crítico

Fuente: esta investigación.

A continuación, se presenta el cuadro que contiene la estimación del riesgo calculada para cada activo de la entidad, pudiendo determinar con estos resultados la escala cualitativa del riesgo que poseen cada uno de ellos.

Cuadro 26. Valoración del riesgo de los activos de la entidad

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgo	
[D] Datos / Información	[copias_seguridad]	[E.2] Errores del administrador	Fallo en la creación de copias de seguridad	MA	M	MA	Crítico
	[Pass_empleados]	[E.2] Errores del administrador	Falta de control sobre contraseñas inseguras	M	A	A	Importante
		[E.19] Fugas de información	Contraseñas inseguras	M	A	A	Importante
		[A.11] Acceso no autorizado	Contraseñas inseguras	M	MA	A	Importante
[S] Servicios	[gest_privilegios]	[E.2] Errores del administrador	Asignación de privilegios inadecuados a usuarios	A	MB	M	Apreciable
		[A.19] Divulgación de información	Acceso a información confidencial	M	MB	B	Bajo
[SW] Software	[oficce]	[E.1] Errores de los usuarios	Personal no capacitado	MB	M	MB	Despreciable
	[antivirus]	[E.1] Errores de los usuarios	Personal no capacitado	MB	A	B	Bajo
		[E.2] Errores del administrador	Instalación de software no licenciado	B	MA	M	Apreciable
		[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de actualización de firmas de virus.	B	A	M	Apreciable

Fuente: Esta investigación.

Cuadro 26. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgo	
[SW] Software	[os_servidor]	[E.2] Errores del administrador	Configuraciones inadecuadas	A	M	A	Importante
		[E.15] Alteración accidental de la información	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones	A	A	MA	Crítico
		[E.20] Vulnerabilidades de los programas (software)	Falta de parches y actualizaciones en el software	A	B	A	Importante
		[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de parches y actualizaciones en el software	A	B	A	Importante
		[A.5] Suplantación de la identidad del usuario	Contraseñas inseguras	A	A	MA	Crítico
		[A.8] Difusión de software dañino	Falta de antivirus licenciados y actualizados, puertos abiertos	MA	M	MA	Crítico
		[A.11] Acceso no autorizado	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones	A	A	MA	Crítico

Fuente: Esta investigación.

Cuadro 26. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgo	
[SW] Software	[os_servidor]	[A.15] Modificación deliberada de la información	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones y contraseñas inseguras en el sistema	A	A	MA	Crítico
	[os_Pcs]	[E.2] Errores del administrador	Instalación de software no licenciado	B	M	B	Bajo
		[E.8] Difusión de software dañino	Propagación de virus por falta de antivirus licenciado.	M	A	A	Importante
		[E.21] Errores de mantenimiento / actualización de programas	Falta de actualizaciones importantes del sistema.	B	B	B	Bajo
		[A.7] Uso no previsto	Instalación de software no licenciado	MB	M	MB	Despreciable
		[A.11] Acceso no autorizado	Falta de cuentas de usuario con contraseñas seguras	B	A	M	Apreciable
	[navegador]	[E.8] Difusión de software dañino	Descarga de malware	B	A	M	Apreciable
		[A.7] Uso no previsto	Uso inadecuado por parte del personal	MB	A	B	Bajo

Fuente: Esta investigación.

Cuadro 26. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgo	
[SW] Software	[info_salud]	[A.5] Suplantación de la identidad del usuario	Contraseñas inseguras	A	A	MA	Crítico
		[A.11] Acceso no autorizado	Contraseñas inseguras	A	A	MA	Crítico
		[A.15] Modificación deliberada de la información	Contraseñas inseguras	A	M	A	Importante
		[A.24] Denegación de servicio	Recursos del servidor insuficientes para las necesidades del sistema.	M	M	M	Apreciable
[HW] Equipos Informáticos	[pc_trabajadores]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	MB	B	MB	Despreciable
		[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	B	B	B	Bajo
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Inadecuada planeación y realización de mantenimientos preventivos.	B	B	B	Bajo
	[impresoras]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	MB	B	MB	Despreciable
		[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	MB	B	MB	Despreciable

Fuente: Esta investigación.

Cuadro 26. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgo	
[HW] Equipos Informáticos	[router]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	B	B	B	Bajo
	[switch]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	B	B	B	Bajo
		[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	B	M	B	Bajo
	[servidor]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	M	B	M	Apreciable
		[E.24] Caída del sistema por agotamiento de recursos	Recursos del equipo insuficientes para las necesidades del sistema.	M	B	M	Apreciable
		[A.11] Acceso no autorizado	Falta de control de acceso	A	M	A	Importante
		[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	A	M	A	Importante

Fuente: Esta investigación.

Cuadro 26. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgo	
[COM] Redes de Comunicaciones	[r_wifi]	[I.8] Fallo de servicios de comunicaciones	Facilidad de acceso a los access point.	B	M	B	Bajo
		[A.7] Uso no previsto	Acceso de los empleados a la red inalámbrica	B	A	M	Apreciable
		[A.14] Interceptación de información (escucha)	Red inalámbrica insegura	B	M	B	Bajo
	[r_Local]	[I.8] Fallo de servicios de comunicaciones	Saturación de tráfico en la red	B	B	B	Bajo
		[E.2] Errores del administrador	Desorganización en la asignación de direcciones IP a los equipos	B	M	B	Bajo
		[A.11] Acceso no autorizado	Puntos de red accesibles fácilmente	B	M	B	Bajo
	[internet]	[I.8] Fallo de servicios de comunicaciones	Inadecuado servicio de banda ancha	B	M	B	Bajo
[MEDIA] Soportes de Información (Electrónico)	[media_dd]	[I.10] Degradación de los soportes de almacenamiento de la información	Daño en los equipos por tiempo de uso y lugar de exposición.	A	B	A	Importante

Fuente: Esta investigación.

Cuadro 26. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgo	
[MEDIA] Soportes de Información (Electrónico)	[media_dd]	[E.2] Errores del administrador	Inadecuada manipulación de los discos duros.	M	B	M	Apreciable
		[A.7] Uso no previsto	Almacenamiento de datos personales.	B	M	B	Bajo
[MEDIA] Soportes de Información (No Electrónico)	[media_hclinicas]	[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	M	M	M	Apreciable
		[E.19] Fugas de información	Extracción de información confidencial	M	B	M	Apreciable
[AUX] Equipamiento Auxiliar	[ups]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	MB	M	MB	Despreciable
		[I.6] Corte del suministro eléctrico	Daño por variaciones de energía eléctrica.	B	B	B	Bajo
		[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	B	A	M	Apreciable
	[gen_electricos]	[I.3] Contaminación mecánica	Falta de mantenimientos preventivos físicos	MB	M	MB	Despreciable
		[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	MB	M	MB	Despreciable

Fuente: Esta investigación.

Cuadro 26. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgo	
[AUX] Equipamiento Auxiliar	[cab_estructurado]	[N.1] Fuego	Instalaciones eléctricas inadecuadas	M	M	M	Apreciable
		[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	M	M	M	Apreciable
[L] Instalaciones	[edf_entidad]	[N.7] Desastres naturales. Fenómeno sísmico.	Temblores o terremotos.	B	B	B	Bajo
[P] Personal	[funcionarios]	[E.19] Fugas de información	Extracción de información confidencial	B	B	B	Bajo
		[A.30] Ingeniería social (picaresca)	Ingenuidad por parte del personal.	B	M	B	Bajo
	[admin_sist]	[E.7] Deficiencias en la organización	Inadecuada asignación de funciones al administrador.	M	M	M	Apreciable
		[E.28] Indisponibilidad del personal	Ausencia laboral por enfermedad.	M	B	M	Apreciable

Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO A. Documento unificado Magerit, hoja Amenazas y vulnerabilidades** o específicamente en la **hoja Riesgo.**

1.9 Evaluación de riesgos

La evaluación de riesgos se basó teniendo en cuenta la escala cualitativa dada para cada uno de los activos según la estimación del riesgo y de acuerdo a esto se dio un tratamiento a cada uno de ellos de la siguiente manera.

Cuadro 27. Tratamiento del riesgo según la escala cualitativa del riesgo.

Escala Cualitativa		**Tratamiento del riesgo según la escala**
Valor	**Escala**	
MA	Crítico	Opciones: a. Transferir el riesgo. b. Evitar el riesgo. c. Reducir o mitigar el riesgo.
A	Importante	
M	Apreciable	
B	Bajo	Aceptar el riesgo.
MB	Despreciable	

Fuente: Esta investigación.

1.9.1 Plan de tratamiento de riesgos

El plan de tratamiento del riesgo pretende tratar los riesgos asociados a los activos de tal forma que, si se llegará a presentar un incidente, este no genere pérdidas o daños significativos sobre el activo en la entidad. La forma de tratar los riesgos puede consistir en: evitar circunstancias que lo provoquen, reducir posibilidades de que ocurran, delimitar las consecuencias que pueda causar, compartir con otra organización (contratando un servicio o un seguro de cobertura) o como última opción, aceptándolo.

En este paso lo que se procuró principalmente es mitigar los riesgos que requieren atención inmediata, ya que estos son los que pueden tener un impacto más alto al momento de generarse, exponiendo los activos de la entidad ya sea a perderse en su totalidad o parcialmente. Es importante tener en cuenta que los riesgos que se

contemplaron en el plan de tratamiento de riesgo para la E.S.E Centro Hospital Luis, son los que fueron valorados con las siguientes escalas: MA (Crítico), A (Importante) y M (Apreciable) ya que ellos requieren más atención y que sea de manera oportuna.

El plan de tratamiento de riesgos para los activos de la entidad se encuentra estipulado en el siguiente cuadro.

Cuadro 28. Plan de tratamiento de riesgos de los activos de la entidad

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Riesgo		PTR
[D] Datos / Información	[copias_seguridad]	[E.2] Errores del administrador	Fallo en la creación de copias de seguridad	MA	Crítico	Verificar el correcto funcionamiento de las copias de seguridad creadas.
	[Pass_empleados]	[E.2] Errores del administrador	Falta de control sobre contraseñas inseguras	A	Importante	Verificar la seguridad de las contraseñas de los empleados.
						Crear políticas de contraseñas seguras.
		[E.19] Fugas de información	Contraseñas inseguras	A	Importante	Crear políticas de contraseñas seguras.
		[A.11] Acceso no autorizado	Contraseñas inseguras	A	Importante	Crear políticas de contraseñas seguras.
[S] Servicios	[gest_privilegios]	[E.2] Errores del administrador	Asignación de privilegios inadecuados a usuarios	M	Apreciable	Revisión de privilegios asignados a los usuarios.

Fuente: Esta investigación.

Cuadro 28. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Riesgo		PTR
[SW] Software	[antivirus]	[E.2] Errores del administrador	Instalación de software no licenciado	M	Apreciable	Compra de antivirus legal.
		[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de actualización de firmas de virus.	M	Apreciable	Programar la actualización del programa y de las firmas de virus.
	[os_servidor]	[E.2] Errores del administrador	Configuraciones inadecuadas	A	Importante	Capacitación del administrador de sistemas sobre el manejo y uso del sistema operativo del servidor.
		[E.15] Alteración accidental de la información	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones	MA	Crítico	Asegurar el área de cuarto de comunicaciones.
		[E.20] Vulnerabilidades de los programas (software)	Falta de parches y actualizaciones en el software	A	Importante	Verificar las sugerencias sobre parches y actualizaciones del sistema.
		[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de parches y actualizaciones en el software	A	Importante	Verificar las sugerencias sobre parches y actualizaciones del sistema.
		[A.5] Suplantación de la identidad del usuario	Contraseñas inseguras	MA	Crítico	Crear políticas de contraseñas seguras.

Fuente: Esta investigación.

Cuadro 28. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Riesgo		PTR
[SW] Software	[os_servidor]	[A.8] Difusión de software dañino	Falta de antivirus licenciados y actualizados, puertos abiertos	MA	Crítico	Adquirir software antivirus licenciado.
						Configurar parámetros de actualización de firmas de virus y análisis de los equipos.
						Verificar la utilización de puertos del sistema.
	[os_servidor]	A.11] Acceso no autorizado	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones	MA	Crítico	Asegurar el área de cuarto de comunicaciones.
		[A.15] Modificación deliberada de la información	Facilidad de acceso de personal no autorizado al cuarto de comunicaciones y contraseñas inseguras en el sistema	MA	Crítico	Asegurar el área de cuarto de comunicaciones.
						Crear políticas de contraseñas seguras.
	[os_Pcs]	[E.8] Difusión de software dañino	Propagación de virus por falta de antivirus licenciado, puertos abiertos.	A	Importante	Adquirir software antivirus licenciado.
						Configurar parámetros de actualización de firmas de virus y análisis de los equipos.
						Verificar la utilización de puertos del sistema.

Fuente: Esta investigación.

Cuadro 28. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Riesgo		PTR
[SW] Software	[os_Pcs]	[A.11] Acceso no autorizado	Falta de cuentas de usuario con contraseñas seguras	M	Apreciable	Creación de cuentas de usuario con contraseñas en el SO.
	[navegador]	[E.8] Difusión de software dañino	Descarga de malware	M	Apreciable	Actualización de firmas de virus.
						Limitar el acceso a páginas inadecuadas.
	[info_salud]	[A.5] Suplantación de la identidad del usuario	Contraseñas inseguras	MA	Crítico	Crear políticas de contraseñas seguras.
	[info_salud]	[A.11] Acceso no autorizado	Contraseñas inseguras	MA	Crítico	Crear políticas de contraseñas seguras.
		[A.15] Modificación deliberada de la información	Contraseñas inseguras	A	Importante	Crear políticas de contraseñas seguras.
		[A.24] Denegación de servicio	Recursos del servidor insuficientes para las necesidades del sistema.	M	Apreciable	Revisión del cumplimiento de los requerimientos del sistema.
[HW] Equipos Informáticos	[servidor]	[I.5] Avería de origen físico o lógico	Daño en los equipos por tiempo de uso y lugar de exposición.	M	Apreciable	Crear planes de mantenimiento preventivo de acuerdo al uso y lugar de ubicación de los equipos.
						Revisión del estado de los componentes.
						Respaldo de copias de seguridad en discos duros alternos y la nube.

Fuente: Esta investigación.

Cuadro 28. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Riesgo		PTR
[HW] Equipos Informáticos	[servidor	[E.24] Caída del sistema por agotamiento de recursos	Recursos del equipo insuficientes para las necesidades del sistema.	M	Apreciable	Revisión del cumplimiento de los requerimientos del sistema.
		[A.11] Acceso no autorizado	Falta de control de acceso	A	Importante	Asegurar el área de cuarto de comunicaciones.
		[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	A	Importante	Asegurar el área de cuarto de comunicaciones.
[COM] Redes de Comunicaciones	[r_wifi]	[A.7] Uso no previsto	Acceso de los empleados a la red inalámbrica	M	Apreciable	Establecer los parámetros para una red inalámbrica segura.
[MEDIA] Soportes de Información (Electrónico)	[media_dd]	[I.10] Degradación de los soportes de almacenamiento de la información	Daño en los equipos por tiempo de uso y lugar de exposición.	A	Importante	Crear planes de mantenimiento preventivo de acuerdo al uso y lugar de ubicación de los equipos.
						Revisión del estado de los componentes.
						Respaldo de copias de seguridad en la nube.
		[E.2] Errores del administrador	Inadecuada manipulación de los discos duros.	M	Apreciable	Definir el uso y lugar de exposición de los discos duros alternos.

Fuente: Esta investigación.

Cuadro 28. (Continuación)

Grupo de activos	Código activo	Amenazas	Vulnerabilidades	Riesgo		PTR
[MEDIA] Soportes de Información (No Electrónico)	[media_hclinicas]	[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	M	Apreciable	Revisión del estado de las instalaciones.
		[E.19] Fugas de información	Extracción de información confidencial	M	Apreciable	Realizar acuerdos de confidencialidad con los empleados.
[AUX] Equipamiento Auxiliar	[ups]	[A.25] Robo	Deficiencia en la seguridad del cuarto de comunicaciones.	M	Apreciable	Implementar sistemas de seguridad en el cuarto de comunicaciones.
[AUX] Equipamiento Auxiliar	[cab_estructurado]	[N.1] Fuego	Instalaciones eléctricas inadecuadas	M	Apreciable	Revisar el cumplimiento del reglamento técnico de instalaciones eléctricas (RETIE)
		[I.7] Condiciones inadecuadas de temperatura o humedad	Humedad en las instalaciones.	M	Apreciable	Revisión del estado de las instalaciones.
[P] Personal	[admin_sist]	[E.7] Deficiencias en la organización	Inadecuada asignación de funciones al administrador.	M	Apreciable	Creación de un manual de funciones para los empleados.
		[E.28] Indisponibilidad del personal	Ausencia laboral por enfermedad.	M	Apreciable	Contratación de personal alterno.

Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO B. Plan de tratamiento de riesgos, hoja PTR (Riesgos MA-A-M).**

1.10 Dominios y objetivos de control norma iso 27002

La norma ISO 27002 se encuentra organizada mediante 14 dominios y 35 objetivos de control; de los cuales para continuar con el desarrollo del proyecto en esta etapa se debieron seleccionar los que fueron aplicables, basándose en los activos encontrados en la E.S.E Centro Hospital Luis Antonio Montero. En la siguiente tabla se muestra el resultado de esta selección.

Cuadro 29. Selección de dominios, objetivos de control y controles de la Norma ISO 27002

Dominios	Objetivos de control	Controles
5. Políticas de Seguridad	5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Políticas para la seguridad de la información
		5.1.2 Revisión de las políticas para la seguridad de la información
6. Aspectos Organizativos	6.1 Organización interna	6.1.1 Asignación de responsabilidades para la SI
	6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad
7. Seguridad Ligada a los recursos humanos	7.2 Durante la contratación	7.2.2 Concienciación, educación y capacitación en SI
		7.2.3 Proceso disciplinario
	7.3 Cese o cambio de puesto de trabajo	7.3.1 Cese o cambio de puesto de trabajo
8. Gestión de activos	8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos
		8.1.2 Propiedad de los activos
		8.1.3 Uso aceptable de los activos
		8.1.4 Devolución de activos
	8.3 Manejo de los soportes de almacenamiento	8.3.1 Gestión de soportes extraíbles
		8.3.2 Eliminación de soportes
		8.3.3 Soportes físicos en tránsito

Fuente: Adaptación de la Norma ISO 27002.

Cuadro 29. (Continuación)

Dominios	Objetivos de control	Controles
9. Control de Accesos	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de accesos
		9.1.2 Control de acceso a las redes y servicios asociados
	9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios
		9.2.2 Gestión de los derechos de acceso asignados a usuarios
		9.2.4 Gestión de información confidencial de autenticación de usuarios
		9.2.5 Revisión de los derechos de acceso de los usuarios
		9.2.6 Retirada o adaptación de los derechos de acceso
	9.3 Responsabilidades del usuario	9.3.1 Uso de información confidencial para la autenticación
	9.4 Control de acceso a sistemas y aplicaciones	9.4.1 Restricción del acceso a la información
		9.4.2 Procedimientos seguros de inicio de sesión
		9.4.3 Gestión de contraseñas de usuario
11. Seguridad física y Ambiental	11.1 Áreas seguras	11.1.1 Perímetro de seguridad física
		11.1.2 Controles físicos de entrada
		11.1.3 Seguridad de oficinas, despachos y recursos
		11.1.4 Protección contra las amenazas externas y ambientales
	11.2 Seguridad de los equipos	11.2.2 Instalaciones de suministro
		11.2.3 Seguridad del cableado

Fuente: Adaptación de la Norma ISO 27002.

Cuadro 29. (Continuación)

Dominios	Objetivos de control	Controles
11. Seguridad física y Ambiental	11.2 Seguridad de los equipos	11.2.4 Mantenimiento de los equipos
12. Seguridad en la Operativa	12.2 Protección contra código malicioso	12.2.1 Controles contra el código malicioso
	12.3 Copias de seguridad	12.3.1 Copias de seguridad de la información
	12.5 Control del software en explotación	12.5.1 Instalación del software en sistemas en producción
	12.6 Gestión de la vulnerabilidad técnica	12.6.2 Restricciones en la instalación de software
	12.7 Consideraciones de las auditorías de los sistemas de información	12.7.1 Controles de auditoría de los sistemas de información
13. Seguridad en las Telecomunicaciones	13.1 Gestión de la seguridad en las redes	13.1.1 Controles de red
		13.1.3 Segregación de redes.
14. Adquisición, desarrollo y Mantenimiento de los sistemas de información	14.2 Seguridad en los procesos de desarrollo y soporte	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Fuente: Adaptación de la Norma ISO 27002.

Este material también se puede consultar en el **ANEXO C. Documento unificado ISO-IEC 27001 - 27002 y matriz de aplicabilidad, hoja Dominios-objetivos-controles.**

1.11 Lista de chequeo

De acuerdo a los dominios, objetivos de control y controles seleccionados anteriormente de la Norma ISO 27002, se realizó una lista de chequeo formulando preguntas para cada control en el cual las opciones de respuesta fueron SI o No, además de una columna de Observaciones para posibles aclaraciones. Mediante este proceso se pretendió verificar la existencia o inexistencia de los controles sobre los activos de la E.S.E Luis Antonio Montero.

A continuación, se presenta las respuestas obtenidas respecto al dominio 8. Gestión de activos de la lista de chequeo aplicada a la entidad. Debido a la extensión de las preguntas realizadas por los dominios seleccionados, el formato completo se encuentra en el **ANEXO C. Documento unificado ISO-IEC 27001 - 27002 y matriz de aplicabilidad, hoja Lista de chequeo.**

Cuadro 30. Lista de chequeo dominio 8 gestión de activos

Dominio	Objetivo de control	Control	Descripción	Pregunta	SI	NO	Observaciones
8. Gestión Activos	8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos	Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.	¿Todos los activos están claramente identificados manteniendo un inventario con los más importantes?		X	

Fuente: Esta investigación.

Cuadro 30. (Continuación)

Dominio	Objetivo de control	Control	Descripción	Pregunta	SI	NO	Observaciones
8. Gestión Activos	8.1 Responsabilidad sobre los activos	8.1.2 Propiedad de los activos	Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.	¿Dentro de la organización existe personal asignado para el tratamiento de los activos y el inventario asociado a los recursos de la información?	X		
		8.1.3 Uso aceptable de los activos	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.	¿Se identifican, documentan e implantan regulaciones para el uso adecuado de la información y los activos asociados a esta?	X		Se identifican e implantan regulaciones, pero no se tiene documentado el uso de la información y los activos asociados a estos.
		8.1.4 Devolución de activos	Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.	¿Los empleados devuelven los activos de la organización que estén en su posesión una vez finalice el su contrato o actividades laborales?	X		
	8.3 Manejo de los soportes de almacenamiento	8.3.1 Gestión de soportes extraíbles	Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.	¿Se establece procedimientos para la gestión de los medios informáticos removibles?		X	

Fuente: Esta investigación.

Cuadro 30. (Continuación)

Dominio	Objetivo de control	Control	Descripción	Pregunta	SI	NO	Observaciones
8. Gestión Activos	8.3 Manejo de los soportes de almacenamiento	8.3.2 Eliminación de soportes	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.	¿Se eliminan los medios de almacenamiento de información de forma segura y sin riesgo cuando ya no son requeridos, utilizando procedimientos formales?		X	
		8.3.3 Soportes físicos en tránsito	Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.	¿Se protegen los medios que contienen información contra acceso no autorizado mal uso o corrupción?		X	

Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO C. Documento unificado ISO-IEC 27001 - 27002 y matriz de aplicabilidad, hoja Lista de chequeo.**

Los resultados obtenidos de la aplicación de la lista de chequeo demuestran que principalmente no se cuenta con una política para la seguridad de la información, por consiguiente, se puede ir descartando que se cumpla de manera adecuada el objetivo de resguardar la información y los elementos asociados a ella, en cuanto a fenómenos físicos o humanos sean de carácter involuntario o intencional.

En algunas ocasiones se presentó la opción de que el control no se cumple cabalmente, por ejemplo puede que se tome algunas medidas sobre ciertos aspectos tales como el uso de recursos móviles, uso adecuado de la información y recursos asociados a ella, control de accesos, alta y baja de usuarios, inicios de sesión seguros y contraseñas, pero a pesar de que se implementan diferentes acciones para mantener de forma adecuada estos aspectos; no se cuentan con políticas debidamente establecidas en donde se determine los objetivos y procesos que se deberían cumplir, lo cual hace que se presenten falencias en las medidas que realmente se necesitan y el cumplimiento de ellas.

Además de lo mencionado anteriormente, existieron controles que no se cumplen y que deben ser motivo de revisión inmediata ya que son factores que pueden afectar la seguridad de la información en un grado mínimo o en mayor cantidad, es así el caso de los medios informáticos removibles en los cuales se podría extraer información o infectar con malware los equipos informáticos, también no se tiene en cuenta procesos para la eliminación de medios que contengan información cuando ya no sean requeridos lo que podría causar que la información quede expuesta porque no se tiene control sobre ella. Algo importante que cabe resaltar es que no se da de baja a los usuarios en el momento en que dejan de trabajar con la entidad si no es mediante una solicitud específica, este error puede afectar demasiado ya que la información se puede encontrar en manos de personas que pueden sacar provecho de ella, ya sea modificándola, eliminándola o agregándola. Existen muchos aspectos como estos, que aún no han sido tomados en cuenta en la entidad y se pueden evidenciar en la lista de chequeo realizada.

Así como existen cosas por mejorar también hay aspectos que se encuentran implementados de la mejor manera, lo cual es un avance; por lo tanto lo ideal sería que se siga reforzando y llevando un control sobre ellos para que exista una mejora continua. Es así el caso de las políticas de historias clínicas en cuanto a formato físico, las cláusulas de contratos en cuanto a compromisos y responsabilidades, el inventario de los activos de la entidad, entre otros.

1.12 Nivel de cumplimiento

El nivel de cumplimiento se determinó por cada dominio seleccionado y permitió medir en una escala de porcentaje la madurez de los dominios evaluados en la E.S.E Luis Antonio Montero.

Para obtener el nivel de cumplimiento se debió tener el total de las preguntas realizadas por dominio y el número de respuestas obtenidas con descripción de SI y NO. De acuerdo a esto, al número total de las preguntas se le resta las respuestas con descripción NO y este resultado se dividió entre el Número total de preguntas realizadas; al valor obtenido se lo multiplicó por 100 y de esta manera se consiguió el porcentaje del nivel de cumplimiento. Acorde a lo explicado se tiene que:

$$Nivel\ de\ cumplimiento\ por\ Dominio = \left(\frac{Total\ preguntas - Respuestas\ NO}{Total\ preguntas}\right)\ x\ 100$$

Ejemplo para calcular el nivel de cumplimiento por dominio:

- Total, preguntas por dominio = 4
- Total, respuestas NO = 2

Por medio de los datos proporcionados y reemplazando en la formula se obtuvo el siguiente resultado:

$$Nivel\ de\ cumplimiento\ por\ Dominio = \left(\frac{4-2}{4}\right)\ x\ 100$$

$$Nivel\ de\ cumplimiento\ por\ Dominio = (0.5)\ x\ 100$$

$$Nivel\ de\ cumplimiento\ por\ Dominio = 50\ \%$$

En este caso el nivel de cumplimiento con estos datos dio un resultado del 50%.

Mediante lo explicado anteriormente, se procedió a determinar el nivel de cumplimiento para cada uno de los dominios seleccionados, obteniendo los siguientes resultados.

Cuadro 31. Nivel de cumplimiento por dominio

Dominio	Objetivo de control	Control	SI	NO	(%) Nivel de cumplimiento
5. Políticas Seguridad	5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Políticas para la seguridad de la información		X	0
		5.1.2 Revisión de las políticas para la seguridad de la información		X	
6. Aspectos Organizativos SI	6.1 Organización interna	6.1.1 Asignación de responsabilidades para la SI	X		100
	6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad	X		
7.Seguridad Ligada a los RRHH	7.2 Durante la contratación	7.2.2 Concienciación, educación y capacitación en SI	X		100
		7.2.3 Proceso disciplinario	X		
	7.3 Cese o cambio de puesto de trabajo	7.3.1 Cese o cambio de puesto de trabajo	X		
8. Gestión Activos	8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos	X		57
		8.1.2 Propiedad de los activos	X		
		8.1.3 Uso aceptable de los activos	X		
		8.1.4 Devolución de activos	X		
	8.3 Manejo de los soportes de almacenamiento	8.3.1 Gestión de soportes extraíbles		X	
		8.3.2 Eliminación de soportes		X	
		8.3.3 Soportes físicos en tránsito		X	

Fuente: Esta investigación.

Cuadro 31. (Continuación)

Dominio	Objetivo de control	Control	SI	NO	(%) Nivel de cumplimiento
9. Control de Accesos	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de accesos	X		45
		9.1.2 Control de acceso a las redes y servicios asociados		X	
	9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios		X	
		9.2.2 Gestión de los derechos de acceso asignados a usuarios		X	
		9.2.4 Gestión de información confidencial de autenticación de usuarios	X		
		9.2.5 Revisión de los derechos de acceso de los usuarios		X	
		9.2.6 Retirada o adaptación de los derechos de acceso		X	
	9.3 Responsabilidades del usuario	9.3.1 Uso de información confidencial para la autenticación	X		
	9.4 Control de acceso a sistemas y aplicaciones	9.4.1 Restricción del acceso a la información	X		
		9.4.2 Procedimientos seguros de inicio de sesión	X		
		9.4.3 Gestión de contraseñas de usuario		X	

Fuente: Esta investigación.

Cuadro 31. (Continuación)

Dominio	Objetivo de control	Control	SI	NO	(%) Nivel de cumplimiento
11. Seguridad física y Ambiental	11.1 Áreas seguras	11.1.1 Perímetro de seguridad física	X		86
		11.1.2 Controles físicos de entrada		X	
		11.1.3 Seguridad de oficinas, despachos y recursos	X		
		11.1.4 Protección contra las amenazas externas y ambientales	X		
	11.2 Seguridad de los equipos	11.2.2 Instalaciones de suministro	X		
		11.2.3 Seguridad del cableado	X		
		11.2.4 Mantenimiento de los equipos	X		
12. Seguridad en la Operativa	12.2 Protección contra código malicioso	12.2.1 Controles contra el código malicioso		X	0
	12.3 Copias de seguridad	12.3.1 Copias de seguridad de la información		X	
	12.5 Control del software en explotación	12.5.1 Instalación del software en sistemas en producción		X	
	12.6 Gestión de la vulnerabilidad técnica	12.6.2 Restricciones en la instalación de software		X	
	12.7 Consideraciones de las auditorías de los sistemas de información	12.7.1 Controles de auditoría de los sistemas de información		X	

Fuente: Esta investigación.

Cuadro 31. (Continuación)

Dominio	Objetivo de control	Control	SI	NO	(%) Nivel de cumplimiento
13. Seguridad en las Telecomunicaciones	13.1 Gestión de la seguridad en las redes	13.1.1 Controles de red		X	50
		13.1.3 Segregación de redes.	X		
14. Adquisición, desarrollo y Mantenimiento de los sistemas de información	14.2 Seguridad en los procesos de desarrollo y soporte	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	X		100

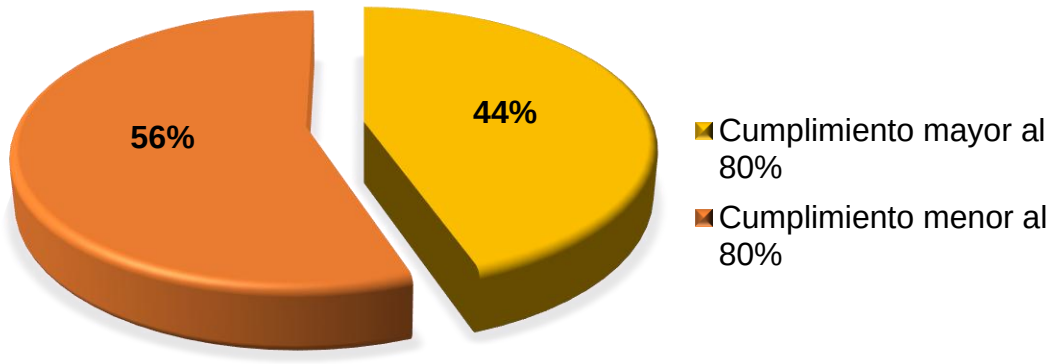
Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO C. Documento unificado ISO-IEC 27001 - 27002 y matriz de aplicabilidad, hoja Nivel de cumplimiento.**

1.12.1 Gráfico nivel de cumplimiento

Analizando la información obtenida del porcentaje del nivel de cumplimiento por dominio, se pudo evidenciar que de los nueve dominios seleccionados solo cuatro de ellos (6. Aspectos Organizativos SI, 7. Seguridad Ligada a los recursos humanos, 11. Seguridad física y Ambiental y 14. Adquisición, desarrollo y Mantenimiento de los sistemas de información) tuvieron un cumplimiento con más del 80 %. Los dominios restantes tuvieron porcentajes que van desde el 57 % hasta un 0 % de nivel cumplimiento, estos dominios presentaron deficiencias en el cumplimiento de controles para la seguridad de la información en la E.S.E centro hospital Luis Antonio Montero y deben ser tratados para mejorarlos. En el siguiente gráfico se puede evidenciar a cuanto equivale el porcentaje de los dominios con más del 80 % de cumplimiento y cuales con menos del 80 %.

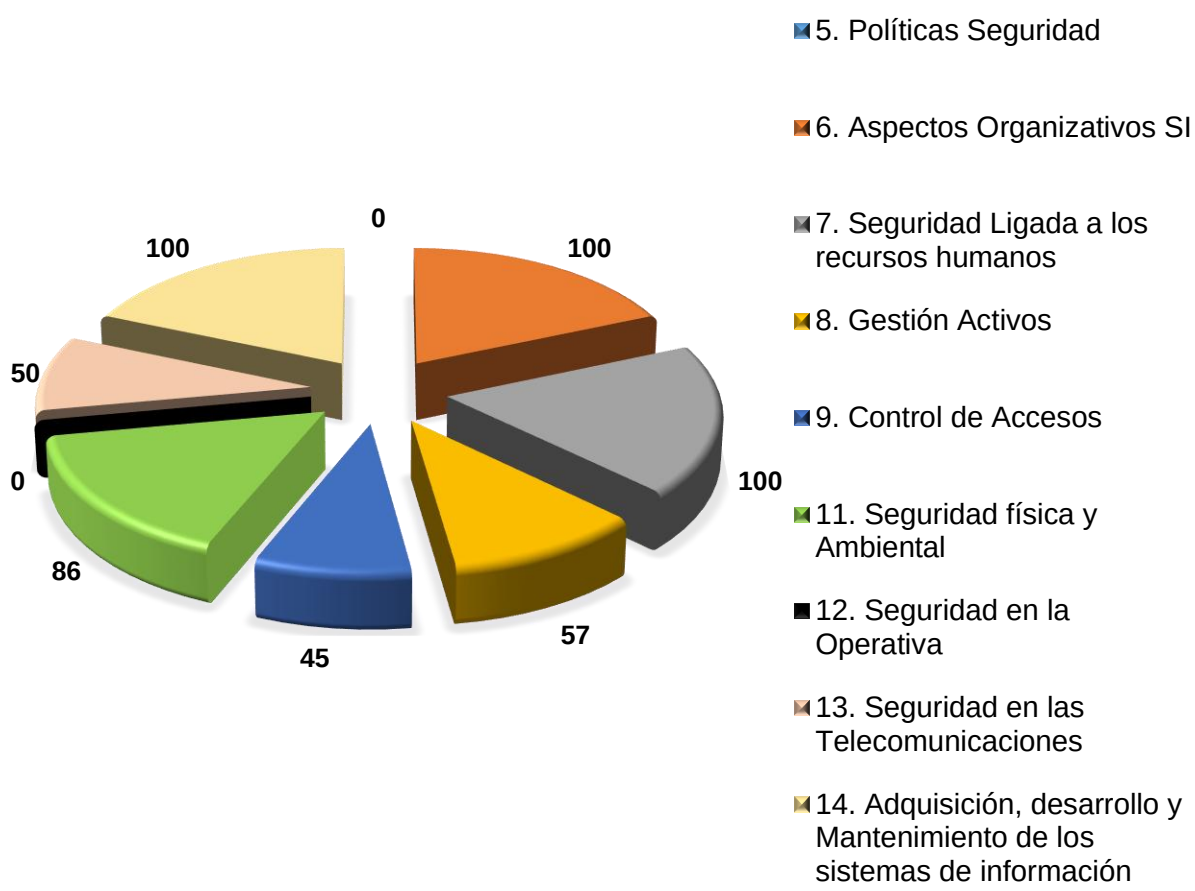
Gráfico 4. Proporción del nivel de cumplimiento de los dominios



Fuente: Esta investigación.

Para detallar de una manera más clara los resultados obtenidos del nivel de cumplimiento por cada dominio en la E.S.E Luis Antonio Montero, se realizó el siguiente gráfico circular en el cual se puede evidenciar cuales dominios tuvieron mayor y menor nivel de cumplimiento.

Gráfico 5. Proporción del nivel de cumplimiento por dominio.



Fuente: Esta investigación.

De los nueve dominios y los controles analizados de la norma ISO/IEC 27001 e ISO/IEC 27002 mediante el grafico anterior se pudo evidenciar lo siguiente.

- Los dominios 5. Políticas de seguridad y 12. Seguridad en la operativa tuvieron un nivel de complimiento del 0%; esto es debido a que ninguno de los controles analizados es implementado por la entidad, lo cual debe ser tenido en cuenta para una posterior mejora que ayude a incrementar estos niveles de cumplimiento de una manera significativa.

- Los dominios 6. Aspectos organizativos SI, 7. Seguridad ligada a los recursos humanos y 14. Adquisición, desarrollo y mantenimiento de los sistemas de información tuvieron un nivel de cumplimiento del 100% esto es debido a que la entidad tiene implementado aspectos establecidos de los controles de la norma, esto permite destacar que la entidad tiene un buen desempeño en cuanto a estos procesos.

- Los dominios restantes mostraron un nivel de desempeño intermedio ya que cumplieron de cierta manera algunos aspectos de los controles de la norma, es por esto que no deben ser dejados de tener en cuenta para su futuro tratamiento y mejoramiento para que de esta manera alcancen un nivel óptimo.

Este material también se puede consultar en el **ANEXO C. Documento unificado ISO-IEC 27001 - 27002 y matriz de aplicabilidad, hoja Gráficos nivel de cumplimiento.**

1.13 Declaración de aplicabilidad

La declaración de aplicabilidad determinó cuáles son los controles existentes y cuáles son los que hacen falta implementar en la organización de acuerdo a las respuestas obtenidas de la lista de chequeo y sus observaciones. De esta manera para cada control se establecieron cinco columnas de las cuales, en las dos primeras se especificó si el control existe o no existe, en las dos siguientes se determinó si el control es aplicable o no es aplicable en la entidad y en la columna final se presentó una justificación en donde se explica si se encontró implementado o en caso contrario porque se debería implementar.

La declaración de aplicabilidad para el centro hospital Luis Antonio Montero muestra de forma resumida lo que esta y no está implementado en la entidad y permite que de esta manera sea más fácil saber en qué aspectos se requiere atención inmediata, en cuales se debe realizar algunas mejoras y en cuales se debe mantener un control para mantener lo que se tiene. Además, esta declaración sirve como referencia en el momento de iniciar el proceso para la creación de las políticas de seguridad necesarias y posteriormente un sistema de gestión de seguridad de la información.

A continuación, se presenta la declaración de aplicabilidad para el dominio 8. Gestión de activos en donde se especificó si el control existe o no en la entidad y su respectiva justificación. Debido a la extensión de la declaración para cada dominio y controles establecidos, esta se encuentra redactada en el **ANEXO C. Documento unificado ISO-IEC 27001 - 27002 y matriz de aplicabilidad, hoja Declaración de aplicabilidad.**

Cuadro 32. Declaración de aplicabilidad por dominio

Dominio	Objetivo de control	Control	Existe	No existe	Es aplicable	No es aplicable	Justificación
8. Gestión Activos	8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos	X		X		En cualquier organización sea cual sea su objeto es importante llevar un inventario, esto ayuda a llevar un orden de que activos están presentes en dichas instalaciones.

Fuente: Esta investigación.

Cuadro 32. (Continuación)

Dominio	Objetivo de control	Control	Existe	No existe	Es aplicable	No es aplicable	Justificación
8. Gestión Activos	8.1 Responsabilidad sobre los activos	8.1.2 Propiedad de los activos	X		X		En el centro hospital existe un encargado de llevar el control de los activos esta persona tiene a su cargo el área de almacén y es la directamente responsable sobre cada activo, en especial los activos informáticos.
		8.1.3 Uso aceptable de los activos	X		X		Se hace uso adecuado de los activos y se identifican e implantan regulaciones sobre estos sin embargo se recomienda que este proceso este documentado.
		8.1.4 Devolución de activos	X		X		Existe un control de los activos, por tanto, los empleados del centro hospital una vez finaliza su relación laboral con la entidad hacen la respectiva devolución de activos que se encuentren bajo su responsabilidad.
	8.3 Manejo de los soportes de almacenamiento	8.3.1 Gestión de soportes extraíbles		X	X		Se debería implementar el control sobre el uso de dispositivos extraíbles sobre todo en dispositivos de almacenamiento, ya que el mal uso de estos implicaría perdida de valiosa información del centro hospital.

Fuente: Esta investigación.

Cuadro 32. (Continuación)

Dominio	Objetivo de control	Control	Existe	No existe	Es aplicable	No es aplicable	Justificación
8. Gestión Activos	8.3 Manejo de los soportes de almacenamiento	8.3.2 Eliminación de soportes		X	X		Se justifica tener un plan o manejo de protocolo sobre el uso adecuado de dispositivos de almacenamiento ya que se controlaría la eliminación de información dentro de los soportes.
		8.3.3 Soportes físicos en tránsito		X	X		No toda la información en el centro de salud esta almacenada en un medio electrónico existe documentación que está impresa por lo tanto se recomienda su protección y debe tener alguien encargado que lleve el control si se la necesita trasladar de un área a otra.

Fuente: Esta investigación.

Este material también se puede consultar en el **ANEXO C. Documento unificado ISO-IEC 27001 - 27002 y matriz de aplicabilidad, hoja Declaración de aplicabilidad.**

2. PLANES DE MEJORAMIENTO

Una vez identificadas las amenazas y determinado el riesgo e impacto derivado de la posible materialización de las mismas sobre los activos de la entidad, se han presentado las siguientes propuestas de mejoras integrales para que puedan ser tenidas en cuenta como base al momento de realizar la política de seguridad de la información correspondiente para la E.S.E Centro Hospital Luis Antonio Montero, de acuerdo a los hallazgos encontrados en el transcurso del desarrollo de este proyecto.

1. Plan de mejora. Uso de dispositivos móviles

Objetivo. Usar de una manera correcta los dispositivos móviles en horario laboral.

Responsables. Se debe definir un supervisor del cual dependerá se dé cumplimiento a lo antes mencionado.

Consideraciones.

Se entiende como dispositivo móvil:

- Celulares, smartphones.
- Tablets.
- Portátiles.
- Dispositivos reproductores.
- GPS.

Los empleados en el centro hospital deben tener conocimiento que el uso de dispositivos móviles tales como celulares, tablets, portátiles etc. para fines personales se deben hacer en horario extra laboral.

Se debe restringir el uso compartido de la información del centro hospital usando estos medios, por el nivel de riesgo existente en la pérdida o sustracción de la misma.

Beneficios

El principal beneficio se verá reflejado en la buena prestación de los servicios y mayor rendimiento en las funciones del personal de trabajo del centro hospital.

2. Plan de mejora. Uso adecuado de los activos

Objetivo. Establecer los lineamientos a fin de clasificar, organizar y dar buen uso de los activos existentes en el centro hospital Luis Antonio montero.

Responsables. Personal encargado de llevar la relación de los activos existentes en la entidad y cada empleado que tenga a su cargo activos asignados.

Consideraciones.

Se debe definir la información como el activo más importante en el centro hospital la cual requiere protección, clasificación y cuidado.

Todo activo debe tener:

- Un identificador
- Un nombre
- Un propietario
- Una dependencia
- Un delegado

Se debe tener en cuenta la fecha de ingreso y salida de un activo en el inventario, el tipo de activo, si es hardware, software, de información, físico, servicios, etc., descripción del estado y además su respectiva clasificación.

Beneficios

Se tendrá un mayor control sobre los activos existentes en la entidad, identificando su uso, estado, además de la persona responsable de él en la entidad.

3. Plan de mejora. Manejo adecuado de contraseñas

Objetivo. Establecer los criterios necesarios para la creación y manejo de contraseñas.

Responsables. Encargado del área de sistemas y empleados de la entidad que hagan uso de los computadores y aplicativos.

Consideraciones.

Las contraseñas permiten asegurar las plataformas tecnológicas y así poder dar garantía en cuanto a confidencialidad, integridad y disponibilidad de la información por lo que es de carácter confidencial su manejo.

Los empleados, contratistas y terceros que tengan acceso al sistema Infosalud, y en si tengan acceso a cualquier estación de trabajo debe:

- Custodiar la contraseña con el mayor de los cuidados,
- Tomar responsabilidad ante la entidad por cualquier uso indebido que se le pueda dar.
- Conocer los cuidados que deben tener con esta y los posibles fraudes que se pueden cometer por su uso indebido.

No es recomendable:

- Utilizar la opción de almacenar contraseña cuando el aplicativo es de tipo web.
- Utilizar contraseñas que sean obvias como números telefónicos, nombres propios o de familiares, apellidos, fechas, etc.
- Guardar en algún medio físico la contraseña como escritos en papel, agendas, notas etc.
- Compartir las contraseñas con otros funcionarios del personal.
- Utilizar contraseñas muy débiles.

Se aconseja:

- Utilizar más de 8 caracteres para estaciones de trabajo en cada dependencia del centro hospital.
- Utilizar más de 12 caracteres para servidores y equipos de comunicación.
- Utilizar combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
- Se debe tener confidencialidad en todo momento.
- Cambiar periódicamente la contraseña.

Beneficios

Se tendrá mayor seguridad, confidencialidad e integridad sobre la información que se maneja en la entidad.

No existirán accesos indebidos por personal diferente al especificado para cierto cargo.

4. Plan de mejora. Mantenimiento en equipos de cómputo del centro hospital

Objetivo. Crear lineamientos para el proceso de mantenimiento sobre los equipos de cómputo.

Responsables. Encargado de sistemas o empresa contratista que se encargue de este procedimiento.

Consideraciones.

El mantenimiento en los equipos de cómputo es de vital importancia ya que ayuda a prevenir errores en el sistema, así como a corregirlos por eso se debe tener las siguientes consideraciones para realizar un buen proceso de mantenimiento.

- El tipo de mantenimiento puede ser: preventivo, correctivo, predictivo y de actualización.

- Debe existir un encargado de realizar los mantenimientos necesarios para los equipos de la entidad, él es el directamente responsable de velar por la salud de los equipos de cómputo.
- Los mantenimientos se deben realizar en todas las estaciones de trabajo y en los equipos servidores del centro hospital según sean requeridos.
- Los equipos de la entidad deben tener creada una hoja de vida para llevar la bitácora de mantenimiento. En este formato estará plasmado quien realizara el mantenimiento, el tipo de mantenimiento a realizar, las características del equipo, el tipo de mantenimiento, la fecha en la que se realizó, observaciones por si se encuentra algún defecto y la firma de la aprobación del gerente encargado.
- Cada vez que exista un cambio o modificación del equipo, se debe actualizar la hoja de vida.

Beneficios:

La infraestructura tecnológica donde se procesa y almacena la información tendrá mayor vida útil y no generará perdidas de información o estancos en procesos debido al no funcionamiento de los equipos.

Realizar los mantenimientos en el tiempo adecuado y de manera acorde a los equipos reducen el riesgo de fallos y de costos generados por complicaciones con el hardware.

5. Plan de mejora. Red de datos del centro hospital

Objetivo. organizar la estructura de red del centro hospital

Responsables. Para realizar una buena organización en la red de datos del centro hospital el directamente responsable de esta tarea es el jefe del departamento de sistemas de la entidad, en él está la función de realizar una buena segmentación de red, así como una buena organización y asignación de direccionamiento IP para los equipos de cómputo.

Consideraciones

- Se debe empezar por realizar un buen diseño de topología de red tanto lógica como física, tener en cuenta todos los elementos de red a utilizarse como routers, switches, Access point, cable UTP, además de las normas técnicas existentes para que rigen el cableado estructurado.
- Organizar cuantos puntos de red van a ser necesarios de acuerdo al número de estaciones de trabajo en el centro hospital.
- Segmentar la red para la asignación de las direcciones IP a cada equipo de cómputo.
- Llevar un registro de los puntos de red activo y no activos para tener control sobre estos.
- Los puntos de red que no sean utilizados por ningún equipo deben estar sellados o en su defecto no presentar conexión con el cuarto de comunicaciones.

Beneficios

Se podrá tener más seguridad en la información, porque al no tener una buena organización en la red de datos y mediante la no utilización de un punto de red que este accesible a personas ajenas a la entidad, se puede acceder al sistema y hurtar información importante.

Mayor calidad de la prestación de servicios.

Buena utilización de los recursos.

6. Plan de mejora. Acceso al cuarto de comunicaciones

Objetivo. Fortalecer la seguridad de las instalaciones que albergan los equipos servidores del sistema Infosalud en el centro hospital.

Responsables. La responsabilidad recae para las directrices del centro de salud, cuerpo de vigilancia contratado por la entidad y quien manipule estos equipos.

Consideraciones

- Dentro del centro de salud se debe adecuar un espacio dedicado a albergar los equipos servidores del sistema Infosalud.
- Este espacio debe tener las normas técnicas necesarias.
- Se debe tener en cuenta las normas de seguridad en cuanto al acceso a este espacio.
- Quien este encargado de la vigilancia debe llevar un control de ingreso en él, debe registrar quien entra, quien sale, llevando el respectivo registro de fecha y hora.

Beneficios

El mayor de los beneficios es la seguridad y la preservación del buen estado de los equipos.

Garantizar el buen funcionamiento de los equipos y por ende el buen funcionamiento a nivel operativo.

Proteger contra intrusiones los equipos de cómputo y los equipos servidores de la entidad y así garantizar la integridad de la información.

7. Plan de mejora. Eliminar usuarios del sistema

Objetivo. Crear un protocolo para dar de baja a un usuario del sistema.

Responsables. El encargado del área de sistemas es el encargado de dar de baja a un usuario en el sistema.

Consideraciones

Cuando un usuario del sistema ya no tenga ninguna obligación contractual con la entidad se debe eliminar sus credenciales de ingreso tanto en los aplicativos de la entidad, como en el sistema operativo de los equipos.

Se puede restringir el acceso del personal retirado de la entidad al sistema operativo mediante el cambio de contraseña de la cuenta del sistema operativo.

Se debe eliminar todo registro y contraseñas existentes del usuario excluido en el sistema Infosalud para que no pueda acceder a la información que proporciona este aplicativo.

Beneficios

El mayor de los beneficios es preservar la integridad de la información.

Se garantiza que personas ajenas al centro de salud no puedan manipular el sistema y sustraer información importante.

Realizar una depuración al sistema Infosalud genera un incremento en su funcionalidad.

3. CONCLUSIONES

Mediante las visitas realizadas a la E.S.E Centro Hospital Luis Antonio Montero se pudo analizar el sistema utilizado en la entidad además de los activos que se relacionan con él, logrando determinar cuáles pueden ser las posibles vulnerabilidades y amenazas que podrían materializarse sobre ellos mediante observación directa y entrevistas realizadas a los empleados.

Por medio de la metodología de trabajo utilizada, MAGERIT; se pudo clasificar los activos de la entidad y evaluar de manera cualitativa y cuantitativa cada uno de ellos; de acuerdo a esto se pudo valorar las amenazas y vulnerabilidades que se pueden materializar determinando de esa manera el impacto, frecuencia y riesgo, para establecer cuáles deben ser tratados de manera inmediata.

De acuerdo a los hallazgos encontrados con la metodología, se pudo realizar el plan de tratamiento de riesgos correspondiente a los activos que presentaban un nivel crítico, apreciable e importante; por lo cual la E.S.E Centro Hospital Luis Antonio Montero podrá tener presente este plan para realizar una política de seguridad de la información junto con otros papeles de trabajo que resultaron de esta investigación como son la matriz de aplicabilidad, las recomendaciones y planes de mejoramiento.

Mediante las normas ISO/IEC 27001 e ISO/IEC 27002 se estableció los dominios, objetivos de control y controles de acuerdo a los activos de la entidad y con la ayuda de la lista de chequeo, se ha determinado el nivel de cumplimiento de los dominios en la entidad; por lo cual se ha logrado establecer la matriz de aplicabilidad que permitirá tener como referencia los controles que se tienen o no, para que de esta manera se pueda realizar las respectivas correcciones en los casos donde se identifique la falta de controles.

La información de la E.S.E Centro Hospital Luis Antonio Montero es uno de los activos más importantes, por lo que se debe cuidar y preservar su integridad, disponibilidad y confidencialidad, por lo tanto, la entidad por medio de los hallazgos encontrados en esta investigación tendrá la oportunidad de determinar las políticas necesarias para ser creadas e implementadas de la manera más adecuada.

4. RECOMENDACIONES

Las siguientes recomendaciones son necesarias para que las debilidades encontradas en la E.S.E Centro Hospital Luis Antonio Montero se conviertan en fortalezas y así con esto poder mejorar el nivel de productividad y seguridad de la información en dicha entidad.

Después de hacer un análisis a los hallazgos encontrados y a los resultados obtenidos a partir de los papeles de trabajo utilizados en esta auditoria se procedió a hacer las siguientes recomendaciones:

- Para salvaguardar la información se recomienda la creación de políticas de seguridad, políticas en las cuales se deba plasmar el acceso, manipulación y divulgación de la información.

- Si se decide crear políticas para la seguridad de la información, tales como la buena manipulación de la información, confidencialidad de la información, seguridad e integridad de la información, se recomienda que exista un equipo de trabajo responsable con el fin de garantizar su implementación, cumplimiento y constante control en el centro hospital.

- En el centro hospital Luis Antonio Montero se debe crear conciencia a través de charlas y constantes capacitaciones a empleados sobre la importancia de la información como activo fundamental en la organización, por tal motivo es deber de todo el personal velar por su seguridad y protección.

- Para incrementar el nivel de buen servicio, se recomienda regular el uso de dispositivos móviles mediante la creación de una política de uso de dispositivos móviles tales como tablets, celulares, entre otros los cuales puedan disminuir la productividad y atención que requieren los usuarios en la entidad.

- Se sugiere que se haga uso aceptable de los activos, aunque existe un orden y un encargado de llevar el control sobre estos es indispensable que este proceso este documentado para saber qué activos se encuentran, a que dependencia están asignados y quien es el responsable de su uso.

- Para el soporte físico en tránsito que se lleva en el centro hospital se recomienda la protección de toda información que está impresa y no está almacenada en algún dispositivo electrónico para tal motivo debe existir un formato en donde se contemple el ingreso, la salida, el fin para cual se va a usar y un encargado del traslado de esta en caso de ser necesario.

- Se recomienda realizar una política que garantice el control de acceso al sistema Infosalud en donde se debe contemplar la eliminación de usuarios que ya no estén vinculados a la entidad, de igual manera al ingresar al sistema operativo se aconseja tener creadas credenciales de autenticación y estar muy pendientes del puesto de trabajo ya que por lo general se lo abandona dejando iniciada la sesión en el equipo de cómputo.

- Se aconseja tener cuidado y control sobre las redes de datos instaladas en la entidad, se debe desactivar los puntos de acceso a la red que no estén asignados a algún empleado para evitar el robo de la información.

- Cuando un empleado deja de pertenecer a la entidad este debe ser eliminado junto a sus credenciales del sistema que se maneja en el centro de salud, por ello debe existir una política para dar de baja a usuarios que ya no estén vinculados laboralmente con la institución.

- Parte importante en el centro de salud debe ser la organización en cuanto al buen uso del sistema existente, se hace la sugerencia que exista una revisión de los derechos de acceso de los usuarios a través de una política en donde se especifique la configuración de los privilegios de los usuarios del sistema.

- Para evitar que la información confidencial en este caso información de pacientes, trabajadores, información del sistema se filtre en otras organizaciones es recomendable que se trabaje conjuntamente con el departamento jurídico para incluir en los contratos cláusulas que eviten la divulgación de la misma.

- Parte importante de la información es garantizar su seguridad por ello, el buen uso de una contraseña es primordial a la hora de preservar y cuidar de accesos indebido; la recomendación que se hace al centro hospital es tener una política de creación de contraseñas seguras y que estas sean cambiadas con regularidad, dicha contraseña debería tener un nivel alto de seguridad y cumplir con una configuración adecuada.

- Invertir en seguridad puede salir costoso pero vale hacer la recomendación para así garantizar la integridad de los equipos de cómputo por tal motivo se sugiere se haga una mayor inversión en el perímetro de seguridad en donde se encuentren los equipos de cómputo del personal y teniendo mayor cuidado sobre la zona en donde se encuentra ubicado el servidor; debería invertirse en sistemas de seguridad con tecnología basados en autenticación o ingreso a través de una clave de seguridad, lector de huellas digitales etc.

- En cuanto al mantenimiento de equipos se debe proceder como se ha venido trabajando, pero se hace la recomendación que a través de una política se cree un plan de mantenimiento periódico en donde este contemplado una hoja de vida de equipos y se registre las fallas que reporten en cada estación de trabajo.

- La instalación de software que mitigue el riesgo y proteja a los equipos de cómputo de software malicioso es necesario en el centro de salud porque así se evita que se pierda información por tal razón se recomienda que su instalación esté presente en el plan de mantenimiento de equipos de cómputo del centro hospital.

- Una política para la creación y verificación de un plan de respaldo de la información es recomendable en el centro hospital; ya que las copias de seguridad de la información deben tener prioridad en la organización estas se deben hacer de manera periódica, tener un encargado, llevar un registro, un control y verificación de su correcto funcionamiento.

- Es necesario crear un protocolo para instalación y revisión de software en los equipos de trabajo ya que cualquier aplicación que se instale debe quedar documentada en cuanto a su instalación, modificación o eliminación del sistema, además de su debida justificación de la utilidad que representa en la entidad. Las aplicaciones no deben ser instaladas por cualquier usuario sino únicamente por el administrador de sistemas para llevar un control sobre ellas.

- Se aconseja tener prevención en cuanto al uso de dispositivos removibles como USB, discos duros portables ya que estos instrumentos son portadores de virus además de ser el medio por donde se puede extraer información importante, la recomendación se basa en la creación de una política de control sobre dispositivos removibles en donde se especifique su manipulación, su fin, a quien pertenece etc.

- Los archivos digitales que se utilizan en el hospital a menudo contienen información confidencial o estratégica de la actividad que se desarrolla en la entidad, por eso en caso de ser necesario prescindir de dichos soportes se recomienda eliminar la información de manera segura de cualquier dispositivo extraíble, se aconseja se haga una revisión periódica en estos instrumentos de almacenamiento para hacer una constante depuración de la información contenida en ellos y llevar un reporte cuando se requiera eliminar información en donde se especifique el nombre del archivo, la dependencia a la que pertenece, dar una descripción de que contiene, quien se encarga y el por qué se realiza la acción; esto con el fin de llevar un control sobre este proceso.

BIBLIOGRAFÍA

BARRERA Hurtado de, Jacqueline. El Proyecto de Investigación: Sypal; Caracas, 2008.

BICHACHI, Diana Susana. El uso de las Listas de Chequeo (CheskList) como herramienta para controlar la calidad de la ley. [En línea]. Disponible en internet: http://www.claudiabernazza.com.ar/ssgp/html/pdf/check_list.pdf

BURGOS Jenny, DOMINGUEZ María Carolina. Auditoria del módulo de historia clínica electrónica del sistema de información del hospital universitario departamental de Nariño, San Juan de Pasto, 2008. 435h. Trabajo de Grado (ingeniero de sistemas). Universidad de Nariño. Facultad de Ingeniería

CANO, Jeimy. La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes [en línea], 2011, vol. 5. Disponible en internet: https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx

COLUNGE Denis Alfredo, PORTILLA Jorge Alexis. Auditoria al módulo de inventario del sistema de información en el hospital universitario departamental de Nariño, San Juan de Pasto, 2013, 165h. Trabajo de Grado (ingeniero de sistemas). Universidad de Nariño. Facultad de Ingeniería

Coppola y García. Test de Intrusión. [en línea]. Montevideo. Disponible en internet: http://www.cyg.com.uy/documentos/test_de_intrusion.pdf

CORTES CAMACHO Jesús German. Auditoria a la seguridad de la red de datos de la empresa panavias s.a, San Juan De Pasto,2016, 197h, Trabajo de grado, Universidad Abierta Y Distancia “Unad”, Facultad De Ciencias Básicas e Ingeniería

CUELLAR MEJIA, Guillermo Adolfo. Teoría General De La Auditoria y Revisoría Fiscal [en línea]. Septiembre de 2003. Disponible en internet: http://fccea.unicauca.edu.co/old/tgarf/marcos.html

DELGADO ROJAS, Xiomar. Auditoria Informática. [en línea] Euned. 209 p. Disponible en internet: https://vdocuments.site/auditoria-informatica-xiomar-delgado-rojas-uned.html

DUQUE OCHOA, Blanca Rubiela, Metodologías de Gestión de Riesgos 24h, Trabajo Final de auditoria, Universidad de Caldas, Facultad de Ingeniería [en línea]. Disponible en internet: http://docplayer.es/23365963-Metodologias-de-gestion-de-riesgos-octave-magerit-dafp-blanca-rubiela-duque-ochoa-codigo-auditoria-carlos-hernan-gomez.html

ECHENIQUE GARCÍA, José Antonio. Auditoria Informática. Edición 2. McGraw-Hill Interamericana. 2001. 300 p. ISBN 9789701033562.

ERB, Markus. Amenazas y Vulnerabilidades. [en línea]. Disponible en internet: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/ [citado 2016]

-------- Seguridad de la Información y Protección de Datos. [en línea]. Disponible en internet: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/ [citado 2016]

Extracto del documento UNE-EN ISO/IEC 27002, Objeto y campo de aplicación

FERRER, Rodrigo, Metodología de análisis de riesgo, Bogotá Colombia. 7 h. en línea]. Disponible en internet: http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_DE_ANALISIS_DE_RIESGO.pdf

GARCÍA ESTUDILLO, Victoriano. La información como recurso estratégico para las empresas. [en línea]. Gestiopolis. 13 de abril de 2015. [citado en 2016] Disponible en internet: http://www.gestiopolis.com/la-informacion-como-recurso-estrategico-para-las-empresas/

GLASS, G y STANLEY, J.S. Métodos Estadísticos Aplicados a las ciencias sociales: Prentice-Hall; México, 1996

Herramienta para Stress test de base de datos, [en línea]. Noticias Seguridad. 7 de diciembre de 2017. [citado en 2018]. Disponible en internet:

http://noticiasseguridad.com/seguridad-informatica/herramienta-para-stress-test-de-bases-de-datos-2/

KRIPPENDORFF, K. Content analysis. An introduction to its methodology: Sage; Beverly Hills, 1980

MAGERIT, Introducción. En: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos: Libro I – Método. Madrid, octubre de 2012. 127 p

MARTÍNEZ DE LA CRUZ, Sergio Alejandro. Importancia de los sistemas de información para las Pymes. [en línea]. Gestiopolis. 01 de noviembre de 2005. [citado en 2016] Disponible en internet: http://www.gestiopolis.com/importancia-sistemas-informacion-pymes/

MÉNDEZ, C. Metodología, Diseño y Desarrollo del Proceso de Investigación: Mc Graw-Hill; Caracas, 2001

MISFUD Elvira, Introducción a la seguridad informática. Ministerio de educación, cultura y deporte España, 26 de marzo de 2012. Disponible en internet: http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

MUÑOZ RAZO Carlos, Auditoría en Sistemas Computacionales. Pearson Educación. México. 816 p. ISBN 970-17-0405-3.

Norma NTC ISO/IEC 27001. 45 p.

Norma Técnica Colombiana. NTC ISO 9000:2005. Sistemas de Gestión de la Calidad. Fundamentos y Vocabulario. Bogotá, Colombia. ICONTEC.

RESTREPO, María Consuelo. Producción de textos educativos. [en línea]. Ediciones Bogotá D.C; Colombia. 290 p. ISBN: 978-958-20-0850-4. Disponible en internet: http://biblioteca.salamandra.edu.co/libros/Produccion%20de%20textos%20educativos.pdf

REVISTA GERENCIA. Seguridad informática ¿Qué hacer para proteger la información? [en línea]. Gerencia. Noviembre de 2009. Disponible en internet: http://www.emb.cl/gerencia/articulo.mvc?xid=932

SANTILLANA GONZÁLEZ Juan Ramón. Auditoria Fundamentos: Thomson. 2004

SOSA, Johana. Análisis de Riesgos. [en línea]. 27 de enero de 2012. Disponible en internet:
http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

TABANGO GOYES Marcelo, GUERRERO Camilo. Sistema de gestión de seguridad de la información basado en la norma ISO 27001 y 27002 para la unidad de informática y telecomunicaciones de la universidad de Nariño, San Juan De Pasto, 2014, 150h. Trabajo de Grado (ingeniero de sistemas). Universidad de Nariño. Facultad de Ingeniería

TAMAYO, Mario. El Proceso de la investigación científica. Limusa; México, 2001

TESCH, R. Qualitative research: analysis types and software tolos: The Falm Press; New York, 1992

VILLALÓN HUERTA Antonio, Seguridad de los sistemas de información. Octubre 2007

ANEXOS

ANEXO A. Documento unificado Magerit (Ver archivo adjunto a este trabajo: ANEXO A. Documento unificado Magerit.xlsx)

ANEXO B. Plan de tratamiento de riesgos (Ver archivo adjunto a este trabajo: ANEXO B. Plan de tratamiento de riesgos.xlsx)

ANEXO C. Documento unificado ISO-IEC 27001 - 27002 y matriz de aplicabilidad (Ver archivo adjunto a este trabajo: ANEXO C. Documento unificado ISO-IEC 27001 - 27002 y matriz de aplicabilidad.xlsx)

ANEXO D. Informe general (Ver archivo adjunto a este trabajo: ANEXO D. Informe general.docx)

ANEXO E. Informe gerencial (Ver archivo adjunto a este trabajo: ANEXO E. Informe gerencial.docx)