AUDITORIA AL SISTEMA DE INFORMACION DE LA CLINICA LAURA DANIELA DE LA CIUDAD DE VALLEDUPÁR

NEHEMIAS SARABIA DIAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFÓRMÁTICA
VALLEDUPAR
2017

AUDITORIA AL SISTEMA DE INFORMACION DE LA CLINICA LAURA DANIELA DE LA CIUDAD DE VALLEDUPÁR

NEHEMIAS SARABIA DIAZ

Trabajo de grado para optar al título de Especialista en seguridad informática

Director

Jorge Enrique Ramírez Montañez
Ingeniero de sistemas
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
VALLEDUPAR
2017

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Valledupar, Cesar. Día___ Mes___ Año____

DEDICATORIA

Primero que todo quiero darle las gracias a Dios por este nuevo escalón que doy en mi vida profesional, por darme la sabiduría y valentía para asumir cada reto propuesto en mi carrera.

A mi familia que con su esfuerzo, empeño y dedicación siempre me han apoyado.

En especial a mi esposa Nury Menco, mis hijos Lucas David y Gabriela son el motor que me impulsa a seguir preparándome.

A mis amigos desde lo más profundo de mi corazón, Gracias.

NEHEMIAS SARABIA DIAZ

AGRADECIMIENTOS

Al Ingeniero Salomón González por brindarme la asesoría necesaria en el momento que lo necesité gracias por su apoyo para la ejecución de este trabajo. Gracias por ser una guía en este proceso de formación.

A todos los tutores de la Universidad Abierta y a Distancia – UNAD a la que debemos nuestra formación profesional, compañeros y amigos por compartir con nosotras gratos momentos y enseñanzas de vida.

CONTENIDO

pág.

pág.

LISTA DE CUADROS

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

pág.

pág.

LISTA DE ANEXOS

pág.

RESUMEN

El proyecto **" Auditoria al sistema de información de la clínica Laura Daniela de la ciudad de Valledupar"**, fue desarrollado con el objetivo de realizar un estudio detallado del funcionamiento y protección de los activos informáticos en especial de la aplicación Krystalos, utilizada en el procesamiento de la información manejada en la Clínica Laura Daniela. Para esto, se aplicó la metodología ISO/IEC 27001, que proporciona técnicas claras que van desde el análisis de los procesos informáticos hasta la implementación de medidas que contribuyan al mejoramiento de éstos.

Se clasifica como tipo de investigación descriptiva, de diseño de investigación de campo, transeccional, según los autores Fidias G. Arias (2012) y Sampieri (1998), se tomó como población los empleados de las áreas de sistemas, contabilidad, recursos humanos, etc. que laboran en las mismas y se les aplicó un instrumento tipo encuesta, entrevista y observación directa. El análisis de los resultados, permitió observar el estado actual del tratamiento de los activos, sus vulnerabilidades y niveles de riesgos. Se concluye que la empresa requiere un manual oficial de políticas de seguridad de la información y disminuir los riesgos asociados al sistema de información. Se recomienda implementar los controles sugeridos y estrategias para involucrar a todo el personal en el cuidado de la información.

Por otra parte, con miras a establecer Políticas de Seguridad Informática que conlleven a minimizar los riesgos informáticos a los cuales se encuentran expuestos los procedimientos informáticos, se realizó un proceso de análisis de riesgos, utilizando la Metodología *MAGERIT*, que fue diseñada como respuesta al constante crecimiento tecnológico, y que además, presenta técnicas enfocadas a la detección de amenazas que permiten dimensionar la magnitud de los riesgos existentes en los sistemas de Información. Las fases que se implementaron en la realización de este proyecto son las siguientes:

1. Identificación y Valoración de Activos

2. Identificación y Valoración de Amenazas

3. Identificación y Valoración de Salvaguardas

4. Determinación del Impacto y Estimación del Riesgo

Como resultado de este trabajo investigativo se presentarán alternativas claras de mejoras y medidas preventivas para contribuir a un mejoramiento en los procedimientos del manejo de la información en la Clínica Laura Daniela, facilitando así la toma de decisiones por la administración y el Área de Sistemas.

Palabras Claves: *Auditoría, información, seguridad.*

ABSTRACT

The project "Audit to the information system of the Laura Daniela clinic in the city of Valledupar" was developed with the objective of carrying out a detailed study of the operation and protection of computer assets, especially of the Krystalos application, used in the processing of the information handled at the Laura Daniela Clinic. For this, the methodology was applied ISO / IEC 27001, which provides clear techniques ranging from the analysis of computer processes to the implementation of measures that contribute to the improvement of these.

According to authors Fidias G. Arias (2012) and Sampieri (1998), it is classified as a type of descriptive research, field research design, transectional, the population was taken from the areas of systems, accounting, human resources, etc. that work in the same and were applied an instrument type survey, interview and direct observation. The analysis of the results, allowed to observe the current state of the treatment of the assets, their vulnerabilities and levels of risks. It is concluded that the company requires an official manual of information security policies and reduce the risks associated with the information system. It is recommended to implement the suggested controls and strategies to involve all the personnel in the care of the information.

On the other hand, in order to establish Computer Security Policies that lead to minimize the computer risks to which the computer procedures are exposed, a process of risk analysis was carried out using the MAGERIT Methodology, which was designed in response to the constant Technological growth, and that also presents techniques focused on the detection of threats that allow to size the magnitude of the existing risks in Information systems. The phases that were implemented in the realization of this project are the following:

1. Identification and Valuation of Assets

2. Identification and Assessment of Threats

3. Identification and Valuation of Safeguards

4. Impact Determination and Risk Estimation

As a result of this research, clear alternatives for improvements and preventive measures will be presented to contribute to an improvement in the procedures of information management in the Laura Daniela Clinic, thus facilitating decision making by the administration and the Area of Systems.

Key Words*: Audit, information, security.*

INTRODUCCIÓN

El objetivo principal de éste proyecto es contribuir al mejoramiento de los procesos informáticos llevados a cabo dentro de la Clínica Laura Daniela de la Ciudad de Valledupar, mediante la ejecución de 2 procedimientos enfocados puntualmente al análisis y gestión de riesgos existentes dentro de dicha institución. Estos procedimientos son:

1. La realización de una auditoría a los activos informáticos con énfasis en la aplicación en funcionamiento Krystalos, utilizada como principal herramienta en el procesamiento de datos dentro de la institución. Para esto, se hará uso de las directrices establecidas en el estándar ISO/IEC 27001, con el fin de realizar un estudio detallado de los procesos realizados por esta aplicación, detectar las falencias y presentar alternativas de mejoras que contribuyan a un avance sustancial mediante una toma de decisiones acertada.

2. El diseño e implementación de pruebas de detención de vulnerabilidades utilizando Software especializados y de uso libre como el VEGA, que permitan establecer controles y acciones preventivas para un mejor uso de las tecnologías de la información dentro de la Clínica Laura Daniela. Para lograr objetividad y acierto en esta fase, se realizará un análisis de riesgos conforme a lo establecido en la Metodología *Magerit*, la cual proporciona un conjunto de técnicas que implican diversos procesos cualitativos y/o cuantitativos para la caracterización de los activos, amenazas y salvaguardas, con miras a determinar los riesgos existentes dentro del sistema informático.

1. TITULO

AUDITORIA AL SISTEMA DE INFORMACION DE LA CLINICA LAURA DANIELA DE LA CIUDAD DE VALLEDUPÁR

2. PLANTEAMIENTO DEL PROBLEMA

La auditoría de sistemas permite examinar y evaluar los procesos y recursos que intervienen en la automatización de la información, para llegar a establecer el grado de eficiencia, efectividad, seguridad y economía de los sistemas computacionales utilizados en una organización empresarial; presentando conclusiones y recomendaciones encaminadas a mejorar el desarrollo de estos procedimientos.

A nivel general, actualmente los activos no sólo son los bienes muebles e inmuebles, también lo constituye la información que administran y generan las empresas sobre clientes, productos, ventas, entre otro.

Es así, como surge la necesidad de parte de la alta gerencia, de realizar la auditoria a sus sistemas informáticos. Esto debido a que están expuestos a amenazas y riesgos que afectan la seguridad de la información. Al respecto, se observan problemas tales como fallas en la integridad de la información, poco valor a la organización de la infraestructura informática, y déficit de normas de usabilidad del sistema.

En este sentido, por el volumen de información que se produce diariamente y al no contar con una adecuada infraestructura, los equipos de cómputo estarían en peligro, puesto que no hay una adecuada distribución de espacios, suficiente ventilación y salidas de emergencia a las cuales acudir ante algún siniestro. Todo lo anterior pone en peligro la integridad de los equipos y registros manuales de información.

Así mismo, en el nivel físico de las redes por los problemas antes mencionados se observa inadecuada distribución del cableado estructurado, a raíz de ausencia de cuarto de telecomunicaciones, el cual se encuentra improvisado con la oficina de Coordinación de Sistemas.[1]

La clínica Laura Daniela posee el software krystalos, el cual es un sistema integral diseñado para clínicas y hospitales, el cual permite unificar toda la información en aspectos asistenciales, administrativos financieros y contables, facilitando de esta manera su uso a lo largo y ancho de todas las áreas de la entidad.

[1] López, 2012. ¿Qué es la Auditoria de sistemas de información?, Universidad veracruzana [Disponible en]: http://www.uv.mx/personal/artulopez/files/2012/10/07-Auditoria-de-SI.pdf

krystalos, es la plataforma utilizada en la clínica Laura Daniela para la gestión de actividades tales como: el control y manejo de inventarios, la optimización de los ciclos de recaudo de cartera, la contabilización automática, la generación de RIPS, el control de glosas, el manejo de unidosis, las hojas de tratamiento y balance de líquidos y un programa de ayuda de *outsourcing* de medicamentos, materiales y demás insumos médicos; procesos que son trascendentales para el desarrollo eficiente de los servicios prestados en esta entidad.

Actualmente, Krystalos está presentando inconsistencias en algunas de sus funciones, razón por la cual, no genera un alto nivel de confiabilidad en el flujo de la información, y ocasiona muchas veces fallas en el desarrollo normal de las labores, generando retrasos en los procesos y en su defecto pérdidas económicas para la empresa. En cuanto a las falencias más marcadas, se encuentran la realización de consultas y generación de reportes, procedimientos que influyen directamente en la toma de decisiones de la empresa, y que por no estar siendo realizados en forma eficiente se están convirtiendo en procesos engorrosos que conllevan a la pérdida de tiempo, control ineficiente de actividades, cambio o reparación de equipos, emisión repetitiva de reportes que ocasionan problemas de almacenamiento, gastos de papel y pérdida de información. Además, existen ciertas falencias notadas por algunos de los trabajadores que hacen uso de la aplicación Krystalos, quienes no se sienten seguros con la integridad de la información generada y recibida; por lo que se sienten forzados a realizar verificaciones constantes para confirmar la veracidad de la información.

Por todo ello, se hace necesario la realización de una auditoria que permita la revisión y evaluación de todos los aspectos concernientes a los sistemas automáticos que intervienen en el procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes, con el objeto de detectar errores, presentar sugerencias que contribuyan a un mejoramiento en los procedimientos y diseñar políticas de seguridad que garanticen confiabilidad y seguridad en las procesos de operación.

2.1. FORMULACIÓN DEL PROBLEMA

¿De qué manera la realización de una auditoría de sistemas de información, contribuirá al mejoramiento de los procesos para garantizar la integridad, confiabilidad, seguridad y confidencialidad de los datos en la clínica Laura Daniela?

3. OBJETIVOS DEL PROYECTO

3.1. OBJETIVO GENERAL

Realizar una auditoría al sistema de información de la clínica Laura Daniela de la ciudad de Valledupar en el marco de la norma NTC-ISO/IEC 27001 y el referente metodológico *Magerit* para el mejoramiento de los procesos garantizando la integridad, confiabilidad, seguridad y confidencialidad de los datos.

3.2. OBJETIVOS ESPECÍFICOS

- Identificar los componentes del sistema de información actual mediante revisión documental y entrevistas para establecer el plan de auditoria a desarrollar en la clínica Laura Daniela de la ciudad de Valledupar.

- Realizar las pruebas de auditorías mediante la metodología de análisis y gestión de riesgos *Magerit* y herramientas de *petesting* para determinar los riesgos presentes en la clínica Laura Daniela de la ciudad de Valledupar.

- Formular el informe de auditoría, recomendando los controles adecuados para el tratamiento de los riesgos según los parámetros de la norma ISO 27001, describiendo las recomendaciones y conclusiones.

4. JUSTIFICACIÓN

Para la clínica Laura Daniela es de gran importancia la realización de una auditoria que permita identificar las anomalías presentes en su sistema de información y que conlleve a proponer mejoras a la administración que contribuyan al buen desarrollo de los procesos informáticos llevados a cabo en esta entidad.

La relevancia de este proyecto radica en que a través de él, la empresa clínica Laura Daniela tendrá un paso adelante ante entidades de certificación que auditan la implantación y aplicación de las normas internacionales, ya que la empresa en el año 2018 aspira ser una de las organizaciones líderes de la región Caribe, en la prestación de los servicios de forma integral, con identidad propia, cumpliendo los estándares de calidad, soportados con un talento humano competente, instalaciones modernas y tecnológicamente avanzadas.

Por todo lo anterior expresado, se hace necesario realizar una auditoría de sistemas de información teniendo en cuenta la norma NTC-ISO/IEC 27001.

5. MARCOS DE REFERENCIA

5.1. DELIMITACIÓN ESPACIO - TEMPORAL

El entorno de la realización del proyecto tendrá lugar en la Clínica Laura Daniela de la Ciudad de Valledupar, ubicada en el departamento del Cesar.

Este proyecto se desarrollará en el tiempo comprendido entre junio 2016 a junio de 2017.

5.2. MARCO CONCEPTUAL

Para obtener una visión del contenido del proyecto se definen varios conceptos que facilitaran la comprensión de los temas a tratar. Estos conceptos son:

Auditoria: La Auditoría puede definirse como «un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso».

"Un proceso sistemático que consiste en obtener y evaluar objetivamente evidencia sobre las afirmaciones relativas a los actos y eventos de carácter económico; con el fin de determinar el grado de correspondencia entre esas afirmaciones y los criterios establecidos, para luego comunicar los resultados a las personas interesadas"[2].

Sistemas de información: Un sistema de información puede definirse como un conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar y distribuir la información para apoyar la toma de decisiones y el control en una empresa

[2] UNIVERSIDAD DEL CAUCA. Aspectos Organizacionales de los Sistemas de Información. 1. Conceptos Básicos de Sistemas de Información. En: http://fccea.unicauca.edu.co/old/siconceptosbasicos. [s.f.]

Auditoría de sistemas de información: Es muy compleja y por tanto es necesario contar con ciertas habilidades que te permitan a provechar al máximo este tipo de auditorías y hacer que su uso sea el adecuado y obtener el beneficio de adquirir con la práctica la habilidad necesaria para realizar una correcta auditoría de sistemas de información.

Actualmente la auditoria de los sistemas de información es definida como cualquier auditoria que abarque la revisión y evaluación de todos los aspectos de los sistemas automáticos de procesamiento de la información, incluyendo los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Es indispensable tomar en cuenta que, para hacer una adecuada planeación de la auditoria en sistemas de información, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.[3]

Políticas de seguridad informática: Las políticas de seguridad informática tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de las empresas.[4]

Pruebas de penetración: Las pruebas de penetración es un proceso en donde se realizan distintos tipos de tareas que identifican, en una infraestructura objetivo, las vulnerabilidades que podrían explotarse y los daños que podría causar un atacante. En otras palabras, se realiza un proceso de hacking ético para identificar qué incidentes podrían ocurrir antes de que sucedan y posteriormente, reparar o mejorar el sistema, de tal forma que se eviten estos ataques.

Tipos de pruebas de penetración: Existen diferentes tipos de Pruebas de Penetración, las más comunes y aceptadas son las Pruebas de Penetración de Caja Negra *(Black-Box)*, las Pruebas de Penetración de Caja Blanca *(White-Box)* y las Pruebas de Penetración de Caja Gris *(Grey-Box)*.

[3] Op. Cit. Ibíd.
[4] BENÍTEZ, Moisés. Gestion Integral. Políticas de Seguridad Informática. En: http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf. [2013]

- **Prueba de Caja Negra**. No se tienen ningún tipo de conocimiento anticipado sobre la red de la organización. Un ejemplo de este escenario es cuando se realiza una prueba externa a nivel web, y está es realizada solo con el detalle de una URL o dirección IP proporcionado al equipo de pruebas.

- **Prueba de Caja Blanca**. El equipo de pruebas cuenta con acceso para evaluar las redes y ha sido dotado de diagramas de la red y detalles sobre el hardware, sistemas operativos, aplicaciones, entre otra información antes de realizar las pruebas.

- **Prueba de Caja Gris**. El equipo de pruebas simula un ataque realizado por un miembro de la organización inconforme o descontento. En este caso se deben dar los privilegios adecuados a nivel de usuario, además de permitirle acceso a la red interna.

Para este caso se realizaron Pruebas de Penetración de Tipo de Caja Negra al sistema web de la *Clínica Integral de Emergencias Laura Daniela* empleando las herramientas Vega Vulnerability Scanner y NMAP Security Scanner.

HERRAMIENTAS Y TECNICAS PARA LA AUDITORÍA INFORMÁTICA:

Cuestionarios: Las Auditorias informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios pre impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de

la Auditoria. Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otros medios la información que aquellos pre impresos hubieran proporcionado.[5]

Entrevistas: La entrevista es una técnica eficaz para obtener datos relevantes y significativos, la información que el auditor obtiene a través de la entrevista es muy superior que cuando se limita a la lectura de respuestas escritas y a través de la entrevista se pueden captar los gestos, los tonos de voz, los énfasis, etc., que aportan una importante información sobre el tema y las personas entrevistadas.[6]

Checklist: Es un instrumento de verificación de datos muy práctico debido a que enmarca al auditado en la precisión de su respuesta, en el caso de la auditoria de sistemas, no se trata de discutir específicamente los detalles técnicos de la prevención en los sistemas informáticos específicos, sino que proporcionará una lista de verificación general para examinar la seguridad de un sistema informático.

Seguridad en la informática: Es una disciplina relativamente nueva cuya finalidad es proteger la integridad, confidencialidad y la disponibilidad de los activos de un sistema de información. En este sentido, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.

Bases de datos: Se pueden definir como un sistema integrado e interrelacionado de datos, organizados en un disco lo cual permite el acceso a esos datos a través de una aplicación informática. Recientemente, el término base de datos comenzó a utilizarse casi exclusivamente en referencia a bases construidas a partir de software informático, que permiten una más fácil y rápida organización de los datos. Las bases de datos informáticas pueden crearse a partir de software o incluso de forma online usando Internet. En cualquier caso, las funcionalidades disponibles son prácticamente ilimitadas.[7]

Aplicación (informática): Es un programa diseñado para facilitar al usuario la realización de un determinado tipo de trabajo, y que suele convertirse en una solución para la automatización de tareas con cierto grado de complejidad, como puede ser la contabilidad o gestión de una empresa.

Sistema de Información: es un conjunto de elementos orientados al tratamiento y

---

[5] **LÓPEZ,** Hector. *et. al*. Archivos Auditoría En Sistemas. En: http://archivosauditoria.blogspot.com.co/. [2009]
[6] Op. Cit. Ibíd.
[7] **DEFINICIONABC.** Definición de Base de datos. En: http://www.definicionabc.com/tecnologia/base-de-datos.php. [s.f.]

administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad.

Krystalos: Es un sistema integral diseñado para clínicas y hospitales, el cual permite unificar toda la información en aspectos asistenciales, administrativos financieros y contables, facilitando de esta manera su uso a lo largo y ancho de todas las áreas de la entidad.

Clínica Laura Daniela: Es una institución prestadora de Servicios de salud de III y IV Nivel, que cuenta con tecnología de punta disponible en la región puesta al servicio de la comunidad del Cesar, Guajira y Magdalena, con profesionales altamente calificados y capacitados para atender a cada uno de sus clientes con actitud humanizada, cálida y eficiente.

Valledupar: Es una ciudad colombiana, capital del departamento del Cesar, ubicada al nororiente de la Costa Caribe Colombiana, a orillas del río Guatapurí, en el valle del río Cesar formado por la Sierra nevada de Santa Marte y la serranía del Perijá al este.

5.3. MARCO DE ANTECEDENTES

Auditoria del sistema informático del hospital del sur enrique Garcés

Del hierro Pablo, Trujillo Freddy, Enero 2012, este trabajo estaba compuesto de cuatro capítulos, y anexos, los cuales tenían como principal objetivo mostrar los resultados obtenidos de la auditoría, utilizando el marco de trabajo y las directrices de auditoría propuestas por COBIT, realizada a la unidad informática del Hospital General “Enrique Garcés”.

El Capítulo I presentaba una descripción tanto del alcance del proyecto como la descripción de la unidad informática del Hospital General “Enrique Garcés”, su ubicación dentro del hospital, características principales y nivel de decisión. Además, este capítulo contaba con un análisis que se realizó para determinar cuál sería la metodología más adecuada para realizar la presente auditoria.

El Capítulo II detallaba una visión de la situación del área informática del Hospital General Enrique Garcés, y de la planificación y realización de la auditoria, en donde

se seleccionarán los procesos más adecuados propuestos por COBIT que se ajustaban a la situación de la unidad de TI, en donde se evaluaba, media el modelo o de madurez, y se realizaba recomendaciones a mediano y largo plazo de cada uno de ellos.

El Capítulo III se presentaba los resultados de la auditoria a través de un conjunto de informes que serían entregados tanto a la parte gerencial como a la unidad de TI del Hospital General Enrique Garcés, en donde se mostrará el análisis de los resultados, y se entregará las conclusiones finales por cada proceso evaluado.

Finalmente, en el Capítulo IV se presentaron las conclusiones y recomendaciones del Proyecto. Esta auditoría pudo ayudar a determinar los procesos que la unidad de TI debió implementar, determinar la criticidad de los mismos y así tomar medidas correctivas que permitieron mejorar el desempeño de la unidad y lograr como objetivo el buen funcionamiento del hospital a través del aseguramiento de la continuidad de los servicios

Para esto, los estudiantes seleccionaron la metodología COBIT, a través de su marco de referencia y guías de auditoría proporciono las herramientas necesarias para determinar la situación de los procesos de la unidad de TI del Hospital General “Enrique Garcés” y realizar recomendaciones a corto y largo plazo para tomar acciones correctivas, con lo cual la dirección de TI priorice los procesos y las estrategias para mejorar el desempeño de la unidad dentro del hospital**.**

Esta auditoria pudo ayudar a determinar los procesos que la unidad de TI debe implementar, determinar la criticidad de los mismos y así tomar medidas correctivas que permitan mejorar el desempeño de la unidad y lograr como objetivo el buen funcionamiento del hospital a través del aseguramiento de la continuidad de los servicios.

La metodología COBIT a través de su marco de referencia y guías de auditoria proporciona las herramientas necesarias para determinar la situación actual de los procesos de la unidad de TI del hospital y realizar recomendaciones de corto y largo plazo para tomar acciones correctivas, con lo cual la dirección de la unidad de TI priorice los procesos y las estrategias para mejorar el desempeño de la unidad dentro del hospital.[8]

[8] Piattini, (2003). Piattini Mario y del Peso Emilio, 2003. Auditoría Informática, un enfoque práctico. 659 páginas. Editorial Alfaomega-Rama. ISbn: 958-682-455-1

Los procesos evaluados en el área de la TI del hospital obtuvieron como resultados un nivel de madurez entre 0 y 1demostrando un bajo nivel de la unidad. Se pudieron dar recomendaciones que mejoraran el desempeño de las actividades de la unidad y permitieran elevar el grado de madurez de estos procesos y el grado de madurez en general.

Esta auditoria tiene un nivel de complejidad medio-alto y se logró gracias a la apertura de la unidad de TI del hospital entregándoles la información solicitada, autorizando la realización de encuestas y entrevistas para recolección de información, permitiéndoles el acceso a las distintas dependencias del hospital.

Auditoría de seguridad informática ISO 27001 para la empresa de alimentos "Italimentos cía. Ltda.

Cadme Christian, Duque Diego, 2011, En la empresa de Italimentos existían ciertas vulnerabilidades para acceder a cierta información, para ello se realizó una auditoria de seguridad informática basada en un estándar internacional ISO 27001, el cual tuvo como objetivo la confidencialidad e integridad de los datos.

Para lo cual, se describió a la empresa, la producción, la comercialización, los empleados, la ubicación, etc.; con el objetivo de familiarizarse con el entorno laboral en el que se realizó la auditoría. Se realizaron estudios adecuados para comprobar que en la empresa existían normas, políticas y estándares de seguridad informática y de la información, con el objetivo de verificar si se cumplían las mismas.

Después, se investigó que tipos de activos informáticos poseían, como lo administraban, como se actualizaban; con el objetivo de verificar que el uso de los mismos era adecuado, teniendo en cuenta la seguridad de la información que contenían los recursos informáticos. Aquí se comprobó que el personal específico podía acceder a recursos e información confidencial. Se verificó que el personal cumplía con los privilegios de acceso otorgados por un administrador. Se observó que los recursos informáticos se encontraban ubicados en una zona segura, teniendo en cuenta que solo el personal específico podía tener acceso a estos recursos. Comprobó que el departamento de sistemas se encontró en un área desde el cual se pueda dar soporte a usuario.

Se identificó los distintos accesos que los usuarios tenían para acceder a cierto tipo de información digital en una red compartida dentro de la empresa, utilizando cuestionarios ya realizados en capítulos anteriores para tener una mejor visión

sobre los diferentes tipos de accesos. Se realizaron recomendaciones sobre falencias encontradas en ciertas aéreas de seguridad informática y de información en la empresa, dejando a disposición de la gerencia y distintos departamentos la elección a las posibles soluciones.[9]

Guía de buenas prácticas de seguridad de la información en contextos de micro, pequeñas y medianas empresas de la región

Esta guía fue elaborada por, Ayala Gerardo, Gómez Julián, 2011, Para impedir la ejecución de operaciones no autorizadas sobre un sistema informático se asume como vital importancia, puesto que sus efectos con llevan a daños sobre los datos y comprometen la confidencialidad, la autenticidad e integridad de la información organizacional.

Este documento se centró en la aplicación de la norma ISO/IEC 27001 en atención a la Implementación y Operación de un Sistema de Gestión de la Seguridad de la Información (por sus siglas, SGSI), identificando las acciones de: la gestión apropiada, prioridades y responsabilidades de la gerencia en lo que crearon políticas que garantizaron el cumplimiento de los objetivos del SGSI, además se hicieron referencias a la creación de planes de acción para el tratamiento, análisis y gestión de los riesgos implementando procedimientos que brindaron una atención oportuna a los incidentes de seguridad de la información, acompañados de estrategias de capacitación y formación para los integrantes de la organización**.**

Los resultados obtenidos en la realización de esta guía fueron un modelo validado de buenas prácticas de seguridad de la información, un diagnostico general a través de la construcción de tendencias de prácticas de seguridad en Colombia y EE. UU, un proceso investigativo sistematizado para la construcción de un manual de procedimientos para la administración de la seguridad de la información en contextos de micros pequeñas y medianas empresas de la región.

Establecimiento del Sistema De Seguridad De Información en SFG Bajo los estándares de la Norma ISO 27001: 2005

Elaborado por, García Camilo, 2012, *Solution Finders Group* (en adelante SFG) es una empresa que apoya la toma de decisiones de fertilización en palma de aceite y

[9] **CADME, C., y DUQUE, D. (2011-2012).** Auditoria de seguridad informática ISO 27001 para la empresa de alimentos "ITALIMENTOS CIA. LTDA." (Tesis de pregrado). Recuperado de: http://dspace.ups.edu.ec/bitstream/123456789/2644/16/UPS-CT002441.pdf

suministra al palmicultor un conjunto de escenarios y alternativas de decisión para la compra de fertilizantes, que cumpla con todos los requerimientos nutricionales del cultivo y que de manera conjunta con los costos de aplicación represente la opción más económica, viable y efectiva para su plan de manejo de nutricional.

La investigación fue el desarrollo de un marco conceptual y metodológico para la etapa de establecimiento de un sistema de gestión de seguridad de información bajo la perspectiva de las prácticas sugeridas por el estándar ISO 27001:2005 en una empresa de base tecnológica emergente. Se presentó el desarrollo de la metodología sugerida por la literatura y fuentes consultadas en cuanto a la determinación del alcance, identificación de activos, análisis y evaluación del riesgo y selección de controles y objetivos de control. Se resumió este desarrollo con una declaración de aplicabilidad que muestra, en detalle, los objetivos y controles seleccionados.

El desarrollo del trabajo sugirió una necesidad grande de integración entre diferentes marcos normativos y de gestión, como complemento a los esfuerzos en seguridad de información. Dentro de estas relaciones, valió la pena destacar una gran oportunidad con respecto a los esquemas de mejora continua propuestos en particular por la familia de normas ISO 9000 en aspectos relevantes como los controles A.10.1 Procedimientos y responsabilidades operacionales y A.13.2.2 Aprendizaje de los incidentes en la seguridad de la información, que para este caso particular tienen una estrecha relación con los esquemas de aseguramiento de calidad en productos y servicios, fundamental en los requisitos expresados por ISO 9001:2008. Adicionalmente a este punto se encontró una estrecha relación entre los diferentes esquemas de responsabilidad, compromiso y revisión por la dirección, puntos en los cuáles los insumos de información brindados por este trabajo se encontraron objetivos comunes e integrados para tener un concepto fuerte y completo del término calidad y servicio.

Adicionalmente a lo anterior se presentaron oportunidades de integración y complementariedad con respecto a normas técnicas y buenas prácticas en las áreas de seguridad y salud ocupacional, ya que para esta industria en particular dichos riesgos están circunscritos a los ámbitos de trabajo electrónico, teletrabajo y relacionados. Es así como por ejemplo los controles A.9.1.5 Trabajo en áreas seguras y A.9.2 Seguridad del equipo son un buen insumo para el comienzo de actividades en estas áreas de mejora y prevención.

Al aplicar la metodología completa de establecimiento de un sistema de gestión de seguridad de información para esta organización en particular se encontraron, finalmente, 22 objetivos de control y 66 controles relacionados para su cumplimiento. Este número contrastado contra la literatura consultada puede parecer alto, sin embargo, siendo este un caso específico de una organización de base tecnológica, de rápido desarrollo y muy dependiente de los medios tecnológicos y de información es un 55 número proporcionado a la cantidad de procesos de información en los cuáles esta organización incurre todos los días y que dieron origen a los riesgos catalogados en primera instancia.[10]

5.4. RESEÑA HISTORICA

5.4.1. Clínica Laura Daniela. El año 2003 es el punto de partida de la Clínica Integral de Emergencias Laura Daniela que llego a cumplir un servicio humanizado por vocación en el sector de la salud para los departamentos del Cesar, Guajira y Magdalena con un alto sentido humano y un respetuoso ejercicio profesional.

Paso a paso durante los últimos 6 años la Clínica ha ido creciendo en infraestructura física y tecnológica, fortaleciéndose en equipamiento médico hospitalario y posesionándose como una de las IPS más importantes de la región.

Desde sus inicios la institución ofreció múltiples servicios hospitalarios a las empresas promotoras de salud al sistema de salud pública y a la comunidad en general.

En la actualidad, la Clínica Laura Daniela es reconocida como la de mayor proyección y crecimiento en los últimos años en la región, colocándose a la vanguardia en tecnología, para brindar un nivel de compromiso de calidad frente a sus pacientes y la comunidad. Esta institución se orienta hacia el Logro de la satisfacción de los usuarios con servicios oportunos, nuevas tecnologías biomédicas, y una infraestructura adecuada para los procesos de atención al usuario, asegurando una mejora continua de los procesos y de las metas de nuestra organización y de esta forma garantizando los menores riesgos de atención al usuario con los mayores beneficios para la comunidad en general.

[10] GARCIA, C. (2012). Establecimiento del sistema de seguridad de información en SFG bajo los estándares de la norma ISO 27001:2005 (Tesis de Posgrado). Recuperado de: http://repository.ean.edu.co/bitstream/handle/10882/2532/GarciaCamilo2012.pdf?sequence=1

5.5. MARCO TEÒRICO

5.5.1. Auditoría. La Auditoría se puede definir como un proceso sistemático para obtener y evaluar de manera objetiva, las evidencias relacionadas con informes sobre actividades económicas y otras situaciones que tienen una relación directa con los parámetros y actividades que se desarrollan en una entidad pública o privada. El fin del proceso consiste en determinar el grado de precisión del contenido informativo con las evidencias que le dieron origen. La evidencia que debe obtener el auditor consiste en una amplia gama de información y datos que lo puedan ayudar a elaborar su informe final, haciendo uso de su criterio profesional.

El auditor de sistemas juega un rol de mucha importancia en los procesos de la auditoria debido a que le cabe toda la responsabilidad al momento de inspeccionar, verificar y comparar el objeto de estudio con la realidad que presente; de su pericia y el nivel ético de sus informes depende la correcta y oportuna toma de decisiones de la gerencia.

5.5.1.1. Objetivos Generales de la Auditoria. Existen una serie de objetivos que se pretenden alcanzar a través de la realización de una Auditoría. Entre estos encontramos los siguientes:

- Realizar una revisión independiente de las actividades, áreas o funciones especiales de una institución, a fin de emitir un dictamen profesional sobre la razonabilidad de sus operaciones y resultados.

- Hacer una revisión especializada, desde un punto un punto de vista profesional y autónomo del aspecto contable, financiero y operacional de las áreas de una empresa.

- Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la actuación de los empleados y funcionarios de una institución, así como evaluar las actividades que se desarrollan en sus áreas y unidades administrativas.

- Dictaminar de manera profesional e independiente sobre los resultados obtenidos por una empresa y sus áreas, así como sobre el desarrollo de sus funciones y el cumplimiento de sus objetivos.

5.5.1.2. Clasificación de los Tipos de Auditoria. En el ámbito de la administración, la auditoría es una función asesora - técnica al servicio de la dirección superior de la empresa[11], cuya misión fundamental es apoyar la gestión empresarial en lo relativo a las necesidades de información, evaluación y control para el proceso de toma de decisiones, por tal razón, y dependiendo de la necesidad de la empresa, la Auditoría tiene varias clasificaciones:

Auditorías por su lugar de aplicación:

- Auditoría externa
- Auditoría interna

Auditorías por su área de aplicación:

- Auditoría financiera
- Auditoria administrativa
- Auditoria operacional
- Auditoría integral
- Auditoria gubernamental
- Auditoría de sistemas

Auditorías especializadas en áreas específicas

- Auditoría al área médica (evaluación médico—sanitaria)
- Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)
- Auditoría fiscal
- Auditoría laboral
- Auditoría de provectos de inversión
- Auditoría a la caja chica o caja mayor (arqueos)
- Auditoría al manejo de mercancías (inventarios)

[11] **PIATTINI, Mario y DEL PESO , Emilio.** Auditoría Informática, un enfoque práctico. . ISbn: 958-682-455-1 : Alfaomega-Rama, [2003].

- Auditoría ambiental
- Auditoría de sistemas

5.5.2. Análisis y planificación de la auditoria de sistemas. El auditor de sistemas debe comprender el ambiente del negocio en el que se ha de realizar la auditoría, así como los riesgos del negocio y control asociado. A continuación, se menciona algunas de las áreas que deben ser cubiertas durante la planificación de la auditoría.

5.5.2.1. Comprensión del Negocio y de su Ambiente. Los pasos que puede llevar a cabo un auditor de sistemas para obtener una comprensión del negocio son:

- Recorrido de las instalaciones del ente.

- Lectura de material sobre antecedentes que incluyan publicaciones sobre esa industria.

- Revisión de Memorias e informes financieros.

- Entrevistas a gerentes claves para comprender los temas comerciales esenciales.

- Estudio de los informes sobre normas o reglamentos.

- Revisión de planes estratégicos a largo plazo.

- Revisión de informes de auditorías anteriores.

5.5.2.2. Riesgo y Materialidad de Auditoría. Los riesgos de auditoría son aquellos donde la información pueda tener errores materiales (fallas significativas durante la ejecución de una auditoría), o cuando el auditor de sistemas no pueda detectar un error que ha ocurrido. Los riesgos en auditoría pueden clasificarse de la siguiente manera:

- Riesgo Inherente: Cuando un error material no se puede evitar que suceda porque no existen controles compensatorios relacionados que se puedan establecer.

- Riesgo de Control: Cuando un error material no puede ser evitado o detectado en forma oportuna por el sistema de control interno.

- Riesgo de Detección: Es el riesgo de que el auditor realice pruebas exitosas a partir de un procedimiento inadecuado.

La materialidad en la auditoría de sistemas debe ser considerada en términos del impacto potencial total para el ente en lugar de alguna medida basado en lo monetario.

Existe una relación inversa entre materialidad y el nivel de riesgo de auditoría aceptable para el Auditor de Sistemas; es decir, cuanto mayor sea el nivel de materialidad, menor será la capacidad de aceptación del riesgo de auditoría, y viceversa. Esto es un argumento que permite al Auditor determinar la naturaleza, los plazos y el alcance de los procedimientos de auditoría.

5.5.2.3. Técnicas de Evaluación de Riesgos. Actualmente existen varias técnicas de evaluación de riesgos y su elección va a depender directamente de las áreas funcionales a auditar y del origen de la misma, cuyas directrices se deberán aplicar al momento de evaluar el nivel de riesgo que presenta cada una de ellas, y determinar cuáles de esas áreas vulnerables requieren ser auditadas. Entre los motivos o causas para realizar una evaluación de riesgos se pueden evidenciar las siguientes: Por síntomas de descoordinación, debilidades económicas, garantizar que se ha obtenido la información pertinente de todos los niveles gerenciales, y que las actividades de la función de auditoría se dirigen correctamente a las áreas de alto riesgo, constituyendo así, un valor agregado para la gerencia.

5.5.3. El control interno. El control interno es de suma importancia debido a que este integra las herramientas, métodos, procesos y actividades de la organización, entrelazados entre sí con el objetivo de cumplir con su eje misional que abarca los siguientes criterios: La obtención de información financiera correcta y segura, la salvaguarda de los activos y la eficiencia de las operaciones.

Sus objetivos fundamentales son:

Establecer la seguridad y protección de los activos de la empresa, promover la confiabilidad, oportunidad y veracidad de los registros contables, así como de la emisión de la información financiera de la empresa, incrementar la eficiencia y

eficacia en el desarrollo de las operaciones y actividades de la empresa, establecer y hacer cumplir las normas, políticas y procedimientos que regulan las actividades de la empresa, implantar los métodos, técnicas y procedimientos que permitan desarrollar adecuadamente las actividades dentro de la empresa.

5.5.3.1. Elementos del Control Interno. El auditor debe efectuar un estudio y evaluación adecuados del control interno existente, que le sirvan de base para determinar el grado de confianza que va a depositar en él, así mismo, que le permitan determinar la naturaleza, extensión y oportunidad que va a dar a los procedimientos de auditoria[12].

Los elementos del control interno son:

- Elementos de organización
- Elementos de procedimientos
- Elementos de personal
- Elementos de supervisión

5.6. MARCO LEGAL

Actualmente con el auge de la red internet como principal fuente de información ha traído consigo la globalización y el acceso a fuentes de datos de todo el mundo, lo que exige una regulación sobre el uso que se le debe dar a estos. Es por esto que cada persona debe tener una posición objetiva, acorde con las leyes de protección y uso de datos personales, empresariales y gubernamentales según las disposiciones jurídicas de cada país y el entorno jurídico internacional.

Estas medidas son aplicadas en todos los ámbitos que conciernen a las sociedades, pero principalmente el académico y los profesionales de las ciencias informáticas y jurídicas donde es pertinente por la creciente demanda de nuevos tipos de transacciones y/o actividades que se dan en el uso del internet.

[12] AUDITORIASISTEMAS**.** Auditoria Sistemas. Auditoria informática. En: http://auditoriasistemas.com/auditoria-informatica/. [2014]

5.6.1. Legislación nacional de Colombia - ley número 527. Por medio de ésta se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones[13].

5.6.1.1. Artículo 1. Ámbito de Aplicación. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

a)En las obligaciones contraídas por el Estado colombiano en virtud de Convenios o Tratados internacionales.

b)En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

5.6.1.2. Artículo 2. Definiciones. Para los efectos de la presente ley se entenderá por:

a)Mensaje de Datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama o el telefax.

b)Comercio Electrónico. Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera;

[13] **CONGRESO DE COLOMBIA.** LEY 527. En: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276. [1999]

c)Firma Digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

d)Entidad de Certificación. Es aquella persona que, autorizada conforme a la presente Ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

e)Intercambio Electrónico de Datos (EDI). La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto.

Sistema de Información. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

5.6.1.3. Artículo 3. Interpretación. En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspira.

5.6.1.4. Artículo 4. Modificación Mediante Acuerdo. Salvo que se disponga otra cosa, en las relaciones entre partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III, Parte I, podrán ser modificadas mediante acuerdo.

5.6.1.5. Artículo 5. Reconocimiento Jurídico de los Mensajes de Datos. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

La aplicación de los requisitos jurídicos de los mensajes de datos, pueden ser:

5.6.1.6. Artículo 6. Escrito. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.
Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

5.6.1.7. Artículo 7. Firma. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a)Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación.

b)Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

5.6.1.8. Artículo 8. Original. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a)Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma.

b)De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

5.6.1.9. Artículo 9. Integridad de un Mensaje de Datos. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es

íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

5.6.1.10. Artículo 10. Fuerza Probatoria de los Mensajes de Datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el solo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original

5.6.1.11. Artículo 11. Criterio para Valorar Probatoriamente un Mensaje de Datos. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

5.6.1.12. Artículo 12. Conservación de los Mensajes de Datos y Documentos. Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

- Que la información que contengan sea accesible para su posterior consulta.

- Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada, recibida, y

• Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

5.6.1.13. Artículo 13. Conservación de los Mensajes de Datos y Archivo de Documentos a través de Terceros. El cumplimiento de la obligación de conservar documentos, registros o informaciones de mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

5.6.2. Ley 1273 de 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[14].

[14] **LEY 1273 de 2009.** Ministerio de las TIC. Recuperado de: http://www.mintic.gov.co/portal/604/w3-article-3705.html

6. MARCO METODOLOGICO

6.1. TIPO DE ESTUDIO Y DISEÑO DE INVESTIGACIÓN

Se identifica este estudio como tipo de investigación descriptiva pues busca especificar propiedades, y características importantes de cualquier fenómeno que se analice, en especial en la empresa CLINICA LAURA DANIELA, que describe tendencias de un grupo de población[15]. Visto de otra manera, consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento[16].

También, se denota como investigación aplicada que estudia problemas concretos con el objeto de proponer un "plan de acción"[17]. Por otra parte, los estudios de tipo aplicado tienen como fundamento esencial enfocar la atención sobre la solución de teorías a fin de lograr la optimización de la gestión realizada por los sujetos involucrados en el estudio.

En cuanto al diseño de investigación es de campo, pues consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, de allí su carácter de investigación no experimental[18]. También clasifica en diseño transaccional descriptivo porque consiste en medir de un grupo de personas u objetos una o más variables y proporcionar su descripción, lo que presenta un panorama en determinado momento[19].

---

[15] **SABINO, Carlos.** El proceso de investigación, Caracas, Editorial Panapo, En: http://es.slideshare.net/male2712/sabino-carlos-el-proceso-de-investigacion. [2007]

[16] **ARIAS, Fidias.** El proyecto de investigación, introducción a la metodología científica, Sexta edición julio 2012, Editorial Epiteme En: http://es.slideshare.net/paundpro/el-proyecto-de-investigacion-fidias-arias-2012. [2012]

[17] **GIROUX & TREMBLAY.** Metodología de las ciencias humanas, La investigación en acción, Primera edición en español 2004, Editorial Fondo de cultura económica. En: https://imas2010.files.wordpress.com/2010/06/metodologia-de-las-cchh-s-giroux-g-tremblay.pdf [2004]

[18] **TAMAYO & TAMAYO.** El proceso de la investigación científica, Cuarta edición, Editorial Limusa. En: http://es.slideshare.net/sarathrusta/el-proceso-de-investigacion-cientifica-mario-tamayo-y-tamayo1 [2000]

[19] **SAMPIERI**. Roberto Hernández Sampieri, 1998/9, Metodologia de la investigación, Editorial McGraw-Hill En: http://www.univo.edu.sv:8081/tesis/021552/021552_Cap3.pdf [1998]

6.2. POBLACIÓN Y MUESTRA

La población se define como la totalidad del fenómeno a estudiar donde las unidades de población poseen una característica común la cual se estudia y da origen a los datos de la investigación[20].

En este caso, la población objeto de estudio está constituida por el total de los trabajadores de la empresa CLINICA LAURA DANIELA. El tamaño de la población estimada es de 95 empleados los cuales se beneficiarán con el desarrollo del proyecto.

Teniendo en cuenta que una población finita es aquella que todos sus integrantes son conocidos y pueden ser identificados y listados por el investigador en su totalidad para su estudio[21], es posible utilizar un censo poblacional, con el cual es posible estudiar cada uno de los elementos que componen la población cuando ésta es pequeña[22].

6.3. INSTRUMENTOS Y TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Son instrumentos y técnicas de recolección de información de la presente investigación: observación directa, entrevistas y encuestas. Con la colaboración de todo el personal de la empresa CLINICA LAURA DANIELA, será posible realizar las diferentes visitas a las instalaciones de la organización, esto con la finalidad de obtener la información necesaria para la realización del proyecto. Ver anexos D, E, F y G.

6.4. METODOLOGIA PARA EL DESARROLLO DEL PROYECTO

6.4.1. Metodología ISO/IEC 27001. ISO/IEC 27001:2005 es un estándar para la seguridad de la información, aprobado y publicado como estándar internacional en

[20] **TAMAYO & TAMAYO.**, El proceso de la investigación científica, tercera edición, Editorial Limusa. [1997]
[21] **HURTADO,** *Metodología de la investigación holística.* IUTP. Sypal. Caracas MARTINEZ B., C. (1998). *Estadística y muestreo.* Ecoediciones. Colombia. [2000]
[22] **PARRA, J.** Guía de Muestreo. Maracaibo. LUZ. [2003]

octubre de 2005 por *International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission.*

Esta norma ha sido elaborada para 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).

Un SGSI se implanta de acuerdo a estándares de seguridad como el ISO 27001 basado en el código de buenas prácticas y objetivos de control ISO 17799, el cual se centra en la preservación de tres características elementales:

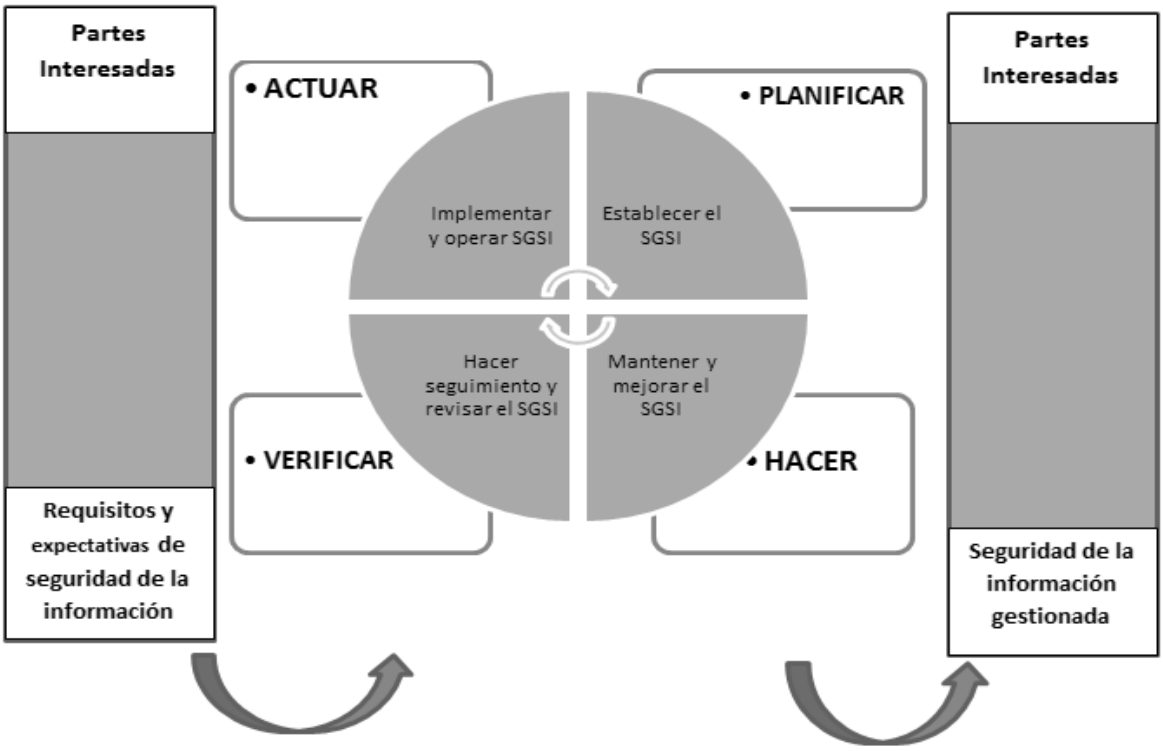
Tabla 1. Clásicos que definen la seguridad de la información basado en la norma ISO/IEC 27001.

- CONFIDENCIALIDAD	La información sólo debe ser vista por aquellos que tienen permiso para ello, no debe poder ser accedida por alguien sin el permiso correspondiente.
- INTEGRIDAD	La información podrá ser modificada solo por aquellos con derecho a cambiarla.
- DISPONIBILIDAD	La información deberá estar disponible en el momento en que los usuarios autorizados requieren acceder a ella.

Fuente: Norma Tecnica Colombiana NTC-ISO/IEC 27001, 2006

Esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI. La figura 1 ilustra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas.

Figura 1. Modelo de procesos PHVA basado en la norma ISO/IEC 27001.



Fuente: Norma Tecnica Colombiana NTC-ISO/IEC 27001, 2006

Tabla 2. Especificación de cada proceso del PHVA basado en la norma ISO/IEC 27001.

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 y la experiencia práctica, y 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.

Fuente: Norma Tecnica Colombiana NTC-ISO/IEC 27001, 2006 Pg 8

Esta norma especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización.

Dentro de las actividades está especificar los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de ellas con el objetivo de asegurar la protección de los activos de información y brinden confianza a las partes interesadas.

6.4.2. Requisitos generales. 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. Para los propósitos de esta norma, el proceso usado se basa en el modelo PHVA que se ilustra en la figura 1.

6.4.3. Establecimiento y gestión del SGSI. La organización debe:

a) Definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.

b) Definir una política de SGSI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología, que:

- Incluya un marco de referencia para fijar objetivos y establezca un sentido general de dirección y principios para la acción con relación a la seguridad de la información.

- Tenga en cuenta los requisitos del negocio, los legales o reglamentarios, y las obligaciones de seguridad contractuales.

- Esté alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del SGSI.

- Establezca los criterios contra los cuales se evaluará el riesgo.

- Haya sido aprobada por la dirección.

c) Definir el enfoque organizacional para la valoración del riesgo.

- Identificar una metodología de valoración del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de seguridad de la información del negocio, identificados.

- Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables.

- La metodología seleccionada para valoración de riesgos debe asegurar que dichas valoraciones producen resultados comparables y reproducibles.

d) Identificar los riesgos

- Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos.

- Identificar las amenazas a estos activos.

- Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.

- Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos.

e) Analizar y evaluar los riesgos.

- Valorar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos.

- Valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente.

- Estimar los niveles de los riesgos.

- Determinar la aceptación del riesgo o la necesidad de su tratamiento a partir de los criterios establecidos literal c).

f) Identificar y evaluar las opciones para el tratamiento de los riesgos. Las posibles acciones incluyen:

- Aplicar los controles apropiados.

- Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos (véase literal c).

- Evitar riesgos, y

- Transferir a otras partes los riesgos asociados con el negocio, por ejemplo: aseguradoras, proveedores, etc.

g)Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos. Los objetivos de control y los controles se deben seleccionar e implementar de manera que cumplan los requisitos identificados en el proceso de valoración y tratamiento de riesgos. Esta selección debe tener en cuenta los criterios para la aceptación de riesgos (literal c), al igual que los requisitos legales, reglamentarios y contractuales.

- Los objetivos de control y los controles se deben seleccionar como parte de este proceso, en tanto sean adecuados para cubrir estos requisitos.

- Los objetivos de control y los controles no son exhaustivos, por lo que puede ser necesario seleccionar objetivos de control y controles adicionales.

h)Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.

i) Obtener autorización de la dirección para implementar y operar el SGSI.

j) Elaborar una declaración de aplicabilidad.

6.4.4. Implementación y operación del SGSI. La organización debe:

a)Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.

b)Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades.

c)Implementar los controles seleccionados para cumplir los objetivos de control.

d)Definir cómo medir la eficacia de los controles o grupos de controles seleccionados, y especificar cómo se van a usar estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles.

NOTA: La medición de la eficacia de los controles permite a los gerentes y al personal determinar la medida en que se cumplen los objetivos de control planificados.

e)Implementar programas de formación y de toma de conciencia,

f) Gestionar la operación del SGSI;

g)Gestionar los recursos del SGSI.

h)Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad.

6.4.5. Seguimiento y revisión del SGSI. La organización debe:

a)Ejecutar procedimientos de seguimiento y revisión y otros controles para:

- Detectar rápidamente errores en los resultados del procesamiento;

- Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron;

- Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada;

- Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores, y

- Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.

b)Emprender revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.

c)Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

d)Revisar las valoraciones de los riesgos a intervalos planificados, y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en:

- La organización,

- La tecnología,

- Los objetivos y procesos del negocio,

- Las amenazas identificadas.

- La eficacia de los controles implementados, y

- EvMentos externos, tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social.

e)Realizar auditorías internas del SGSI a intervalos planificados

NOTA: Las auditorías internas, denominadas algunas veces auditorías de primera parte, las realiza la propia organización u otra organización en su nombre, para propósitos internos.

f) Emprender una revisión del SGSI, realizada por la dirección, en forma regular para asegurar que el alcance siga siendo suficiente y que se identifiquen mejoras al proceso de SGSI.

g) Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión.
h)Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del SGSI.

6.4.6. Mantenimiento y mejora del SGSI. La organización debe, regularmente:

a)Implementar las mejoras identificadas en el SGSI;

b)Emprender las acciones correctivas y preventivas adecuadas. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización;

c)Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias, y en donde sea pertinente, llegar a acuerdos sobre cómo proceder.

6.4.7. Dominios ISO 27001. La norma ISO/IEC 27001 *establece* los requisitos para los Sistemas de Gestión de la Seguridad de la Información (SGSI) de una organización, de tal forma que le permita en todo momento garantizar la confidencialidad, integridad y disponibilidad de la información que maneja.

Esta norma internacional proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI).

La norma ISO/IEC 27001 establece 11 dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

- **Organización de la Seguridad:** que busca establecer un modelo de gerenciamiento para controlar la implementación del sistema y la definición clara de funciones y responsabilidades.

- **Aspectos administrativos:** Este dominio se refiere a la asignación de responsabilidades relativas a la seguridad de la información**,** donde se encuentra el proceso de autorización de recursos para el tratamiento de la información, los acuerdos de confidencialidad, el manejo de los grupos de interés y la revisión independiente de la seguridad de la información. Además, los aspectos que se tienen que tener en cuenta con el manejo de terceros como la identificación de los riesgos derivados del acceso de terceros y la seguridad en contratos con terceros.

- **Gestión de activos:** Este segundo dominio contempla los lineamientos para la gestión de activos que incluye el inventario y las declaraciones de uso de los mismos. Como parte de esta gestión de activos se detallan las directrices para la clasificación de la información.

- **Los recursos humanos y la seguridad de la información:** El recurso humano está considerado como una de las principales fuentes de riesgo para la seguridad de la información por lo tanto en este dominio se tratan los aspectos que se deben tener en cuenta antes, durante y después de la relación laboral. Se incluyen en este apartado los términos y condiciones de contratación, los programas de concienciación, capacitación, los procesos disciplinarios, los puntos a tener en cuenta en caso de cese de la relación laboral o cambio de puesto de trabajo como pueden ser la devolución de activos y la suspensión de las credenciales de acceso.

- **Seguridad física:** Este dominio trata las áreas seguras, donde se incluyen la definición de perímetros de seguridad física y la seguridad de los equipos donde se relaciona, entre otras, la seguridad del cableado, el mantenimiento y la seguridad de los equipos fuera de la compañía.

- **Gestión de comunicaciones:** Este es el dominio más amplio, en él se tratan las responsabilidades y procedimientos de operación, la gestión de los servicios con terceros, la protección contra código malicioso, las **copias de seguridad,** la **seguridad de redes**, el intercambio de información, entre otros aspectos.

- **Control de acceso:** Como parte de este dominio se desarrollan los lineamientos para la **política de control de acceso,** la **gestión de accesos de usuarios,** los controles de acceso a la red, al sistema operativo, a las aplicaciones y a la información. Además, incluye las consideraciones para el manejo de ordenadores portátiles y teletrabajo.

- **Gestión de sistemas de información:** Se desarrollan los requisitos de seguridad de los sistemas de información, el tratamiento correcto de las aplicaciones, los **controles criptográficos**, la seguridad en los procesos de desarrollo y soporte y la gestión de las vulnerabilidades.

- **Gestión de incidentes:** Se tratan recomendaciones alrededor de la notificación de eventos y puntos débiles de seguridad de la información y los procedimientos y responsabilidades que se deberían asignar para la **gestión de incidentes y mejoras de seguridad de la información.**

- **Continuidad del negocio:** Se mencionan los aspectos de seguridad que se deberían tener en cuenta en la gestión de la continuidad del negocio; ya que al ser una etapa donde la información puede estar altamente expuesta se debe desarrollar e implantar de planes de continuidad que incluyan la seguridad de la información.

- **Requisitos legales:** En este apartado se incluyen los aspectos que se deben tener en cuenta para el cumplimiento de los requisitos legales, políticas, normas de seguridad y cumplimiento técnico.

6.4.8. Objetivos de control y controles

ANEXO A NORMA ISO/IEC 27001

(Normativo) Los objetivos de control y los controles enumerados en la Tabla 3 se han obtenido directamente de los de la NTC-ISO/IEC 17799:2005, numerales 5 a

15, y están alineados con ellos. Las listas de estas tablas no son exhaustivas, y la organización puede considerar que se necesitan objetivos de control y controles adicionales. Los objetivos de control y controles de estas tablas se deben seleccionar como parte del proceso de SGSI.

La norma NTC- ISO/IEC 17799:2005, numerales 5 a 15, proporciona asesoría y orientación sobre las mejores prácticas de apoyo a los controles especificados en el literal A.5 a A.15.

6.4.9. Análisis y evaluación de riesgo. El análisis y evaluación de los riesgos se han obtenido directamente de la NTC-ISO 27005 esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001[23].

La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable.

La gestión del riesgo en la seguridad de la información debería contribuir a:

- La identificación de los riesgos.
- La evaluación de los riesgos en términos de sus consecuencias para el negocio y la probabilidad de su ocurrencia.
- La comunicación y entendimiento de la probabilidad y las consecuencias de estos riesgos.
- El establecimiento del orden de prioridad para el tratamiento de los riesgos.[24]

6.4.9.1. Análisis del riesgo.

1. Identificación del riesgo

Introducción a la identificación del riesgo: El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida.

[23] **AREVALO, D. (2014).** Proyecto de norama tecnica colombiana NTC-ISO 27005. Recuperado de: https://fr.slideshare.net/danger-leinad/iso-27005espanol-34883875?cv=1
[24] Op. Cit. Ibíd.

2. Identificación de los activos

Entrada: Alcance y límites para la valoración del riesgo que se va a realizar, lista de los componentes con sus propietarios, ubicación, funciones, etc.

Acción: Se deberían identificar los activos dentro del alcance[25].

Guía para la implementación: Un activo es todo aquello que tiene valor para la organización y por lo tanto requiere de protección. Para la identificación de los activos se recomienda tener en cuenta que el sistema de información consta de más elementos que sólo hardware y software. Este proceso se debe llevar a cabo con un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo.

Se debería identificar al propietario de cada activo, para asignarle la responsabilidad y rendición de cuentas sobre éste. El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización[26].

El límite de la revisión es el perímetro definido de los activos de la organización que debe ser gestionado por parte del proceso de gestión del riesgo en la seguridad de la información.

Salida: una lista de los activos que van a estar sometidos a gestión del riesgo, y una lista de los procesos del negocio relacionados con los activos y su importancia.

3. Identificación de las amenazas

Entrada: Suministra Información sobre las amenazas obtenida de cada uno de los activos, incluyendo su interacción con los usuarios.

Acción: se deberían identificar las amenazas y sus orígenes.
Guía para la implementación: Una amenaza tiene el potencial de causar daños a activos tales como información, procesos, sistemas y por ende a las organizaciones.

---

[25] **AREVALO, D. (2014).** Proyecto de norama tecnica colombiana NTC-ISO 27005. Recuperado de: https://fr.slideshare.net/danger-leinad/iso-27005espanol-34883875?cv=1
[26] Op. Cit. Ibíd.

Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización.

Algunas amenazas pueden afectar a más de un activo, en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

4. Identificación de los controles existentes

Entrada: Documentación de los controles, planes para la implementación del tratamiento del riesgo.

Acción: se deberían identificar los controles existentes y los planificados.

Guía para la implementación: Se debe realizar la identificación de los controles existentes para evitar la duplicación de controles y no incurrir en costos innecesarios. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente, si el control no funciona como se espera, puede causar vulnerabilidades. En un SGSI, de acuerdo con ISO/IEC 27001, se tiene como soporte la revisión de la eficacia del control; Una forma de estimar el efecto del control es ver la manera en que reduce la probabilidad de ocurrencia de la amenaza y la facilidad de explotar la vulnerabilidad, o el impacto del incidente. Las revisiones por parte de la dirección y los reportes de auditoría también suministran información acerca de la eficacia de los controles existentes.

Los controles que se planifican para implementar de acuerdo con los planes de implementación del tratamiento del riesgo, se deberían considerar en la misma forma que aquellos ya implementados.

5. Estimación del riesgo

Metodologías para la estimación del riesgo: El análisis del riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades conocidas y los incidentes anteriores que implicaron a la organización. Una metodología de estimación puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias.

En la práctica, con frecuencia se utiliza la estimación cualitativa en primer lugar para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes.

Posteriormente puede ser necesario realizar un análisis más específico o cuantitativo de los riesgos importantes dado que es, por lo general, menos complejo y menos costoso realizar un análisis cualitativo que uno cuantitativo.

La forma del análisis debería ser consistente con los criterios de evaluación del riesgo desarrollados como parte del establecimiento del contexto.

A continuación, se describen los detalles de las metodologías para la estimación:

a)Estimación cualitativa: La estimación cualitativa utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales (por ejemplo, alta, intermedia y baja) y la probabilidad de que ocurran dichas consecuencias. Una ventaja de la estimación cualitativa es su facilidad de comprensión por parte de todo el personal pertinente, mientras que una desventaja es la dependencia en la selección subjetiva de la escala.

Estas escalas se pueden adaptar o ajustar para satisfacer las circunstancias y se pueden utilizar descripciones diferentes para riesgos diferentes. La estimación cualitativa se puede utilizar:

- Como una actividad de tamizado inicial para identificar los riesgos que requieren un análisis más detallado;

- Cuando este tipo de análisis es adecuado para tomar decisiones;

- Cuando los datos numéricos o los recursos no son adecuados para una estimación cuantitativa.

El análisis cualitativo debería utilizar información con base en hechos y datos, cuando estén disponibles.

b)Estimación cuantitativa: La estimación cuantitativa utiliza una escala con valores numéricos tanto para las consecuencias como para la probabilidad, utilizando datos provenientes de varias fuentes. La calidad del análisis depende de la veracidad y exactitud de los valores numéricos y de la validez de los modelos

utilizados. En la mayoría de los casos, la estimación cuantitativa utiliza datos históricos sobre los incidentes, dando como ventaja que ésta pueda relacionarse directamente con los objetivos de seguridad de la información y los intereses de la organización. Una desventaja es la falta de tales datos sobre riesgos nuevos o debilidades en la seguridad de la información. Una desventaja del enfoque cuantitativo se puede presentar cuando no se dispone de datos basados en los hechos que se puedan auditar, creando así una ilusión del valor y la exactitud de la valoración del riesgo.

La forma en la cual se expresan las consecuencias y la probabilidad, y las formas en las cuales se combinan para proveer el nivel del riesgo varían de acuerdo con el tipo de riesgo y el propósito para el cual se va a utilizar la salida de la valoración del riesgo. La incertidumbre y la variabilidad tanto de las consecuencias como de la probabilidad se deberían ser consideradas en el análisis y comunicarse de manera eficaz.

6.4.9.2. Evaluación del riesgo.

Entrada: una lista de los riesgos con niveles de valor asignado y criterios para la evaluación del riesgo.

Acción: se deberían comparar los niveles de riesgo frente a los criterios para la evaluación del riesgo y sus criterios de aceptación.

Guía para la implementación: La naturaleza de las decisiones pertinentes para la evaluación del riesgo y los criterios de evaluación del riesgo que se utilizarán para tomar dichas decisiones, deben haber sido determinados durante el establecimiento del contexto. Estas decisiones y el contexto se deberían revisar con mayor detalle en esta etapa cuando se sabe más acerca de los riesgos particulares identificados. Con el fin de evaluar los riesgos, las organizaciones deberían comparar los riesgos estimados (utilizando métodos o enfoques seleccionados, tal como se discute en el Anexo E) con los criterios de evaluación del riesgo que se definieron durante el establecimiento del contexto.

6.4.9.3. Identificación y valoración de los activos y evaluación del impacto.

Ejemplos de identificación de los activos: Para realizar la valoración de los activos, es necesario que la organización identifique primero sus activos (con un grado adecuado de detalles). Se pueden diferenciar dos clases de activos.

- Los activos primarios:

- Actividades y procesos del negocio
- Información

- Los activos de soporte (de los cuales dependen los elementos primarios del alcance) de todos los tipos:

- Hardware
- Software
- Redes
- Personal
- Lugar
- Estructura de la organización

Identificación de los activos primarios: Para describir el alcance de manera más precisa, esta actividad consiste en la identificación de los activos primarios (actividades y procesos del negocio, información).

Esta identificación es realizada por un grupo de trabajo mixto que representa al proceso (directores, especialistas en sistema de información y usuarios).

Por lo general, los activos primarios son los procesos y la información centrales de la actividad en el alcance. También se pueden considerar otros activos primarios tales como los procesos de la organización, que serán más convenientes para elaborar una política de seguridad de la información o un plan de continuidad del negocio. Dependiendo del propósito, algunos estudios no exigen un análisis exhaustivo de todos los elementos que constituyen el alcance. En tales casos, las fronteras del estudio pueden estar limitadas a los elementos clave del alcance.

Valoración de los activos: El paso siguiente a la identificación de los activos es pactar la escala que se va a utilizar y los criterios para la asignación de una ubicación particular en esa escala para cada uno de los activos, con base en la valoración. Debido a la diversidad de activos que se encuentran en la mayoría de las organizaciones, es probable que algunos activos que tengan un valor monetario

conocido sean valorados en la moneda local en donde están presentes, mientras otros que tiene un valor más cualitativo se les puede asignar un rango de valores, por ejemplo, desde "muy bajo" hasta "muy alto". La decisión de utilizar una escala cuantitativa en lugar de una cualitativa es realmente un asunto de preferencia organizacional, pero debería ser pertinente para los activos que se están valorando.

Ambos tipos de valoración se pueden utilizar para el mismo activo.

6.4.9.4. Eenfoques para la evaluación de riesgos en la seguridad de la información.

ANEXO E DE LA NORMA ISO 27001

(Informativo)

1. **Evaluación de alto nivel de riesgos en la seguridad de la información:** La evaluación de alto nivel permite la definición de las prioridades y la cronología de las acciones. Por varias razones, tales como el presupuesto, puede no ser posible implementar todos los controles simultáneamente y únicamente se pueden atender los riesgos más críticos a través del proceso de tratamiento de riesgos. De igual modo, puede ser prematuro iniciar una gestión detallada del riesgo si la implementación sólo se puede dar después de uno o dos años. Para lograr este objetivo, la evaluación de alto nivel puede empezar con una evaluación de alto nivel de las consecuencias en lugar de empezar con un análisis sistemático de amenazas, vulnerabilidades, activos y consecuencias.

Otra razón para empezar la evaluación de alto nivel es sincronizar con otros planes relacionados con la gestión de cambios (o continuidad del negocio). Por ejemplo, no está bien asegurar completamente un sistema o aplicación si se planifica subcontratarla en el futuro cercano, aunque aún puede valer la pena hacer la evaluación de riesgos con el fin de definir el contrato de subcontratación.

Las características de la repetición de la evaluación de riesgos de alto nivel pueden incluir las siguientes:

- La evaluación de alto nivel de los riesgos puede abordar una visión más global de la organización y su sistema de información, considerando los aspectos tecnológicos como dependientes de los aspectos del negocio. Al hacer esto, el

análisis del contexto se concentra más en el negocio y el ambiente operativo que en los elementos tecnológicos.

- La evaluación de alto nivel de los riesgos puede abordar una lista más limitada de amenazas y vulnerabilidades agrupadas en dominios definidos o apresurar el proceso, puede enfocarse en riesgos o escenarios de ataque en lugar de sus elementos.

- Los riesgos representados en una evaluación de alto nivel de los riesgos con frecuencia son dominios de riesgo más generales que riesgos específicos identificados. Dado que los escenarios o las amenazas se agrupan en dominios, el tratamiento del riesgo propone listas de controles en este dominio. Las actividades de tratamiento del riesgo intentan primero proponer y seleccionar controles comunes que sean válidos a través de todo el sistema.

- Sin embargo, la evaluación de alto nivel de los riesgos, debido a que pocas veces aborda los detalles tecnológicos, es más adecuada para proporcionar controles organizacionales y no técnicos y aspectos de gestión de los controles técnicos, o salvaguardas técnicas claves y comunes como por ejemplo los antivirus y las copias de respaldo.

Las ventajas de una evaluación de alto nivel de los riesgos son las siguientes:

- La incorporación de un enfoque inicial sencillo probablemente tenga aceptación del programa de evaluación de riesgos.

- Sería posible construir un panorama estratégico de un programa de seguridad de la información en la organización, es decir, actuaría como una buena ayuda de planificación;

- Los recursos y el dinero se pueden aplicar donde son de más beneficio, y se tratarían primero los sistemas que probablemente tenga mayor necesidad de protección.

Dado que los análisis iniciales de riesgos son de alto nivel y potencialmente menos exactos, la única desventaja potencial es que puede no identificarse algunos procesos o sistemas del negocio que requieren de una segunda evaluación detallada del riesgo. Esto se puede evitar si existe información adecuada sobre todos los aspectos de la organización y sus sistemas e información, incluyendo la

información obtenida de la evaluación de los incidentes de seguridad en la información.

La evaluación de alto nivel de los riesgos toma en consideración los valores para el negocio de los activos de información y los riesgos desde el punto de vista del negocio de la organización. En el primer punto de decisión varios factores facilitan la determinación de si la evaluación de alto nivel es adecuada para tratar los riesgos; estos factores pueden incluir los siguientes:

- Los objetivos del negocio que se deben alcanzar utilizando diversos activos de información.

- El grado hasta el cual el negocio de la organización depende de cada activo de información, es decir, si las funciones que la organización considera críticas para su supervivencia por la conducta eficaz del negocio dependen de cada uno de los activos, o de la confidencialidad, integridad, disponibilidad, no repudio, responsabilidad, autenticidad y confiabilidad de la información almacenada y procesada en este activo.

- El grado de inversión en cada uno de los activos de información, en términos de desarrollo, mantenimiento o reemplazo del activo;

- Los activos de información para los cuales la organización asigna directamente un valor.

Al evaluar estos factores, la decisión se hace más fácil. Si los objetivos de un activo son extremadamente importantes para conducir los negocios de la organización, o si los activos están en alto riesgo, se debería llevar a cabo una segunda repetición, la evaluación detallada del riesgo, para el activo particular de información (o parte de él).

Una regla general a aplicar es: si la falta de seguridad de la información puede dar como resultado consecuencias adversas significativas para una organización, sus procesos del negocio o sus activos, es necesaria una segunda repetición de la evaluación del riesgo, en un grado más detallado, para identificar los riesgos potenciales.

2. **Evaluación detallada de los riesgos en la seguridad de la información:** El proceso de evaluación detallada de los riesgos en la seguridad de la información

implica la identificación y evaluación profundas de los activos, la evaluación de las amenazas para tales activos y la evaluación de las vulnerabilidades. Los resultados de estas actividades se utilizan entonces para evaluar los riesgos y luego identificar su tratamiento.

El paso detallado usualmente exige tiempo, esfuerzo y habilidad considerables y por lo tanto puede ser más adecuado para sistemas de información en alto riesgo. La etapa final de la evaluación detallada de los riesgos en la seguridad de la información es evaluar los riesgos globales, lo cual constituye el enfoque de este anexo.

Las consecuencias se pueden evaluar de varias maneras, incluyendo el uso de medidas cuantitativas, por ejemplo, monetarias, y cualitativas (las cuales se pueden basar en el uso de adjetivos tales como moderado o grave) o una combinación de ambas. Para evaluar la probabilidad de ocurrencia de una amenaza, se debería establecer el marco temporal en el cual el activo tendrá valor o necesitará protección. La probabilidad de ocurrencia de una amenaza específica está afectada por los siguientes aspectos:

- Lo atractivo que sea el activo, o el impacto posible aplicable cuando se toma en consideración una amenaza humana deliberada.

- La facilidad de conversión en recompensa de la explotación una vulnerabilidad del activo, aplicable cuando se toma en consideración una amenaza humana deliberada.

- Las capacidades técnicas del agente amenazador, aplicable a amenazas humanas deliberadas.

- La susceptibilidad de la vulnerabilidad a la explotación, aplicable tanto a vulnerabilidades técnicas como no técnicas.

Muchos métodos utilizan tablas y combinan medidas subjetivas y empíricas. Es importante que la organización utilice un método con el cual esté cómoda, en el cual la organización tenga confianza y que produzca resultados repetibles. A continuación, se indican algunos ejemplos de técnicas basadas en tablas.

EJEMPLO 1 Matriz con valores predefinidos: En los métodos de evaluación de riesgos de este tipo, los activos físicos reales o propuestos se evalúan en términos

de costos de reemplazo o de reconstrucción (es decir, mediciones cuantitativas). Estos costos se convierten después en la misma escala cualitativa a la utilizada para la información (véase más adelante). Los activos de software, reales o propuestos, se evalúan de la misma manera que los activos físicos, con costos de compra o reconstrucción identificados y luego se convierten en la misma escala cualitativa de la utilizada para la información. Además, si se observa que algún software de aplicación tiene sus propios requisitos intrínsecos de confidencialidad o integridad (por ejemplo, si el código fuente es en sí mismo sensible comercialmente), se evalúa de la misma manera que la información.

Los valores para la información se obtienen entrevistando a personas seleccionadas de la gerencia del negocio (los "propietarios de los datos"), quienes pueden hablar con autoridad acerca de los datos, determinar los valores y la sensibilidad de los datos realmente el uso o que se van a almacenar, procesar, o a los que se va tener acceso. Las entrevistas facilitan la evaluación del valor y la sensibilidad de la información en términos de los escenarios más desfavorables cuya ocurrencia razonablemente se podría esperar a partir de consecuencias adversas para el negocio, debidas a divulgación no autorizada, modificación no autorizada, falta de disponibilidad durante diversos períodos de tiempo y destrucción.

La evaluación se logra utilizando directrices para evaluación de la información, las cuales comprenden los siguientes temas:

- Seguridad personal.
- Información personal.
- Obligaciones legales y reglamentarias.
- Cumplimiento de la ley.
- Intereses comerciales y económicos.
- Pérdida financiera/alteración de actividades.
- Orden público.
- Políticas y operaciones del negocio.
- Pérdida del buen nombre.

- Contrato o acuerdo con un cliente.

Las directrices facilitan la identificación de los valores en una escala numérica, permitiendo así el reconocimiento de valores cuantitativos cuando es posible y lógico, y valores cualitativos cuando no son posibles los valores cuantitativos, por ejemplo, cuando se pone en peligro la vida humana[27].

La siguiente actividad principal es la terminación de pares de concesionarios para cada tipo de amenaza, para cada agrupación de activos con los cuales se relaciona el tipo de amenaza, con el fin de habilitar la evaluación de los niveles de amenazas (probabilidad de ocurrencia) y niveles de vulnerabilidades (facilidad de explotación por parte de las amenazas para causar consecuencias adversas). Cada respuesta a un interrogante suscita un puntaje. Estos puntajes se acumulan a través de una base de conocimientos y se compara con los rangos. Esto identifica los niveles de amenaza en una escala de alto a bajo y los niveles de vulnerabilidad de manera similar, tal como se presenta en el ejemplo de la matriz, diferenciando entre los tipos de consecuencias según sea pertinente. La información para completar los cuestionarios se debería reunir en entrevistas con personal técnico adecuado y personal de acompañamiento, así como de inspecciones físicas del lugar y revisiones de documentos.

Los valores del activo, y los niveles de amenaza y vulnerabilidad, pertinentes para cada tipo de consecuencias se contrastan en una matriz como la que se indica más adelante con el fin de identificar, para cada combinación, la medida pertinente de riesgo en una escala de 0 a 8. Los valores se ubican en la matriz de manera estructurada. El ejemplo es el siguiente:

Tabla 3. Matriz con valores predefinidos

	Probabilidad de ocurrencia - amenaza	**Baja**			**Media**			**Alta**		
	Facilidad de explotación	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Valor de activo										

Fuente: Guía de Riegos DAFP, adecuación Autor

[27] **AREVALO, D. (2014).** Proyecto de norama tecnica colombiana NTC-ISO 27005. Recuperado de: https://fr.slideshare.net/danger-leinad/iso-27005espanol-34883875?cv=1

Para cada uno de los valores, las vulnerabilidades pertinentes y sus amenazas correspondientes se toman en consideración. Si existe una vulnerabilidad sin una amenaza correspondiente, o una amenaza sin una vulnerabilidad correspondiente, en el momento no existe riesgo (pero se debe tener cuidado en caso de que esta situación cambie). Ahora, la fila adecuada en la matriz se identifica por el valor del activo, y la columna adecuada se identifica por la probabilidad de ocurrencia de la amenaza y la facilidad que explotación. Por ejemplo, si el activo tiene un valor de 3, la amenaza es “alta” y la vulnerabilidad “baja”, la medida del riesgo es de 5[28].

Asumiendo que un activo tiene un valor de 2, por ejemplo, para modificación, el nivel de amenaza es “bajo” y la facilidad de explotación es “alta”, entonces la medida del riesgo es de 4. El tamaño de la matriz, en términos de la cantidad de categorías de probabilidad de la amenaza, categorías de facilidad de explotación y la cantidad de categorías de valoración de activos, se puede ajustar a las necesidades de la organización. Las columnas y las filas adicionales requerirán de medidas adicionales del riesgo. El valor de este enfoque está en la clasificación de los riesgos que se van a tratar.

Una matriz similar a la que se presenta en la Tabla 4 resulta de la consideración de la probabilidad de un escenario de incidente, graficado frente al impacto estimado en el negocio. La probabilidad de un escenario de incidente está dada por una amenaza que explota una vulnerabilidad con una probabilidad determinada. La Tabla indica esta probabilidad frente al impacto en el negocio relacionado con el escenario de incidente. El riesgo resultante se mide en una escala de 0 a 8 que se puede evaluar frente a los criterios de aceptación del riesgo. Esta escala de riesgos también se podría trazar para una clasificación más sencilla del riesgo total, por ejemplo, así:

- Riesgo bajo: 0-2.
- Riesgo medio: 3 - 5.
- Riesgo alto: 6-8

[28] **AREVALO, D. (2014).** Proyecto de norama tecnica colombiana NTC-ISO 27005. Recuperado de: https://fr.slideshare.net/danger-leinad/iso-27005espanol-34883875?cv=1

Tabla 4. Escala de riesgos

	Probabilidad del escenario de incidente	Muy baja (muy improbable)	Baja (Improbable)	Media (Posible)	Alta (Probables)	Muy alta (Frecuente)
Impacto en el negocio	Muy baja					
	Baja					
	Media					
	Alta					
	Muy alta					

Fuente: Guía de riesgos DAFP

EJEMPLO 2 Clasificación de las amenazas mediante las medidas del riesgo: Se puede utilizar una matriz o una tabla para relacionar los factores de consecuencias (valor del activo) y la probabilidad de ocurrencia de la amenaza (teniendo en cuenta los aspectos de vulnerabilidad). El primer paso es evaluar las consecuencias (valor del activo), en una escala predefinida, por ejemplo, de 1 hasta 5, de cada uno de los activos amenazados (columna "b" en la tabla). El segundo paso es evaluar la probabilidad de ocurrencia de la amenaza en una escala predefinida, por ejemplo, de 1 hasta 5, de cada una de las amenazas (columna "c" en la tabla). El tercer paso es calcular la medida del riesgo multiplicando (b x c). Finalmente, las amenazas se pueden clasificar en orden de sus medidas de riesgo asociadas. Observe que, en este ejemplo, 1 se toma como la consecuencia más baja y la probabilidad más baja de ocurrencia.

Tabla 5. Clasificación de las amenazas mediante las medidas del riesgo

Descriptor de la amenaza (a)	Consecuencia (valor del activo) (b)	Probabilidad de ocurrencia de la amenaza (c)	Medida del riesgo (d)	Clasificación de la amenaza (e)
Amenaza A				
Amenaza B				
Amenaza C				
Amenaza D				
Amenaza E				
Amenaza F				

Fuente: Guía de riesgos DAFP

Como se indica en la tabla, este es un procedimiento que permite comparar y clasificar en orden de prioridad diferentes amenazas con diferentes consecuencias y probabilidad de ocurrencia, como se muestra aquí. En algunos casos será necesario asociar valores monetarios a las escalas empíricas utilizadas aquí.

EJEMPLO 3 Evaluación de un valor para la probabilidad y las consecuencias posibles de los riesgos: En este ejemplo, el énfasis se hace en las consecuencias de los incidentes de seguridad de la información (es decir, los escenarios de incidente) y en la determinación de cuáles sistemas deberían tener prioridad. Esto se lleva a cabo evaluando dos valores para cada uno de los activos y riesgos, los cuales en combinación determinarán el puntaje para cada uno de los activos. Cuando los puntajes de todos los activos para el sistema se suman, se determina una medida del riesgo para ese sistema.

Primero, se asigna un valor para cada uno de los activos. Este valor se relaciona con las consecuencias adversas potenciales que se pueden originar si el activo está amenazado.

Para cada amenaza aplicable al activo, este valor se asigna a ese activo.

Enseguida se evalúa el valor de la probabilidad. Esta evaluación se hace a partir de una combinación de la probabilidad de ocurrencia de la amenaza y la facilidad de explotación de la vulnerabilidad, véase la Tabla 6 que expresa la probabilidad de un escenario de incidente.

Tabla 6. Probabilidad de un escenario de incidente.

Posibilidad de amenaza	**Baja**			**Media**			**Alta**		
Niveles de vulnerabilidad	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Valor de la probabilidad de un escenario de incidente	0	1	2	1	2	3	2	3	4

Fuente: Guía de riesgos DAFP

A continuación, se asigna un puntaje para el activo/la amenaza determinando la intersección del valor del activo y del valor de la probabilidad en la tabla 8. Los

puntajes del activo/las amenazas se totalizan para obtener un puntaje total para ese activo. Esta cifra se puede utilizar para diferenciar entre los activos que forman parte de un sistema.

Cuadro 1. Puntaje para el activo/la amenaza

Valor del activo					
Valor de la probabilidad					
0					
1					
2					
3					
4					

Fuente: Guía de riesgos DAFP

El paso final es totalizar todos los puntajes totales de los activos del sistema, obteniendo un puntaje para ese sistema. Este puntaje se puede utilizar para diferenciar entre sistemas y determinar la prioridad que se debería dar a la protección del sistema en los siguientes ejemplos todos los valores se seleccionan al azar.

Suponga que el sistema S tiene tres valores A1, A2 y A3. Suponga también que existen dos amenazas T1 y T2 que se aplican el sistema S. El valor de A1 es 3, el valor de A2 es 2 y el de A3 es 4.

Si para A1 y T1 la probabilidad de amenaza es baja y la facilidad de explotación de la vulnerabilidad es media, entonces el valor de la probabilidad es 1 (Véase Tabla 7).

El puntaje del activo/la amenaza A1/T1 se puede derivar Cuadro 1 como la intersección del valor del activo 3 y el valor de probabilidad 1, es decir 4. De igual modo, para A1/T2, la probabilidad de amenaza es media y la facilidad de explotación de la vulnerabilidad es alta, se tiene un puntaje para A1/T2 de 6.

Ahora, se puede calcular el puntaje total de los activos A1T, es decir 10. El puntaje total del activo se puede calcular para cada uno de los activos y amenazas aplicables. El puntaje del sistema total se calcula sumando A1T + A2T + A3T para obtener ST.

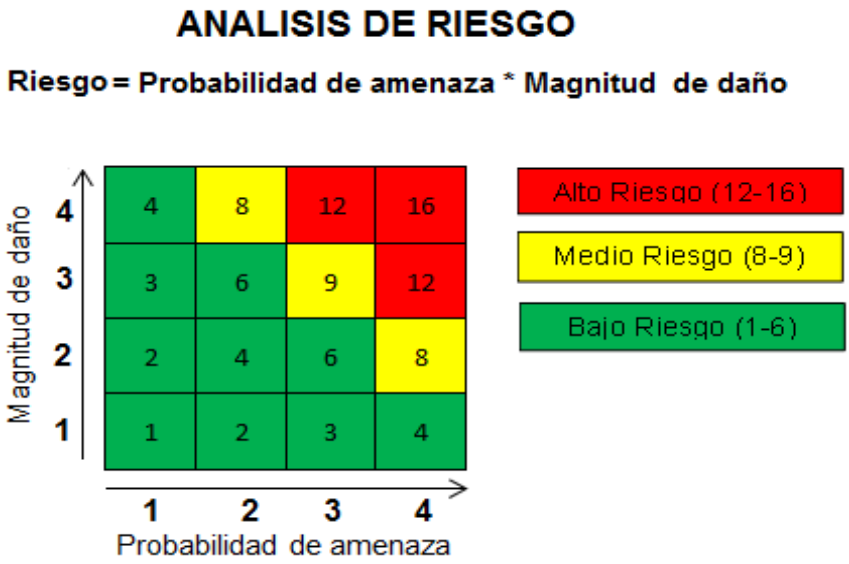
Se pueden comparar sistemas diferentes para establecer prioridades y diferenciar activos dentro de un sistema.

Los ejemplos anteriores se presentan en términos de sistemas de información, sin embargo, un enfoque similar se puede aplicar a los procesos del negocio.

6.4.10. Niveles de riesgo: Para la evaluación de los riesgos se utiliza una matriz o tabla “para relacionar el valor del activo y la probabilidad de ocurrencia de la amenaza, teniendo en cuenta los aspectos de vulnerabilidad”.

El valor del activo se determina teniendo en cuenta “el costo en que se incurre debido a la perdida de confidencialidad, integridad y disponibilidad como resultado de un incidente”.

Figura 2. Análisis de riesgo



Fuente: Guía del Riesgo DAFP

7. DISEÑO Y DESARROLLO DE LA SOLUCIÓN

7.1. PLANEACIÒN DE LA AUDITORÍA

La planeación es el conjunto de procedimientos documentados y diseñados para alcanzar los objetivos específicos de la Auditoria. En ésta se identifican los recursos, procesos y acciones que se necesitan para hacer el trabajo de forma eficiente.

El punto de partida en este proyecto será el conocimiento general acerca de la Clínica Laura Daniela de la ciudad de Valledupar, con el fin de obtener y presentar aspectos relacionados con las áreas legal, comercial e institucional. De igual manera, se realizará un análisis detallado de la aplicación Krystalos en sus procedimientos de manejo y control de los datos; y asociado a éste, se realizará un estudio alrededor de los elementos involucrados en el almacenamiento, procesamiento y distribución de la información.

El paso siguiente será establecer los objetivos, los cuales permitirán obtener pautas claras en la realización de la investigación y enmarcarán la dinámica de trabajo en la Auditoría.

Posteriormente, se procederá a registrar los análisis, comprobaciones, verificaciones e interpretaciones; obtenidos a partir de las evidencias que proporcionarán los datos requeridos para la elaboración de los papeles de trabajo. Estos documentos serán el soporte argumentativo para dar las opiniones, juicios y conclusiones acerca del Sistema de Información examinado. La realización efectiva de visitas, entrevistas y encuestas al personal de labores de esta entidad de salud, con el objeto de obtener información veraz acerca del Sistema de Información Krystalos, garantizará la consecución de los papeles de trabajo y, por consiguiente, la argumentación necesaria para realizar finalmente un informe de Auditoria completo que describa la situación real acerca del manejo y procesamiento de la información.

La investigación estará enmarcada dentro del Tipo de Auditoria Externa. Esta permitirá obtener una opinión independiente y con mayor objetividad acerca de la información procesada mediante la aplicación Krystalos, y facilitará la toma decisiones a la parte administrativa en cuanto a los controles y mejoras que se

requieran para optimizar el rendimiento de los procesos relacionados con el envío, procesamiento y recepción de los datos.

7.2. ALCANCE DE LA AUDITORÍA

El alcance de la auditoria está determinado por los objetivos de la misma, así como también por la verificación de los procesos, procedimientos y actividades que comprometen los activos del sistema de información, relacionados con el área administrativa y financiera. Esta auditoría se realizará en los componentes o activos de la empresa clínica integral Laura Daniela (Hardware, Software, Red, Sitio, Organización) de los cuales se identificarán sus vulnerabilidades y amenazas y se evaluarán para determinar sus controles, teniendo en cuenta la metodología ISO 27001. De lo anterior se desarrollará sus respectivas conclusiones y recomendaciones para cada uno de los procesos evaluados en cada componente.

El alcance define en forma específica el área y los parámetros en que va a desarrollarse la Auditoria informática, complementándose con los objetivos que se han planteado previamente acerca de ésta; determinando así el marco de trabajo y las pautas a utilizar en el procedimiento investigativo.

En esta investigación se analizarán aspectos involucrados con el manejo y tratamiento de la información, dentro de los cuales podríamos mencionar la eficiencia, seguridad, oportunidad e integridad de los datos. Además, se analizarán los recursos necesarios para facilitar el trabajo a los usuarios involucrados con este sistema de Información.

7.3. ANÀLISIS DEL SISTEMA ACTUAL

Es oportuno precisar que la trascendencia que puede tener una buena utilización de los procesos informáticos implementados en cualquier entidad, es crucial para el normal desarrollo de las actividades internas, y, por ende, garantizan la veracidad y la eficiencia en los procesos de emisión – recepción de los datos manejados por la empresa.

Con base a esto, al realizar un análisis al sistema de información Krystalos, que es una de las aplicaciones utilizadas en el desarrollo de los procesos informáticos ejecutados en la Clínica Laura Daniela, es notable la necesidad de realizar un estudio detallado que conduzca a la obtención de falencias y errores presentados en el tratamiento de la información, y si es necesario, proponer e implementar las medidas necesarias para un mejoramiento en estos procedimientos.

Este análisis deberá realizarse a través de encuestas, entrevistas e información personalizada, que conlleven a la obtención de datos reales y actuales acerca de la calidad del sistema, el manejo de los recursos informáticos, los mecanismos que contribuyen a la integridad de los datos y las estrategias utilizadas para minimizar los riesgos existentes.

Finalmente, se plantearán alternativas que contribuyan a la eficiencia y fiabilidad del sistema informático de esta institución, estableciendo controles mediante estándares de seguridad con miras a conseguir un mejoramiento en las necesidades prioritarias de los usuarios, y obteniendo de esta manera, respuestas para la empresa.

7.4. IDENTIFICACIÒN DE NECESIDADES

- Determinar los errores y vulnerabilidades que presente la aplicación Krystalos durante su ejecución.

- Determinar las vulnerabilidades que presente el sistema de información en su totalidad. (Página web, redes, Base de datos)

- Implementar controles y normas de auditoria que garanticen fiabilidad en los procesos Informáticos.

- Elaborar el informe de auditoría de seguridad en Pro del Sistema de Información.

7.5. APLICACIÓN DE LA METODOLOGÍA NTC ISO/IEC 27001

7.5.1. Introducción. La implementación de la metodología NTC ISO/IEC 27001 se hace con el objeto de estudiar a fondo la aplicación Krystalos de la Clínica Laura Daniela, con miras de emitir una opinión independiente sobre la seguridad informática y asegurar que las tecnologías de la información (TI) estén alineadas con los respectivos fines sociales, sus recursos sean usados responsablemente y sus riesgos administrados de forma apropiada.

Para la aplicación adecuada de esta metodología y la norma, se abordarán algunos aspectos fundamentales para conocer en forma general esta institución de prestación de servicios de salud.

7.6. DESCRIPCION GENERAL DE LA EMPRESA

7.6.1. Naturaleza jurídica. Entidad privada con ánimo de lucro.

7.6.2. Objeto social. La Clínica Laura Daniela es una institución de prestación de servicios de salud.

7.6.3. Representante legal. Actualmente, el representante legal de la Clínica Laura Daniela es el Señor JAIME ARCE GARCÍA.

7.6.4. Misión. Somos una Institución Prestadora de Servicios de Salud de alta complejidad, autónoma, visionaria, abierta al cambio, que actúa como centro de referencia ofreciendo atención en salud en forma integral, accesible, oportuna, segura y humanizada, basada en estándares de calidad, apoyados por un talento humano idóneo, una adecuada tecnología y procesos de mejoramiento continuo, contribuyendo a la satisfacción de las necesidades de salud de los usuarios y su familia, garantizando la rentabilidad económica, responsabilidad social y la conservación del medio ambiente.[29]

[29] **CIE. Clinica Integral de Emergencia.** Mision y Vision. Recuperado de: http://www.clinicaintegral.com.co/nosotros/misi%C3%B3n-y-visi%C3%B3n.html

7.6.5. Visión. En el 2019, seremos una Institución Prestadora de Servicios de Salud acreditada con altos estándares de calidad y seguridad clínica, siendo reconocida a nivel regional y nacional por el amplio portafolio e integralidad de nuestros servicios, contando con un talento humano calificado, una infraestructura y tecnología de punta acorde al nivel de complejidad, buscando generar permanentemente un impacto positivo en la sociedad.[30]

7.6.6. Valores institucionales

- Humanización
- Lealtad
- Responsabilidad
- Respeto
- Tolerancia
- Honestidad
- Profesionalismo
- Trabajo en Equipo

7.6.7. Objetivos institucionales

- Consolidar el mejoramiento de la calidad en los servicios ofrecidos y fidelizar a Usuarios y Clientes.

- Contar con empleados idóneos, satisfechos, motivados y con excelente desempeño.

- Fortalecer la integración entre las clínicas de Valledupar para generar acuerdos frente al desarrollo del sector en aspectos de mercadeo, contratación e integración de servicios.

[30] Op. Cit. Ibíd.

• Consolidar un proceso de gestión eficaz que mejore el posicionamiento institucional, mayor competitividad, excelencia en el servicio y la satisfacción del usuario.

• Adoptar los estándares de calidad y de buenas prácticas en manufactura y servicios exigidos por los entes de vigilancia y control.

• Garantizando la seguridad del paciente y su familia.

• Facilitar el acceso a información oportuna y confiable que soporte la toma de decisiones asertivas e incentive grupos y servicios auto gestionados y auto controlados.

• Fortalecer el mejoramiento continúo basado en la innovación, las mejores competencias laborales que soporten el desarrollo institucional.

• Realizar proceso selectivo de mercadeo y contratación con clientes de reconocida capacidad de pago para mejorar el flujo de recursos.

7.6.8. Política de calidad. Prestamos servicios de salud oportunos, pertinentes, seguros, con calidez, atención personalizada, satisfaciendo las necesidades y expectativas de nuestros usuarios y clientes, asegurando la gestión a través de la mejora continúa.

Dentro de los objetivos de la Política de calidad están:

• Operar con una infraestructura adecuada y suficiente.

• Consolidar la proyección integral e idoneidad del talento humano.

• Apropiar una cultura de mejoramiento continuo, basada en la innovación y la investigación científica.

• Diferenciar y optimizar la calidad de todos los servicios y promover la prevención en todos los niveles de atención.

• Diseñar, implantar y operar un sistema de gestión por procesos efectivo.

- Lograr altos índices de satisfacción entre nuestros clientes.

- Optimizar la gestión financiera.

- Aportar al desarrollo social de la población de la región, alcanzando proyección social.

7.6.9. Organigrama (Ver anexo 1)

7.6.9.1. Identificación de los activos. Los activos de información son representados por aquellos elementos que contienen o manipulan información dentro de una organización, motivo por el cual, requieren cuidado y protección por parte de la administración.

La Clínica Laura Daniela de la Ciudad de Valledupar posee una cantidad representativa de activos de información, que se encuentran distribuidos estratégicamente en las distintas áreas de trabajo, y los cuales, trabajando de manera coordinada hacen posible los procesos involucrados con la gestión y transmisión de datos dentro de la empresa.

Para más claridad, en cuanto a los activos involucrados en el procesamiento de la información en la Clínica Laura Daniela, se describen en la siguiente tabla.

- **Equipos De Cómputo En La Clínica Laura Daniela**

Tabla 7. Información de Equipos de Cómputo Activos

CODIGO	DESCRIPCION	CANTIDAD	UBICACIÓN	RESPONSABLE	TIPO
CE	*MARCA DELL VOSTRO 200 PROCESADOR INTEL CELERON 1.60 GHz, 1GB RAM, DD 80 GB.*	*133*	*Admisiones*	*Jenifer*	*Escritorio*
CP	*PORTATIL MARCA LENOVO G470 PROCESADOR INTEL CORE i3 2.30GHz, 4 GB DE RAM, DD 700GB.*	*9*	*Facturación*	*Rikilda*	*Portátil*

Fuente: Autor

- **Impresoras Activas en la Clínica Laura Daniela**

Tabla 8. Información de Impresoras Activas

CÓDIGO	DESCRIPCIÓN	CANTIDAD	UBICACIÓN	RESPONSABLE	TIPO
IMP	*MARCA KYOCERA KM-3040. MULTIFUNCIONAL*	*38*	*Admisiones 2*	*Jenifer*	*Impresora*

Fuente: Autor

- **Switchs Activos en la Clínica Laura Daniela**

Tabla 9. Información de Switchs Activos

CODIGO	DESCRIPCION	CANTIDAD	UBICACIÓN	RESPONSABLE	TIPO
SW-01	*MARCA DLINK 8 PUERTOS DES-1008A COLOR NEGRO.*	*23*	*Admisiones 3*	*Jenifer*	*Switch*

Fuente: Autor

- **Routers Activos en la Clínica Laura Daniela**

Tabla 10. Información de Routers Activos

CODIGO	DESCRIPCION	CANTIDAD	UBICACIÓN	RESPONSABLE	TIPO
ROU	*MARCA LINKSYS WRT320N 4 PUERTOS COLOR NEGRO*	*5*	*Cirugía 2*	*Dolores*	*Router*

Fuente: El Autor

- **Servidores Activos en la Clínica Laura Daniela**

Tabla 11. Información de Servidores Activos

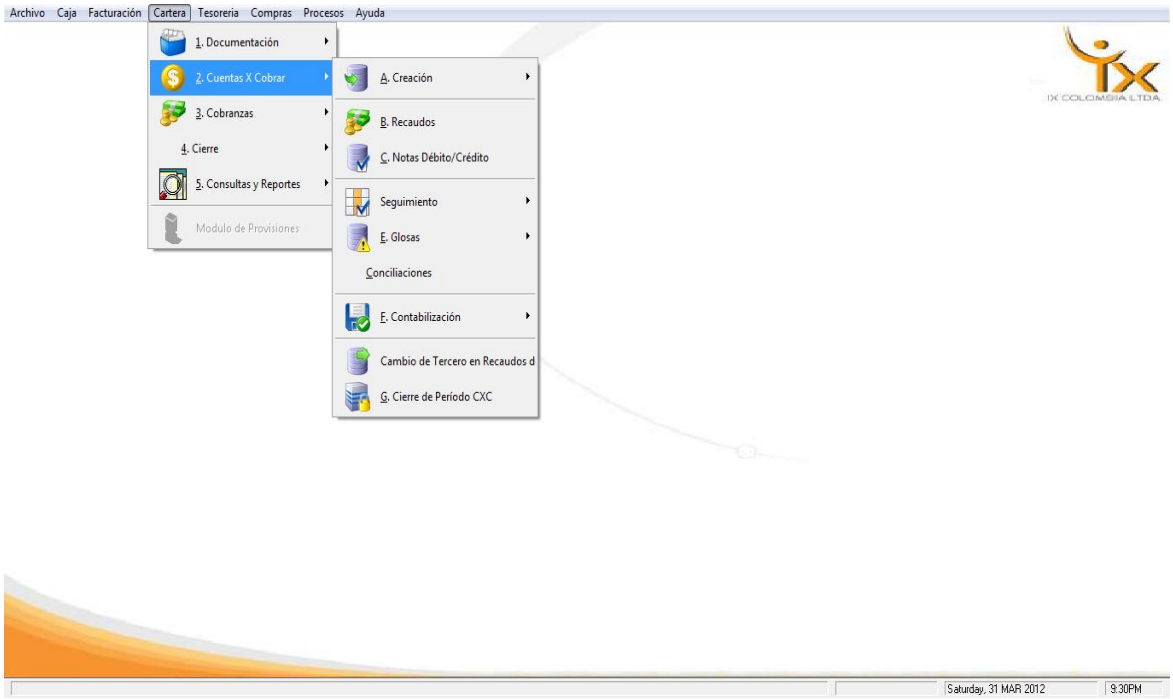
CODIGO	DESCRIPCION	CANTIDAD	UBICACIÓN	RESPONSABLE	TIPO
SER-01	*CPU IMÁGENES RX HP P5700 SERVIDOR.*	*3*	*Sistemas*	*Edgardo*	*Servidor*

Fuente: El Autor

7.7. DESCRIPCIÒN GENERAL DE LA APLICACIÒN KRYSTALOS

7.7.1. Módulo de cartera

Figura 3. Módulo de cartera Aplicación Krystalos



Fuente: Aplicación Krystalos

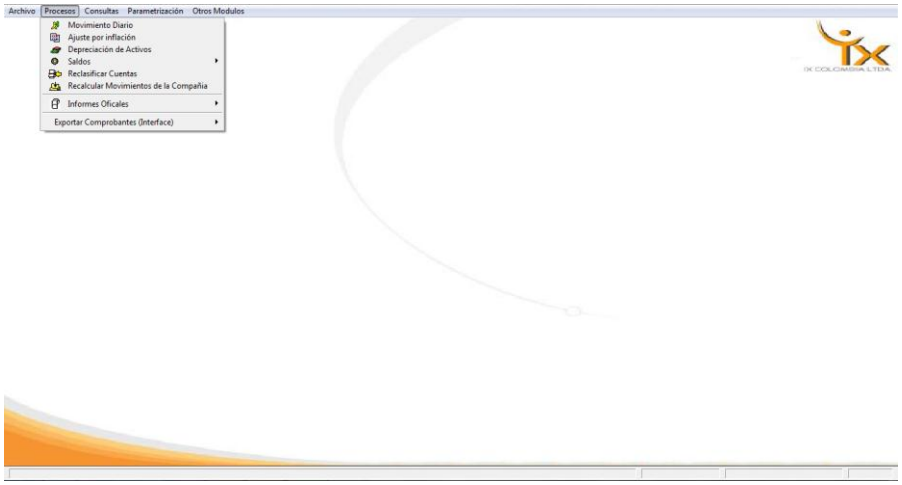
• **Características:** El *MODULO CARTERA* permite mantener el control de las cuentas por cobrar de la empresa, respetando las normas y resoluciones establecidas por los entes de Control y permitiendo el manejo de la gestión de los funcionarios. Además, tiene como fin la generación de registro de las facturas o cuentas por cobrar emitidas por los procesos de inventarios o asistenciales, y de los recibos de caja de tesorería, manejo eficiente del proceso de seguimiento de cuentas y el manejo de acuerdos de pago.

Este módulo cuenta con las siguientes características:

- Manejo de Clientes
- Información en línea de la cartera
- Maneja Acuerdos de Pagos
- Cartera por edades
- Genera Extractos de Clientes.
- Permite realizar la gestión de cartera.
- Permite efectuar traslado de Valores entre Clientes
- Permite el registro de Cuentas por Cobrar.
- Facilita el registro de Notas débito y Crédito
- Hace interfaz con el módulo de Contabilidad.

7.7.2. MÓDULO DE CONTABILIDAD

Figura 4. Módulo de contabilidad Aplicación Krystalos



Fuente: Aplicación Krystalos

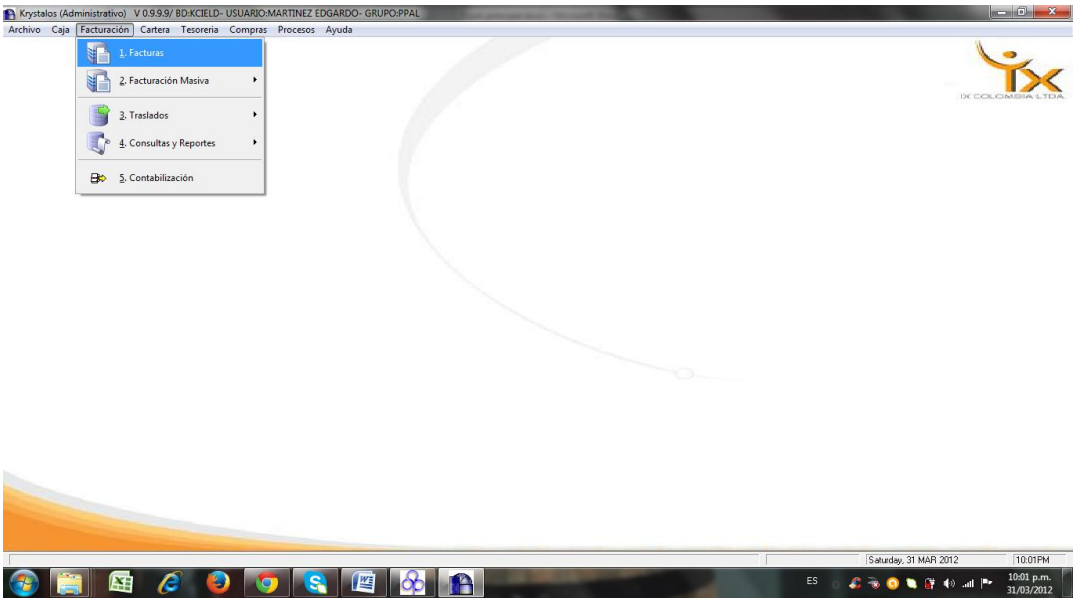
- **Características:** El módulo de *CONTABILIDAD* es el centro de todo el sistema de información, finalmente es a él a quien llegan todos los documentos que se generan desde cualquier otro módulo. Además, se encarga de controlar todos los procesos contables requeridos, cumpliendo con todas las normas legales vigentes hasta la fecha y exigidas por el gobierno para su funcionamiento. Además, tienen como fin la generación rápida de informes financieros y para los entes de control, además de permitir el manejo de los períodos contables abiertos durante todo el año.

Este módulo cuenta con las siguientes características:

- Clases Contables
- Plan de cuentas Parametrizable
- Manejo de Centros de Costos
- Creación de Conceptos de Retención
- Informes Financieros
- Informes de Impuestos
- Generación de Libros Oficiales
- Cierre Anual
- 16 períodos Contables abiertos
- Generación certificados de Retención
- Conciliación de Cuentas
- Consolidación de Empresas

7.7.3. MÓDULO DE FACTURACIÓN

Figura 5. Módulo de Facturación Aplicación Krystalos



Fuente: Aplicación Krystalos

- **Características**

El módulo de *FACTURACIÓN* hace parte del Sistema de KRYSTALOS, el cual permite liquidar los servicios de Salud prestados de acuerdo con la opción escogida (ISS, SOAT o M.U.T). Este proceso se realiza para los pacientes y las EPS.

Este módulo cuenta con las siguientes características:

- Generar Cuentas de Cobro a las entidades Prestadoras de salud.

- Liquidar las facturas por los servicios prestados en accidentes de tránsito.

- Generar automáticamente la partición de cuentas para Aseguradora, FOSYGA, EPS y Paciente

- Facilitar la labor de Auditoría evitando la devolución de las facturas por parte de la EPS.

- Contar con información actualizada sobre los servicios prestados de acuerdo con la contratación.

- Generar información estadística en donde se determinan los valores facturados a la EPS y Pacientes.

- Modificar fácilmente las tarifas de los servicios.

- Generar los archivos planos del decreto 2546 del Ministerio de Salud y Seguridad Social.

- Generar automáticamente los RIPS en cumplimiento al Decreto 3374.

- Realizar la liquidación a varias entidades teniendo como base los servicios cargados al paciente.

- Generación de facturación de servicios captados.

7.7.4. MÓDULO DE HOSPITALIZACIÓN

Figura 6. Módulo de hospitalización Aplicación Krystalos

Fuente: Aplicación Krystalos

• **Características:** El módulo de *HOSPITALIZACIÓN* hace parte del Sistema de Información *KRYSTALOS*, el cual permite controlar la asignación de camas a los pacientes que han ingresado por hospitalización, como también generar informes estadísticos para la toma de decisiones. Este módulo cuenta con las siguientes características:

• Permite conocer el estado actual de ocupación de las camas.

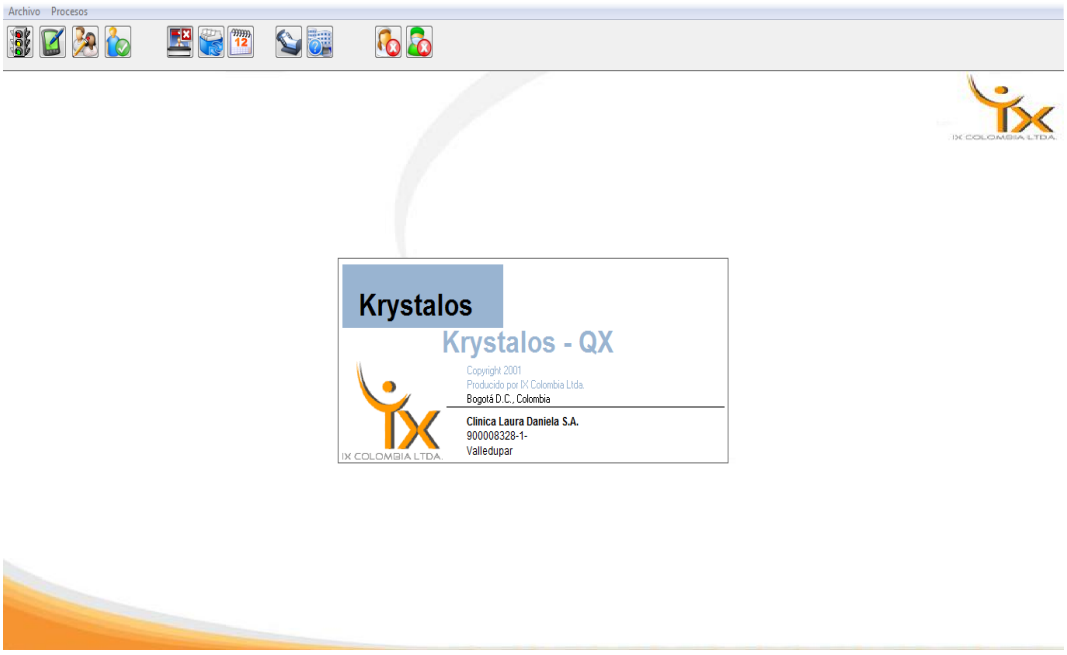
• Permite establecer la frecuencia de pacientes en el área de Hospitalización, de acuerdo con la EPS.

• Permite realizar traslado de camas a pacientes y registro de egreso.

• Brinda disponibilidad de la situación de las camas. Ya sea que estén ocupadas o desocupadas.

7.7.5. MÓDULO DE INVENTARIO

Figura 7. Módulo de inventarios Aplicación Krystalos



Fuente: Aplicación Krystalos

- **Características:** El módulo de *INVENTARIOS* permite controlar los ingresos y salidas de mercancías por cualquier concepto, además permite establecer estadísticas, costos, rentabilidad y movimientos de cada uno de los productos.

Este módulo cuenta con las siguientes características:

- Registro de consumo directo desde las farmacias a las hojas de Trabajo de los pacientes.

- Interface directa con Facturación.

- Manejo de Proveedores por Producto.

- Registro e impresión de ingresos por compra de mercancías a partir de la generación de un pedido, afectando automáticamente cuentas por pagar.

- Listados generales de grupos y subgrupos de productos y Proveedores.

- Listado de Inventario de productos.

- Listado de Productos devueltos.

- Movimiento de inventarios por conceptos varios.

- Control de Almacenes y/o Bodegas.

- Listado de alertas para productos con stock mínimos o máximos.

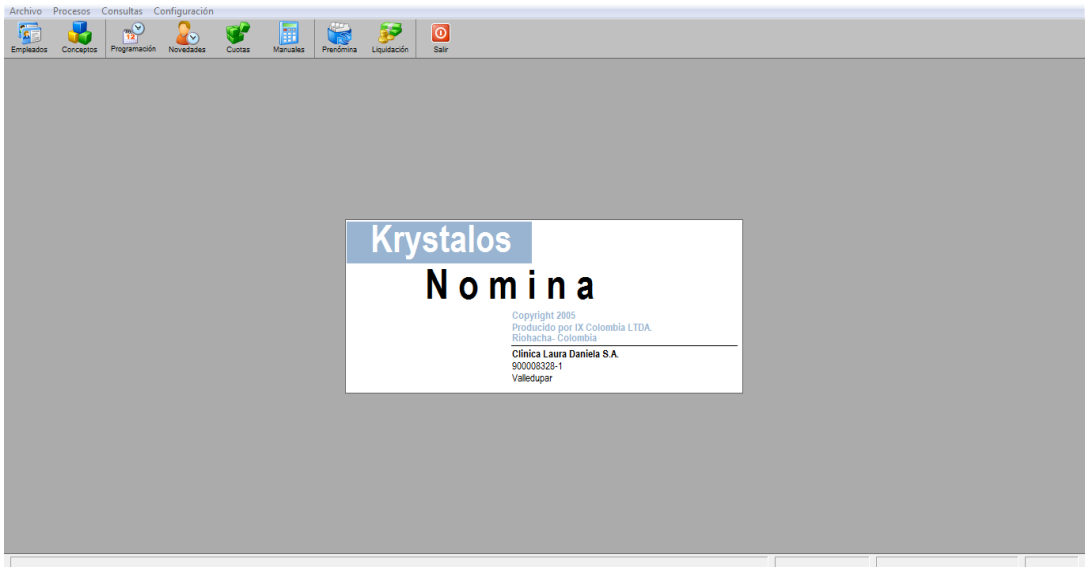
- Manejo de fracciones en los productos, permitiendo trabajar con diferentes unidades de medida.

- Ajustes por inflación.

- Interfaz con el módulo de Presupuestos.

7.7.6. MÓDULO DE NOMINA – TALENTO HUMANO

Figura 8. Módulo de Nómina - talento humano Aplicación Krystalos



Fuente: Aplicación Krystalos

- **Características**

El módulo de *NÓMINA - TALENTO HUMANO* se ajusta a los manejos de Convenciones y liquidaciones especiales de las instituciones por ser un módulo parametrizable y con la posibilidad de definir fórmulas para la liquidación de conceptos.

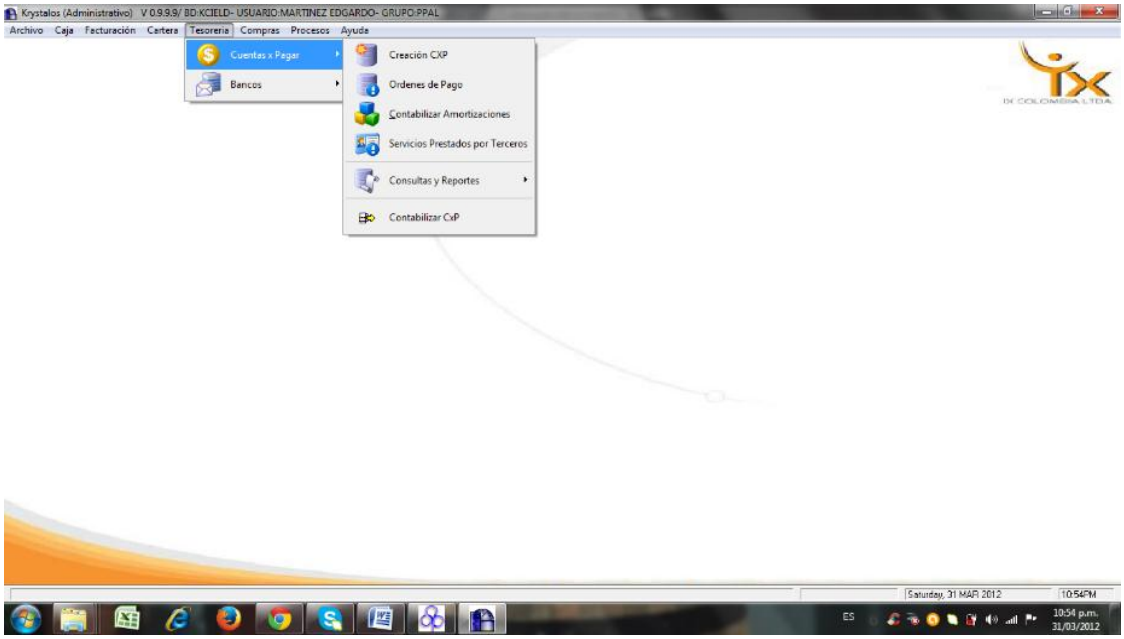
Este módulo cuenta con las siguientes características:

- Manejo de la hoja de vida del empleado
- Facilidad de definir las especificaciones para la liquidación de fórmulas
- Manejo de conceptos de Nómina independientes por grupos
- Facilidad de ingreso de las novedades de Nómina
- Liquidación automática de conceptos de Nómina

- Manejo de Diferentes Fondos de Pensión, Salud etc.
- Generación de Archivos Planos para la Dispersión de Fondos.
- Generación de Cheques para el pago de Nómina
- Generación de la Autoliquidación
- Manejo de Archivos Planos de Autoliquidación
- Liquidación de Licencias e Incapacidades
- Liquidación de Vacaciones
- Manejo y control de Préstamos a Empleados
- Liquidación de todos los valores que se pagan y descuentan a los empleados mensualmente.

7.7.7. MÓDULO DE TESORERÍA

Figura 9. Módulo de tesorería Aplicación Krystalos



Fuente: Aplicación Krystalos

- **Características:** El módulo de *TESORERÍA* permite mantener el control de los fondos financieros de la Compañía o Institución, respetando las normas y resoluciones establecidas por los entes de Control y permitiendo un manejo transparente de la gestión de los funcionarios. Además tiene como fin facilitar el control de los ingresos y egresos, permitiendo un rápido arqueo y control de dineros, mantienen los registros de asientos bancarios al día y permite la generación de informes que facilitan la gestión de los Tesoreros.

Este módulo cuenta con las siguientes características:

- Permite el manejo de diferentes cajas para el recibo de dinero.
- Establece el usuario que recibe y entrega dineros
- Listados de Recibos de Caja y Comprobantes de Egreso por conceptos.
- Impresión de Comprobantes de egreso en formatos personalizados.
- Elaboración de Cheques.
- Consignaciones Bancarias.
- Manejo de Notas Bancarias.
- Informes de Consignaciones y Traslados
- Cruces entre CxC Vs CxP
- Manejo independiente de diferentes Cajas.
- Manejo de Rembolsos.
- Manejo y Control de las inversiones de la entidad.

7.8. PRUEBAS DE AUDITORIA APLICADAS

7.8.1. Pruebas de penetración (PENTESTING). De acuerdo con el informe de las empresas de servicios de pruebas de seguridad informática, hoy en día los ataques cibernéticos se producen no sólo en empresas grandes sino también en PYMES. La seguridad informática es muy fundamental, ya que la pérdida o el robo de datos confidenciales es un riesgo que una empresa, por pequeña que sea, no se puede permitir. Existen datos estadísticos, avalados por empresa de pentesting; que dan cuenta que estos casos ocurren con mayor frecuencia en empresas pequeñas, en dónde la seguridad informática es mínima.

Para estar protegido ante cualquier riesgo informático, una empresa tiene dos alternativas, la primera alternativa es tomar la ayuda de expertos de los servicios de pruebas de seguridad informática y hacer las pruebas de auditoría informática para detectar y solucionar los riesgos o capacitar su equipo de TI.

Las pruebas de auditoría informática usualmente se clasifican en tres clases: pruebas de auditoría informática física, pruebas de auditoría informática lógica o técnica y pruebas de auditoría informática administrativa. Según los expertos de servicios de pruebas de seguridad informática de software (pruebas de penetración), para que sean efectivas, éstas deben estar integradas en una arquitectura de seguridad informática, la cual debe ser conforme con los objetivos empresariales y las posibles vulnerabilidades de acuerdo al impacto que éstas tengan en la empresa.

La auditoría informática conlleva a la implementación de metodologías y pruebas de seguridad informática en todo el entorno de la organización para lo cual se debe considerar los siguientes pasos:

1. Definir los activos informáticos.

2. Identificar las vulnerabilidades.

3. Establecer las probabilidades de la ocurrencia de las vulnerabilidades.

4. Calcular el impacto y la prioridad de cada vulnerabilidad detectada.

5. Documentar los detalles, impactos, prioridades de las vulnerabilidades informáticas.

Para el desarrollo de los anteriores pasos se implementará la metodología de análisis y gestión de riesgos MAGERIT, la cual nos brinda una forma eficiente de gestionar los riesgos y amenazas de cada activo de información, así como el impacto generado por cada uno de ellos ante un eventual ataque. Seguidamente se aplicarán las pruebas o análisis de vulnerabilidades al sitio web de la clínica. Estas pruebas se dividirán en pruebas sustantivas y pruebas de penetración.

El objetivo de las pruebas sustantivas es obtener evidencia suficiente que permita al auditor emitir su juicio en las conclusiones acerca de cuándo pueden ocurrir incidentes o pérdida de información. Se suelen obtener mediante observación,

cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones.

En el desarrollo de la auditoria de seguridad llevada a cabo en la clínica integral Laura Daniela se realizarán las pruebas sustantivas y las pruebas de penetración de acuerdo a los permisos obtenidos para tal fin. Como pruebas sustantivas se aplicarán cuestionarios, entrevistas y visitas de observación a la sede con el objetivo de determinar las falencias encontradas por el personal que maneja directamente los sistemas de información, así como obtener las evidencias de las instalaciones físicas (Cableado, e infraestructura física).

Dentro de las pruebas de penetración se hará uso de varias herramientas a nivel de software como lo son: Vega Vulnerability Scanner y NMAP Security Scanner

8. ANÁLISIS DE CONTROLES

8.1. OPORTUNIDADES DE MEJORAS

R001 Falta de Filtros y Consultas Detalladas

Aunque la aplicación Krystalos ofrece una gran cantidad de alternativas que facilitan la realización de consultas en los diferentes módulos del software; existen formularios donde se hace necesario establecer filtros que posibiliten al usuario realizar búsquedas y consultas detalladas debido a la gran cantidad de registros manejados; a los cuales resulta complicado el acceso por parte del usuario, hasta el punto de realizar prácticamente búsquedas manuales, lo cual implica falencias en el momento de obtener eficiencia y oportunidad en los procesos informáticos.

R002 Limitaciones en la Trazabilidad de Documentos

Debido a que la gran mayoría de los procesos dentro de la Clínica Laura Daniela están sistematizados, el envío de documentación automatizada entre los usuarios que manejan la aplicación Krystalos, sirven para soportar con detalle cada una de las eventualidades realizadas en la institución, generando así, mayor rapidez y eficiencia en el intercambio de información. En contraste a esto, Krystalos no genera las notificaciones suficientes para la argumentación de procesos, puesto que solamente registra la información de los documentos que se comparten en tres áreas específicas: facturación, cartera y auditoría, razón por la cual, no se puede hacer una trazabilidad completa de un documento.

R003 Deficiencias en el Registro de los Costos

Debido a la constante utilización de insumos y medicamentos en las distintas áreas de operación médica que existen dentro de La Clínica Laura Daniela, se hace necesario obtener información puntual acerca de los elementos utilizados en cada sección, con el objeto de justificar los costos que presenta cada área en un periodo determinado o durante un proceso determinado.

La aplicación Krystalos genera información inconsistente, puesto que el registro de los costos está supeditado a la parametrización de la ubicación Computador en el que se registren los datos, es decir, no se puede registrar información diferente a

los correspondientes a la ubicación física del computador, pasando por alto el principio de la universalidad y accesibilidad de la información, dificultando a los usuarios, obtener reportes detallados que permitan someter a evaluación los costos presentados en cada área, y de esta manera realizar una adecuada toma de decisiones por parte de las Áreas de Contabilidad y Administración

R004 Falencias en el Proceso de Devoluciones en Compras

La aplicación Krystalos no genera un registro automatizado de las devoluciones en las compras realizadas por la entidad, en los módulos de Contabilidad y Cuentas por Pagar, tal como sucede con los otros tipos de movimientos de inventario, la salida de pacientes, el despacho de insumos y la compra de medicamentos; imposibilitando de esta manera, obtener información integral en el momento de generar los reportes que describan los compromisos de pagos.

R005 Inconsistencias en el Manejo de Kárdex

El manejo de Kárdex por parte de la aplicación Krystalos es deficiente en el momento de generar reportes que describan la entrada y salida de productos en inventario, donde los saldos de inventarios en el sistema no reflejan con veracidad la información, puesto que éstos no corresponden a los saldos en físico.

R006 Problemas con la Información del Censo de Pacientes

El censo es una de las herramientas más importantes para el control de pacientes dentro de una clínica. Es utilizada por las áreas misionales como enfermería, coordinación médica, auditoria y las áreas de apoyo como: laboratorio, rayos x, farmacia, incluso portería y vigilancia; por tal razón, este proceso debe arrojar información confiable y veras.

Krystalos presenta falencias en el reporte de esta información, causada por dos procesos diferentes; 1 el traslado interno de pacientes y 2 el egreso o alta emitida desde el área de admisión cuando esta no ha sido registrada por el médico.

R007 Falta de Actualización en Cambios Generados desde Contabilidad

Luego de haber registrado una cuenta, producto de una operación contable realizada por la empresa, los otros módulos alimentan la información existente en el área de contabilidad. Al realizar modificaciones desde el área contable, estos

cambios no son reflejados en los demás módulos, dejando áreas sin reflejar los cambios generados y registrados por Contabilidad.

R008 Dificultad para Reversar Procesos de Registro de Compras

Luego de haber registrado una compra de inventario, el usuario no tiene la posibilidad de reversar este proceso en caso de haberse equivocado, y solamente un usuario administrador con acceso a la base de datos puede hacer las correcciones necesarias.

8.2. DESCRIPCION DE CONTROLES EXISTENTES

CE01 Contraseñas Individuales por cada Usuario

El Programa Krystalos asigna inicialmente a cada usuario una contraseña encriptada, la cual, no puede ser posteriormente des encriptada ni por la misma aplicación, dejando solamente al usuario administrador la facultad de cambiar y reasignar las contraseñas.

CE02 Cambios de Contraseñas Periódicamente

Después de asignar por primera vez la contraseña a cada usuario, el programa genera un tiempo de vigencia para esta clave, y luego de transcurrido este intervalo, queda inhabilitada y exige al usuario el cambio de contraseña.

CE03 Manejo de Roles y Privilegios

La aplicación Krystalos permite al administrador de la base de datos la habilitación e inhabilidad de los módulos en forma parcial o total. Esto permite mayor seguridad y control de la información, puesto que cada usuario solamente podrá tener acceso a los datos y formularios necesarios para el adecuado ejercicio de sus labores.

CE04 Control de Acceso a Reportes

Aunque el Programa Krystalos permite a cada usuario acceder a los módulos necesarios para la ejecución de sus labores, existe un control en la generación de reportes, que solamente habilita la información necesaria para llevar a cabo los

procesos involucrados con cada área en específico, impidiendo de ésta manera, que los usuarios accedan a través de reportes a información correspondiente a otras áreas

CE05 Restricción para Modificar Información Registrada

Los registros realizados en la mayoría de los módulos que hacen parte de la aplicación Krystalos solo pueden ser modificados o corregidos por el usuario que llevó a cabo el registro de la información, con la excepción, solamente de la presencia de un súper usuario, que solo puede ser determinado por el administrador de la base de Datos.

CE06 Control en el Acceso y Modificación de Historias Clínicas

Después de haber sido registrada una nota médica, por parte de un médico, de tal manera que alimente la historia clínica de un paciente, esta no puede ser modificada o eliminada por otro galeno, el cual simplemente tiene acceso a esta información para lectura y no para modificación.

CE07 Control de Acceso por Equipos

Todos los equipos utilizados para acceder a la información que maneja la aplicación Krystalos, deben estar registrado en la base de Datos del Programa, de tal manera, que se ejerce un filtro que controla el acceso por equipos, independientemente de que tengan o no, instalada la aplicación.

CE08 Control de Acceso por versión

La aplicación Krystalos verifica que cada equipo donde se ejecute la aplicación tenga la versión que coincida con la que se encuentra instalada en el servidor, para que cualquier acción o novedad sea realizada bajo las pautas actuales de la entidad. Si no corresponden las versiones, la aplicación impide que se establezca la conexión con la base de datos.

CE09 Copias de Respaldo

Al momento de realizar la instalación de la aplicación Krystalos, entra en ejecución una herramienta adicional independiente, cuya función es la de crear

constantemente copias seguridad de la base de datos al transcurrir un determinado intervalo de tiempo, almacenando toda esta información en un disco externo.

CE10 Verificación de Documentos Contables

La aplicación Krystalos verifica los documentos contables que llegan al departamento de contabilidad proveniente de otros módulos, de tal manera, que no presenten errores en su contenido; y en el caso de que contengan fallas, son ubicados automáticamente en otra ventana del módulo para su respectiva corrección.

CE11 Definición de Perfiles y Roles para cada Usuario

A partir de los roles establecidos en el perfil de cada usuario, la aplicación Krystalos define los permisos a asignar, y las actividades que éste puede realizar. Es decir, un usuario con perfil de enfermera no puede realizar notas médicas, aunque tenga los permisos necesarios, debido a que su área de acción no involucra esta actividad.

8.3. DESCRIPCIÓN DE CONTROLES PROPUESTOS

CP01 Control de Acceso por Tiempos

En las áreas de Caja y Facturación, donde hay cargos de actividad continua, que son desarrollados por turnos y manejan flujo constante de dinero; debería existir un control que permita a cada usuario el acceso al equipo, solamente durante un tiempo determinado y de acuerdo a los turnos establecidos, obteniendo de esta manera mayor confidencialidad y seguridad en los procesos.

CP02 Temporizador Configurable para Acceso a Cambios en la Información Digitada por un Usuario del Área Asistencial

Se hace necesario la implementación de un temporizador en el área asistencial, que regule los procedimientos registrados por los profesionales de la salud involucrados; de tal manera, que los médicos y enfermeras tengan un tiempo establecido para agregar o cambiar información de su propio registro, logrando de esta manera mayor eficiencia y oportunidad en los procedimientos.

CP03 Control Secuencial de Registros Asistenciales

En continuidad al anterior, es necesario un control que bloquee acciones posteriores al registro de datos en el departamento asistencial. Este bloqueo será puesto en marcha si la información que se desea ingresar coincide con la línea de acción de la información registrada previamente, dejando abierta la posibilidad para que en otras áreas se hagan los registros necesarios. Es decir, el registro medico solamente influye en el bloqueo de la parte médica, sin crear restricciones en la parte de enfermería, y viceversa.

CP04 Validación de los Centros de costos al Momento de Registrar Información

En los centros de costos existentes en la Clínica Laura Daniela, y que corresponden al área asistencial, se hace necesario la implementación de una herramienta que permita la adición de costos con base al registro del área donde se realizaron los procedimientos y el paciente vinculado con éstos, de tal manera, que se pueda obtener información específica y confiable acerca de los costos por área y por paciente.

CP05 Filtro Referencial para el Registro de Compras

En el proceso de registro de las compras realizadas por La Clínica Laura Daniela, se hace necesario la implementación de un filtro comparativo, que inicie con el ingreso al sistema del valor total de la factura, y a partir de éste, tener una referencia que permita detectar mediante comparaciones, errores o inconsistencias en el ingreso de la información; teniendo en cuenta que el usuario puede cometer errores en las cantidades, impuestos y/o valores detallados en cada factura.

CP06 Actualización de los Módulos Origen frente a Cambios Generados en el Área Contable.

Debido a las modificaciones y correcciones que se realizan en el área de Contabilidad a partir de información registrada en otros módulos; se requiere establecer herramientas, que contribuyan a que estos cambios se vean reflejados también, en los módulos de origen; y de esta manera, mantener información consecuente y veraz en el manejo global de la aplicación Krystalos.

CP07 Administración de la Ubicación del Paciente por el Área de Enfermería

Debido a los inconvenientes presentados en el momento de realizar el traslado interno de pacientes en la Clínica Laura Daniela, es importante implementar una herramienta en la aplicación Krystalos, donde se asigne la administración de pacientes directamente al departamento de enfermería, excluyendo de esta manera, al admisionista de la responsabilidad que esto implica; para que cada enfermera realiza el registro del paciente que entra a su área, y solamente ella, puede ingresar al sistema información de su estado.

CP08 Utilización de Tokens USB

Para garantizar que las claves asignadas a cada usuario no sean prestadas a otros dentro de la Clínica Laura Daniela con el objeto de acceder al sistema, y además evitar el phishing o robo de identidad; se hace necesario la implementación de Tokens USB, que son llaves de firmas digitales encriptadas, las cuales emiten una clave distinta cada vez que el usuario desea registrarse, aumentando así, los niveles de seguridad.

8.4. PARAMETRIZACIÓN Y CLASIFICACIÓN

La parametrización y clasificación de los riesgos frente a los controles existentes en la aplicación Krystalos, serán el soporte argumentativo para el desarrollo de los informes finales de auditoría. El objetivo de clasificar cada uno de los riesgos a los cuales se enfrenta ésta aplicación informática durante su ejecución, es detectar cuáles son los más críticos, y verificar si los controles existentes están aplicando o no ante las diferentes riesgos.

8.4.1. Matriz controles vs riesgos. Al finalizar el análisis de los resultados obtenidos a partir de las encuestas y entrevistas realizadas al personal de labores de la Clínica Laura Daniela, se procede a llenar la Matriz de Control vs. Riesgos, donde se evalúa la magnitud de los riesgos existentes frente a cada una de las áreas de la empresa.

Estas dimensiones serán evaluadas de acuerdo a criterios que describan con claridad el impacto generado por cada factor de riesgo; y contribuyan

posteriormente, a orientar los procedimientos de auditoría que se deben emplear. Los riesgos y controles estarán identificados a través de los siguientes códigos:

R001 para el riesgo número 1 y CE01 para el control existente número 1 y así sucesivamente.

En cuanto a los criterios de evaluación para el impacto generado por cada riesgo, tendremos los siguientes:

0. No Aplica

1. Poco fiable

2. Moderadamente confiable

3. Control muy confiable

TABLA 12. Matriz Riesgos - Controles en la Aplicación Krystalos

	CE01	CE02	CE03	CE04	CE05	CE06	CE07	CE08	CE09	CE10	CE11	Σ
R001	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**
R002	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
R003	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**
R004	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
R005	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**
R006	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
R007	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
R008	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Fuente: El Autor

8.4.1.1. Observaciones de Matriz Riesgos vs. Controles. De acuerdo a lo plasmado en la matriz anterior, donde se confrontaron los riesgos y controles existentes durante la ejecución de la aplicación Krystalos, se puede concluir que los riesgos con mayor probabilidad de ocurrencia son los siguientes:

- ***R002 Limitaciones en la Trazabilidad de Documentos***
- ***R004 Falencias en el Proceso de Devoluciones en Compras***
- ***R006 Problemas con la Información del Censo de Pacientes***
- ***R007 Falta de Actualización en Cambios Generados Desde Contabilidad***
- ***R008 Dificultad para Reversar Procesos de Registro de Compras***

Los demás riesgos (R001, R002 Y R005), aunque no presentan la mayor probabilidad de ocurrencia, también requieren mucha atención, puesto que los controles existentes que aplican son poco fiables para la magnitud de las amenazas presentadas por cada uno de éstos.

La información obtenida a partir de esta matriz, donde queda claro el grado de vulnerabilidad que posee la aplicación Krystalos, marcará el punto de partida para el desarrollo del informe final de auditoría, el cual estará argumentado y orientado por los datos reales obtenidos mediante la confrontación de riesgos y controles.

9. ANÁLISIS Y GESTIÓN DE RIESGOS

Las metodologías de análisis y gestión de riesgos son medidas y técnicas orientadas a mejorar los procesos utilizados en el manejo de la información dentro de una organización empresarial, donde se determinan pautas claras acerca del uso adecuado de los recursos informáticos y los mecanismos de prevención a implementar.

Con miras a establecer políticas de seguridad informática, que contribuyan al mejoramiento de los procesos implementados para el manejo de la información dentro de la Clínica Laura Daniela, se hace necesario realizar previamente un análisis de riesgos, que permita plasmar una serie de planteamientos objetivos y puntuales.

9.1. ANÁLISIS DE RIESGOS

Los Riesgos son aquellas eventualidades que surgen como el resultado probable que pueden arrojar las amenazas y vulnerabilidades existentes dentro de cualquier área, imposibilitando de esta manera, la consecución eficiente de objetivos por parte de una entidad.

En lo que se refiere a la tecnología, los riegos representan la posibilidad de pérdida que pueda existir dentro del funcionamiento de un sistema tecnológico o informático, y en el cual se ve expuesta el procesamiento seguro y confiable de los datos procesados. Para el desarrollo de éste, implementaremos las técnicas establecidas en la metodología Magerit 3.0.

9.1.1. Implementación de la metodología MAGERIT. Magerit es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración empresarial, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La puesta en marcha de Magerit en los procesos involucrados con el procesamiento de la información en la Clínica Laura Daniela, contribuirá a mejorar el uso de las

tecnologías de la información, mediante la detección e identificación de los riesgos a los cuales están sometidos los elementos de trabajo, paso que será necesario para la gestión integral de estas amenazas y el diseño de las Políticas de Seguridad.

Magerit permitirá obtener datos aproximados, pero con bases reales; a través de los cuales, se podrá determinar el valor que se encuentra expuesto de cada uno de los elementos que hacen parte del sistema de información, con el objeto de desarrollar herramientas que fortalezcan la seguridad en dichos procesos.

La Metodología Magerit se presenta como una alternativa formal para investigar los riegos que presenta el Sistema de Información en la Clínica Laura Daniela y formular las medidas necesarias que se deben adoptar para controlar estos riesgos.

De esta manera, la estructura operacional que presenta el método Magerit contribuirá a un mejoramiento pleno del Sistema de Información a partir de los datos obtenidos en la investigación. El Modelo de trabajo de Magerit en torno al proceso de análisis de riesgos se encuentra seccionado en 4 bloques, que son:

1. Identificación y valoración de los activos.

2. Identificación de las amenazas asociadas a los activos

3. Identificación de salvaguardas o controles existentes.

4. Estimación del impacto y riesgo al que están sometidos los activos del sistema.

9.1.1.1. Identificación de los Activos (Ver tabla 9, tabla 10, tabla, 11, tabla 12 y tabla 13). Los activos de información son representados por aquellos elementos que contienen o manipulan información dentro de una organización, motivo por el cual, requieren cuidado y protección por parte de la administración.

La Clínica Laura Daniela de la Ciudad de Valledupar posee una cantidad representativa de activos de información, que se encuentran distribuidos estratégicamente en las distintas áreas de trabajo, y los cuales, trabajando de manera coordinada hacen posible los procesos involucrados con la gestión y transmisión de datos dentro de la empresa.

Para más claridad, en cuanto a los activos involucrados en el procesamiento de la información en la Clínica Laura Daniela, los describiremos en las siguientes tablas.

9.1.1.2. Valoración de los Activos. De acuerdo a los procedimientos descritos en la estructura de trabajo de la Metodología Magerit, una vez realizada la identificación de los activos que intervienen en el procesamiento de la información, se realiza la valoración de cada uno de éstos, con el objeto de determinar el nivel puntual de importancia por activo dentro del sistema informático, y de esta manera, poder tener una visión más clara al momento de determinar los niveles de riesgos correspondientes.

Este procedimiento de valoración se realizará cualitativamente, por lo tanto, tendremos como referencia 3 factores de estudio determinados por la Seguridad Informática y los cuales servirán de apoyo en esta investigación, contribuyendo a determinar el nivel de importancia de cada uno de los activos de información. Estos factores son:

1. **Disponibilidad**
2. **Integridad**
3. **Confidencialidad**
4. **Autenticidad**
5. **Trazabilidad**

A través de estos frentes de estudio serán sometidos a evaluación cada uno de los activos descritos anteriormente, los cuales serán agrupados estratégicamente de acuerdo a la ubicación que presentan y la información que manejan. Los Criterios de evaluación son los siguientes:

TABLA 13. Criterios de valoración para Activos de Información

VALOR	CRITERIO	DESCRIPCIÓN
1	Muy Bajo	Irrelevante
2	Bajo	De Menor Importancia
3	Medio	Importante
4	Alto	Altamente Importante
5	Muy Alto	De Vital Importancia

Fuente: Metodología Magerit

Estos serán utilizados para evaluar los 3 aspectos de estudio, y de esta manera, obtener el grado de importancia que presenta cada uno de los activos dentro del sistema de información.

- **Equipos de Cómputo:** La valoración correspondiente a los equipos de cómputo se realizará de acuerdo a los siguientes interrogantes que giran en torno a la disponibilidad, integridad y confidencialidad de los datos manipulados:

Disponibilidad (D): ¿Qué tan importante sería para el Sistema de Información que el computador estuviera disponible?

Integridad (I): ¿Qué importancia tendría para el Sistema de Información que el computador no fuese alterado sin autorización ni control?

Confidencialidad (C): ¿Qué importancia tendría para el Sistema de Información que el acceso al computador solo fuese de manera autorizada?

Autenticidad (A): ¿Qué importancia tendría para el Sistema de Información que origen y el acceso al computador sea legítimo y verificable?

Trazabilidad (T): ¿Qué importancia tendría para el Sistema de Información conocer la trazabilidad de los datos?

Conforme a los criterios e intervalos de evaluación establecidos y los interrogantes planteados, la valoración cualitativa para los computadores existentes en la Clínica Laura Daniela es la siguiente:

TABLA 14. Valoración en Equipos de Cómputo

CODIGO	DESCRIPCION	UBICACIÓN	D	I	C	A	T
CE-01	*MARCA DELL VOSTRO 200 PROCESADOR INTEL CELERON 1.60 GHz, 1GB RAM, DD 80 GB.*	*Admisiones*	*3*	*3*	3	3	3

Fuente: El Autor

- **Valoración de Impresoras**: La valoración correspondiente a las impresoras se realizará de acuerdo a los siguientes interrogantes que giran en torno a la disponibilidad, integridad y confidencialidad:

Disponibilidad (D): ¿Qué tan importante sería para el Sistema de Información que la impresora estuviera disponible?

Integridad (I): ¿Qué importancia tendría para el Sistema de Información que la impresora no fuese alterada sin autorización ni control?

Confidencialidad (C): ¿Qué importancia tendría para el Sistema de Información que el acceso a la impresora solo fuese de manera autorizada?

Autenticidad (A): ¿Qué importancia tendría para el Sistema de Información que el acceso a la impresora solo fuese de manera autorizada?

Trazabilidad (T): ¿Qué importancia tendría para el Sistema de Información conocer la trazabilidad de uso de las impresoras?

Conforme a los criterios e intervalos de evaluación establecidos y los interrogantes planteados, la valoración cualitativa para las impresoras existentes en la Clínica Laura Daniela es la siguiente:

TABLA 15. Valoración en Impresoras

CÓDIGO	DESCRIPCIÓN	UBICACIÓN	D	I	C	A	T
IMP-01	*MARCA KYOCERA KM-3040. MULTIFUNCIONAL*	*Admisiones 2*	*4*	*4*	*4*	*4*	*4*

Fuente: El Autor

- **Valoración de Switchs:** La valoración correspondiente a las switchs se realizará de acuerdo a los siguientes interrogantes que giran en torno a la disponibilidad, integridad y confidencialidad:

Disponibilidad (DISP): ¿Qué tan importante sería para el Sistema de Información que el switch estuviera disponible?

Integridad (INT): ¿Qué importancia tendría para el Sistema de Información que el switch no fuese alterado sin autorización ni control?

Confidencialidad (CONF): ¿Qué importancia tendría para el Sistema de Información que el acceso al switch solo fuese de manera autorizada?

Autenticidad (A): ¿Qué importancia tendría para el Sistema de Información que el acceso a los switch fuese verificable y autorizada?

Trazabilidad (T): ¿Qué importancia tendría para el Sistema de Información conocer quién y cómo accedieron a los switch?

Conforme a los criterios e intervalos de evaluación establecidos y los interrogantes planteados, la valoración cualitativa para los switchs existentes en la Clínica Laura Daniela es la siguiente:

TABLA 16. Valoración en Switchs

CODIGO	DESCRIPCIÓN	UBICACIÓN	D	I	C	A	T
SW-01	*MARCA DLINK 8 PUERTOS DES-1008A COLOR NEGRO.*	*Admisiones 3*	*5*	*5*	5	5	5

Fuente: El Autor

- **Valoración de Routers:** La valoración correspondiente a las routers se realizará de acuerdo a los siguientes interrogantes que giran en torno a la disponibilidad, integridad y confidencialidad:

Disponibilidad (DISP): ¿Qué tan importante sería para el Sistema de Información que el router estuviera disponible?

Integridad (INT): ¿Qué importancia tendría para el Sistema de Información que el router no fuese alterado sin autorización ni control?

Confidencialidad (CONF): ¿Qué importancia tendría para el Sistema de Información que el acceso al router solo fuese de manera autorizada?

Autenticidad (A): ¿Qué importancia tendría para el Sistema de Información que el acceso a los router solo fuese de manera verificada y autorizada?

Trazabilidad (T): ¿Qué importancia tendría para el Sistema de Información conocer la trazabilidad en el tráfico de la información?

Conforme a los criterios e intervalos de evaluación establecidos y los interrogantes planteados, la valoración cualitativa para los Routers existentes en la Clínica Laura Daniela es la siguiente:

TABLA 17. Valoración en Routers

CODIGO	DESCRIPCIÓN	UBICACIÓN	D	I	C	A	T
ROU-01	*MARCA LINKSYS WRT320N 4 PUERTOS COLOR NEGRO*	*Cirugía 2*	*3*	*3*	**3**	**3**	**3**

Fuente: El Autor

- **Valoración de Servidores:** La valoración correspondiente a los servidores se realizará de acuerdo a los siguientes interrogantes que giran en torno a la disponibilidad, integridad y confidencialidad:

Disponibilidad (DISP): ¿Qué tan importante sería para el Sistema de Información que el servidor estuviera disponible?

Integridad (INT): ¿Qué importancia tendría para el Sistema de Información que el servidor no fuese alterado sin autorización ni control?

Confidencialidad (CONF): ¿Qué importancia tendría para el Sistema de Información que el acceso al servidor solo fuese de manera autorizada?

Autenticidad (A): ¿Qué importancia tendría para el Sistema de Información que el acceso a los servidores solo fuese de manera autenticada?

Trazabilidad (T): ¿Qué importancia tendría para el Sistema de Información conocer la trazabilidad en el acceso a los servidores?

Conforme a los criterios e intervalos de evaluación establecidos y los interrogantes planteados, la valoración cualitativa para los servidores existentes en la Clínica Laura Daniela es la siguiente:

TABLA 18. Valoración en Servidores

CODIGO	DESCRIPCION	UBICACIÓN	D	I	C	A	T
SER-01	*CPU IMÁGENES RX HP P5700 SERVIDOR.*	*Sistemas*	*5*	*5*	5	5	5

Fuente: El Autor

9.1.1.3. Identificación de Amenazas. Una amenaza en un Sistema informático representa un evento que puede generar incidentes negativos dentro de la organización hasta el punto de causar daños y pérdidas en los activos involucrados con la información; afectando directamente las actividades de almacenamiento, transmisión y procesamiento de datos.

En la Clínica Laura Daniela, existen distintos factores que pueden convertirse en determinado momento en eventualidades que afectan significativamente el funcionamiento del Sistema Informático; por tal razón, es necesaria la atención y el control por parte del área de Sistemas. Entre las amenazas más relevantes dentro de la Clínica Laura Daniela están las siguientes:

TABLA 19. Identificación de Amenazas

AMENAZA	DESCRIPCIÓN
Manipulación de la Configuración	Es un riesgo que se presenta y ésta relacionado con tareas del administrador como son: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento.
Suplantación de la Identidad del Usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.
Abuso de privilegio de Acceso	Ocurre cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia.
Uso no Previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal (juegos, consultas personales en Internet, almacenamiento de datos personales, etc.).

AMENAZA	DESCRIPCIÓN
Difusión de Software Dañino	Consiste en la propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
Acceso no Autorizado	Sucede cuando el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
Intercepción de la Información	Ocurre cuando el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
Modificación de la Información	Corresponde a la alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
Corrupción de la Información	Es la degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
Destrucción de la Información	Es la eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
Divulgación de la Información	Revelación de información.
Ataque Destructivo	Vandalismo, terrorismo acción militar
Indisponibilidad del Personal	Ausencia deliberada del puesto de trabajo, como: huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.

Fuente: Metodología Magerit, adaptada por el Autor

9.1.1.4. Valoración de las Amenazas. Para conocer o dimensionar el alcance que puede tener una amenaza dentro del Sistema de información se hace necesario realizar la respectiva valoración de éstas; y luego establecer la *probabilidad de ocurrencia* y el *nivel de degradación* en función de los activos que se ven involucrados al momento de materializarse el ataque. La Valoración de estos 2 factores se realizará con base los siguientes criterios:

- **Nivel de Degradación**

TABLA 20. Criterios de valoración – Nivel de Degradación

VALOR	NIVEL DE DEGRADACIÓN	OCURRENCIA
1	MUY BAJO (MB)	El activo no sufre daños relevantes.
2	BAJO (B)	El activo sufre daños, pero puedes seguir operando.
3	MODERADO (M)	El activo sufre daños y queda restringida su operación
4	ALTO (A)	El activo sufre daños que impiden su trabajo, pero que pueden recuperarse para continuar operando.
5	MUY ALTO (MA)	El activo sufre daños irreparables y la operación se ve afectada más allá de lo tolerable.

Fuente: Metodología Magerit

- **Probabilidad de Ocurrencia**

TABLA 21. Criterios de valoración – Probabilidad de Ocurrencia

VALOR	FRECUENCIA	PROBABILIDAD DE OCURRENCIA
1	MUY POCO FRECUENTE (MPF)	0-20%
2	POCO FRECUENTE (PF)	20-40%
3	NORMAL (N)	40-60%
4	FRECUENTE (F)	60-80%
5	MUY FRECUENTE (MF)	80-100%

Fuente: Metodología Magerit

En la Clínica Laura Daniela, todos los equipos que hacen parte del Sistema de Información" Krystalos", están organizados por áreas; donde a cada usuario se le asignan privilegios de acceso y manipulación de su entera competencia; razón por la cual, el riesgo existente en cada equipo depende del tipo de información que maneje y su ubicación de trabajo.

Siguiendo los lineamientos del método, realizaremos la valoración de las amenazas en función de los activos involucrados con la información procesada por la aplicación en estudio.

TABLA 22. Identificación de Amenazas

ACTIVO	AMENAZAS	FRECUENCIA	IMPACTO					RIESGO				
			D	I	C	A	T	D	I	C	A	T
DATOS / INFORMACION	Errores de los usuarios	4	5	5	5	5	5	20	20	20	20	20
	Escapes de información	4	5	5	5	5	5	20	20	20	20	20
	Alteración de la información	4	5	5	5	5	5	20	20	20	20	20
	Destrucción de información	4	5	5	5	5	5	20	20	20	20	20
	Acceso no autorizado	4	5	5	5	5	5	20	20	20	20	20
	Modificación de la información	4	5	5	5	5	5	20	20	20	20	20
SERVICIOS [PORTAL WEB]	Errores de los usuarios	2	3	3	3	3	3	6	6	6	6	6
	Escapes de información	2	3	3	3	3	3	6	6	6	6	6
	Alteración de la información	2	3	3	3	3	3	6	6	6	6	6
	Destrucción de información	2	3	3	3	3	3	6	6	6	6	6
	Acceso no autorizado	2	3	3	3	3	3	6	6	6	6	6
	Modificación de la información	2	3	3	3	3	3	6	6	6	6	6

TABLA 22. (Continuación)

ACTIVO	AMENAZAS	FRECUENCIA	IMPACTO					RIESGO				
			D	I	C	A	T	D	I	C	A	T
APLICACIONES	Errores de los usuarios	4	4	4	4	4		16	16	16	16	0
	Escapes de información	4	4	4	4	4		16	16	16	16	0
	Alteración de la información	4	4	4	4	4		16	16	16	16	0
	Destrucción de información	4	4	4	4	4		16	16	16	16	0
	Acceso no autorizado	4	4	4	4	4		16	16	16	16	0
	Modificación de la información	4	4	4	4	4		16	16	16	16	0
EQUIPAMIENTO INFORMATICO [HARDWARE]	Errores de los usuarios	4	5	5	5			20	20	20	0	0
	Escapes de información	4	5	5	5			20	20	20	0	0
	Alteración de la información	4	5	5	5			20	20	20	0	0
	Destrucción de información	4	5	5	5			20	20	20	0	0
	Acceso no autorizado	4	5	5	5			20	20	20	0	0
	Modificación de la información	4	5	5	5			20	20	20	0	0
REDES DE COMUNICACIONES	Errores de los usuarios	4	5	5	5			20	20	20	0	0
	Escapes de información	4	5	5	5			20	20	20	0	0
	Alteración de la información	4	5	5	5			20	20	20	0	0
	Destrucción de información	4	5	5	5			20	20	20	0	0
	Acceso no autorizado	4	5	5	5			20	20	20	0	0
	Modificación de la información	4	5	5	5			20	20	20	0	0
EQUIPAMIENTO AUXILIAR	Errores de los usuarios	1	3	3	3			3	3	3	0	0
	Escapes de información	1	3	3	3			3	3	3	0	0
	Alteración de la información	1	3	3	3			3	3	3	0	0
	Destrucción de información	1	3	3	3			3	3	3	0	0
	Acceso no autorizado	1	3	3	3			3	3	3	0	0
	Modificación de la información	1	3	3	3			3	3	3	0	0
INSTALACIONES	Errores de los usuarios	1	4	4	2			4	4	2	0	0
	Escapes de información	1	4	4	2			4	4	2	0	0
	Alteración de la información	1	4	4	2			4	4	2	0	0
	Destrucción de información	1	4	4	2			4	4	2	0	0
	Acceso no autorizado	1	4	4	2			4	4	2	0	0
	Modificación de la información	1	4	4	2			4	4	2	0	0
PERSONAL	Errores de los usuarios	1	5	5	5	5	5	5	5	5	5	5
	Escapes de información	1	5	5	5	5	5	5	5	5	5	5
	Alteración de la información	1	5	5	5	5	5	5	5	5	5	5
	Destrucción de información	1	5	5	5	5	5	5	5	5	5	5
	Acceso no autorizado	1	5	5	5	5	5	5	5	5	5	5
	Modificación de la información	1	5	5	5	5	5	5	5	5	5	5

Fuente: El Autor

9.1.1.5. Identificación de Salvaguardas. Teniendo en cuenta el riesgo que existe en un sistema de información a raíz de las distintas amenazas contempladas durante la ejecución de los procesos informáticos, podemos definir las salvaguardas como las medidas o procedimientos empleados para reducir las probabilidades de que estas amenazas se materialicen, y generen daños potenciales en la información.

Por ser la Clínica Laura Daniela, una institución de salud que maneja una gran cantidad de datos a través de la aplicación Krystalos, existen salvaguardas que han sido diseñados e implementados para minimizar el riesgo, y de esta manera reducir la probabilidad de ocurrencia de las acciones que puedan causar daños o alteraciones en el procesamiento de la información.

Con base al listado general de salvaguardas presentadas en la documentación de la Metodología Magerit; en la Clínica Laura Daniela se cuenta con las siguientes:

TABLA 23. Identificación y Descripción de Salvaguardas

SALVAGUARDA	DESCRIPCIÓN
Identificación y Autenticación	Este servicio constituye la primera línea de defensa para el sistema, previniendo el ingreso de usuarios no autorizados.
Gestión de Incidencias	Esta permite hacer frente a los eventos que comprometen la seguridad del sistema (confidencialidad, integridad o disponibilidad).
Segregación de Tareas	Entra en desarrollo a través de los privilegios y roles asignados a los usuarios involucrados con la información manejada dentro del sistema.
Herramienta Contra Código Dañino	Son medidas que se adoptan para prevenir infecciones que alteren el procesamiento adecuado de la información.
Detección y Prevención de Intrusos	Su función es detectar las actividades maliciosas en la red, crear un archivo log y tratar de bloquear estos procesos.
Copias de Seguridad (Backup)	Implica la creación de Copias de respaldo de la información frente a posibles eventualidades.
Aseguramiento de la Integridad	Abarca las diferentes medidas que se toman para garantizar la calidad de la información procesada.
Cifrado de la Información	Permite aumentar la seguridad de la información mediante la codificación del contenido.
Aseguramiento de la Disponibilidad	Garantiza que los servicios que intervienen en el sistema estén disponibles cuando los requiera el usuario.
Aplicación de Perfiles de Seguridad	Control y asignación de los permisos estrictamente necesarios por parte del usuario.

TABLA 23. (Continuación)

SALVAGUARDA	DESCRIPCIÓN
Gestión de Cambios	Hace referencia a las actualizaciones y mejoras implementadas dentro del sistema informático.
Protección de Aplicaciones Web	Este control abarca de los aplicativos que manejan entorno web durante su ejecución.
Protección del Correo Electrónico	Hace referencia a los controles establecidos para los correos electrónicos institucionales.
Protección de los Equipos de Frontera	Abarca el control de equipos específicos en las comunicaciones del sistema como: switchs, Routers, modem, etc.

Fuente: Metodología Magerit

9.1.1.6. Valoración de Salvaguardas. Para determinar el alcance de los controles existentes dentro de la Clínica Laura Daniela, es necesario realizar una valoración objetiva que permita establecer la eficacia de éstos frente a las amenazas que ponen en riesgo los procesos del Sistema informático.

La Valoración de las salvaguardas se realizará con miras a estimar el impacto y el riesgo dentro del sistema informático. Esta valoración la realizaremos con base a los siguientes criterios:

Tabla 24. Criterios de Valoración para Salvaguardas

CUALIFICACIÓN (NIVEL DE PROTECCIÓN)	EFICIENCIA	MARGINALIDAD
Muy Bajo	10%	0.9
Bajo	30%	0.7
Moderado	50%	0.5
Alto	70%	0.3
Muy Alto	90%	0.1

Fuente: Metodología Magerit

Al realizar un estudio en las distintas áreas involucradas en el procesamiento de la información y partiendo de la definición cualitativa expuesta, la tabla que describe el alcance de las salvaguardas implementadas frente a las amenazas existentes es la siguiente:

Cuadro 2. Nivel de Protección de Salvaguardas por Áreas

SALVAGUARDA	ÁREAS PROTEGIDAS	NIVEL DE PROTECCIÓN
Identificación y Autenticación	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Sistemas • Subgerencia • Telemática • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	Muy alto
Gestión de Incidencias	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía	Alto

SALVAGUARDA	ÁREAS PROTEGIDAS	NIVEL DE PROTECCIÓN
	• Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Sistemas • Subgerencia • Telemática • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	
Segregación de Tareas	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana	Alto

SALVAGUARDA	ÁREAS PROTEGIDAS	NIVEL DE PROTECCIÓN
	• Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Sistemas • Subgerencia • Telemática • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	
Herramienta contra Código Dañino	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Sistemas • Subgerencia • Telemática • Terapia Física	Alto

SALVAGUARDA	ÁREAS PROTEGIDAS	NIVEL DE PROTECCIÓN
	• Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	
Detección y Prevención de Intrusos	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Sistemas • Subgerencia • Telemática • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	Moderado
Copias de Seguridad (Backup)	• Sistemas • Telemática • Laboratorio	Muy alto
	• Consultorios • Consultorios Ginecología	Moderada

SALVAGUARDA	ÁREAS PROTEGIDAS	NIVEL DE PROTECCIÓN
	• Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Observación • Rips • Siau • Subgerencia • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	
Aseguramiento de la Integridad	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips	Alto

SALVAGUARDA	ÁREAS PROTEGIDAS	NIVEL DE PROTECCIÓN
	• Siau • Sistemas • Subgerencia • Telemática • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	
Cifrado de la Información	• sistemas	Muy alto
	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Subgerencia • Telemática • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal	Moderado

SALVAGUARDA	ÁREAS PROTEGIDAS	NIVEL DE PROTECCIÓN
	• Uci Pediátrica	
Aseguramiento de la Disponibilidad	• Sistemas	Muy alto
	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Sistemas • Subgerencia • Telemática • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	alto
Aplicación de Perfiles de Seguridad	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera	Muy alto

SALVAGUARDA	ÁREAS PROTEGIDAS	NIVEL DE PROTECCIÓN
	• Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Sistemas • Subgerencia • Telemática • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	
Gestión de Cambios	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia	Moderado

SALVAGUARDA	ÁREAS PROTEGIDAS	NIVEL DE PROTECCIÓN
	• Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Sistemas • Subgerencia • Telemática • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	
Protección de Aplicación de Web	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Sistemas • Subgerencia • Telemática	Alto

SALVAGUARDA	ÁREAS PROTEGIDAS	NIVEL DE PROTECCIÓN
	• Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	
Protección del Correo Electrónico	• Admisiones • Auditoría • Autorizaciones • Biomédicos • Calidad • Cartera • Cirugía • Consultorios • Consultorios Ginecología • Contabilidad • Coordinación Financiera • Correspondencia • Envíos • Facturación • Farmacia • Gerencia • Gestión humana • Ginecobstetricia • Hospitalización • Laboratorio • Observación • Rips • Siau • Sistemas • Subgerencia • Telemática • Terapia Física • Tesorería • Triage • Uci Adultos • Uci Neonatal • Uci Pediátrica	Muy alto
Protección de los Equipos de Frontera	• Sistemas	Alto

9.1.1.7. Determinación del Impacto. En el proceso de análisis y gestión de riesgos informáticos se denomina impacto a la medida del daño sobre el activo, derivado de la materialización de una amenaza. Por esta razón, tomaremos como base la tabla de criterios utilizada para valorar la degradación de los activos, los cuales fueron relacionados en la tabla correspondiente a las amenazas presentes dentro de la Clínica Laura Daniela. La tabla de criterios a utilizar para valorar el impacto que una amenaza genera sobre los activos de información serán los siguientes:

Tabla 25. Criterios de Valoración para Determinar el Impacto de amenazas

VALOR	IMPACTO (DEGRADACIÓN)	OCURRENCIA
1	MUY BAJO (MB)	El activo no sufre daños relevantes.
2	BAJO (B)	El activo sufre daños, pero puedes seguir operando.
3	MODERADO (M)	El activo sufre daños y queda restringida su operación
4	ALTO (A)	El activo sufre daños que impiden su trabajo, pero que pueden recuperarse para continuar operando.
5	MUY ALTO (MB)	El activo sufre daños irreparables y la operación se ve afectada más allá de lo tolerable.

Fuente: Metodología Magerit

9.1.1.8. Estimación del Riesgo. Dentro de un Sistema Informático, se denomina riesgo a la magnitud del daño probable que pueda afectar los activos involucrados en el procesamiento de la información. Por tal motivo, la frecuencia de ocurrencia y el impacto generado por las amenazas, determinarán conjuntamente los riesgos existentes en los procesos informáticos que se llevan a cabo dentro de la Clínica Laura Daniela.

Para realizar la estimación del riesgo de forma cualitativa, se implementará un sencillo proceso matricial, donde se establecerá una relación de los niveles de vulnerabilidad (frecuencia) y los niveles de impacto. Esta técnica nos proporcionará

una escala de medidas lógicas (criterios) que faciliten la interpretación de los resultados obtenidos. Este procedimiento se realizará inicialmente mediante el uso de algunos valores cuantitativos. Las variables a utilizar serán:

- ***En lo que corresponde a la Vulnerabilidad (Frecuencia) tendremos:***

Muy poco frecuente → MPF = 1

Poco Frecuente → PF = 2

Normal → N = 3

Frecuente → F = 4

Muy Frecuente → MF = 5

- ***En lo que corresponde al Impacto tendremos:***

Muy Bajo → MB = 1

Bajo → B = 2

Medio → M = 3

Alto → A = 4

Muy Alto → MA = 5

Con base a los valores asignados, aplicaremos un proceso matricial establecido en la metodología Magerit, donde aplicaremos en cada punto de intersección la fórmula de estimación de riesgo, con el objeto de tener una escala lógica de valores para los activos de información. La fórmula para determinar el riego es la siguiente:

Riesgo = Impacto x Frecuencia

Mediante la implementación de esta, tendremos que la matriz referente para la estimación del riesgo será la siguiente:

Tabla 26. Valoración para Estimación del Riesgo

ESTIMACIÓN DEL RIESGO		VULNERABILIDAD (FRECUENCIA)				
		MPF(1)	*PF(2)*	*N(3)*	*F(4)*	*MF(5)*
IMPACTO	*MA(5)*	5	10	15	20	25
	A(4)	4	8	12	16	20
	M(3)	3	6	9	12	15
	B(2)	2	4	6	8	10
	MB(1)	1	2	3	4	5

Fuente: Metodología Magerit

Donde los tipos de riesgos quedan representados en los siguientes intervalos:

Tabla 27. Rangos de Valoración para la Estimación de Riesgos

CLASE DE RIESGO	VALORACIÓN CUALITATIVA	VALORACIÓN CUANTITATIVA
Crítico	Muy Alto	15 – 25
Grave	Alto	10 – 14
Moderado	Medio	5 – 9
Menor	Bajo	1 – 4

Fuente: Metodología Magerit

Tomando en cuenta estas consideraciones y criterios planteados por la metodología Magerit, se realizará una estimación de riesgo de acuerdo a la recolección de información mediante entrevistas y encuestas realizadas al personal que maneja el sistema de información dentro de la Clínica Laura Daniela. Para esto, aplicaremos la fórmula para determinar el riesgo por amenaza en cada una de las áreas:

Riesgo = Impacto x Frecuencia

Este proceso, se llevará a cabo evaluando las áreas que contienen activos de información, contemplando, además, las salvaguardas o controles existentes hasta el momento:

- ***Área de Admisiones***

Tabla 28. Estimación de Riesgos en el Área de Admisiones

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(MPF x MB = 1 x 1 = 1) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(PF x MB = 2 x 1 = 2) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x M = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x M = 1 x 1 = 1) → Menor
Modificación de la Información	(PF x M = 2 x 3 = 6) → Moderado
Corrupción de la Información	(PF x MB = 2 x 1 = 2) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(PF x MB = 2 x 1 = 2) → Menor
Ataque destructivo	(MPF x MA = 1 x 5 = 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 3 = 3) → Menor

Fuente: El Autor

- ***Área de Auditoría***

Tabla 29. Estimación de Riesgos en el Área de Auditoría

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(MPF x MB = 1 x 1 = 1) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(N x A = 3 x 4 = 12) → Grave
Acceso no Autorizado	(PF x B = 2 x 2 = 4) → Menor
Intercepción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(PF x MB = 2 x 1 = 3) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Menor
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Autorizaciones***

Tabla 30. Estimación de Riesgos en el Área de Autorizaciones

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(PF x M = 2 x 3 = 6) → Moderado
Suplantación de la Identidad del Usuario	(MPF x MB = 1 x 1 = 1) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(PF x A = 2 x 4 = 8) → Moderado
Acceso no Autorizado	(MPF x B = 1 x 2 = 2) → Menor
Intercepción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(PF x A = 2 x 4 = 8) → Moderado
Divulgación de la Información	(PF x MB = 2 x 1 = 2) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Menor
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Biomédicos***

Tabla 31. Estimación de Riesgos en el Área de Biomédicos

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x MB = 1 x 1 = 1) → Menor
Suplantación de la Identidad del Usuario	(MPF x MB = 1 x 1 = 1) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(PF x A = 2 x 4 = 8) → Moderado
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(PF x B = 2 x 2 = 4) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(PF x MB = 2 x 1 = 2) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Menor
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Calidad***

Tabla 32. Estimación de Riesgos en el Área de Calidad

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x MB = 1 x 1 = 1) → Menor
Suplantación de la Identidad del Usuario	(MPF x MB = 1 x 1 = 1) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 2 x 4 = 8) → Moderado
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 2 x 2 = 4) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(MPF x MB = 2 x 1 = 2) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Menor
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Cartera***

Tabla 33. Estimación de Riesgos en el Área de Cartera

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x B = 1 x 2 = 2) → Menor
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x B = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 2 x 2 = 4) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Menor
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Cirugía***

Tabla 34. Estimación de Riesgos en el Área de Cirugía

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x B = 1 x 2 = 2) → Menor
Suplantación de la Identidad del Usuario	(PF x B = 2 x 2 = 4) → Menor
Abuso de Privilegios de Acceso	(MPF x B = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(PF x A = 2 x 4 = 8) → Moderado
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 2 x 2 = 4) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(F x MB = 3 x 1 = 3) → Menor
Ataque destructivo	(PF x A = 2 x 4= 8) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Consultorios***

Tabla 35. Estimación de Riesgos en el Área de Consultorios

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x MB = 1 x 1 = 1) → Menor
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x B = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 2 x 2 = 4) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(PF x A = 2 x 4= 8) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Consultorios Ginecología***

Tabla 36. Estimación de Riesgos en el Área de Consultorios Ginecología

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x MB = 1 x 1 = 1) → Menor
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x B = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 2 x 2 = 4) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Menor
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Contabilidad***

Tabla 37. Estimación de Riesgos en el Área de Contabilidad

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(F x B = 3 x 2 = 6) → Moderado
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x B = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Modificación de la Información	(F x B =3 x 2 = 6) → Moderado
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(PF x MB = 2 x 1 = 2) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Coordinación Financiera***

Tabla 38. Estimación de Riesgos en el Área de Coord. Financiera

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(PF x B = 2 x 2 = 4) → Menor
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x B = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(PF x A = 1 x 4= 4) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Correspondencia***

Tabla 39. Estimación de Riesgos en el Área de Correspondencia

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(PF x M = 2 x 3 = 6) → Moderado
Suplantación de la Identidad del Usuario	(MPF x MB = 1 x 1 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Modificación de la Información	(MPF x M = 1 x 3 = 3) → Menor
Corrupción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x MA = 1 x 5= 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Envíos***

Tabla 40. Estimación de Riesgos en el Área de Envíos

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x B = 1 x 2 = 2) → Menor
Intercepción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Modificación de la Información	(MPF x M = 1 x 3 = 3) → Menor
Corrupción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x MA = 1 X 5= 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Facturación***

Tabla 41. Estimación de Riesgos en el Área de Facturación

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(F x M = 1 x 1 = 1) → Menor
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x B = 1 x 2 = 2) → Menor
Intercepción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Modificación de la Información	(PF x M = 2 x 3 = 6) → Moderado
Corrupción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(PF x MB = 2 x 1 = 2) → Menor
Ataque destructivo	(MPF x MA = 1 x 5 = 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Farmacia***

Tabla 42. Estimación de Riesgos en el Área de Farmacia

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(PF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x B = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 2 x 2 = 4) → Menor
Modificación de la Información	(MPF x M = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x MB = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x A = 1 x 2 = 2) → Menor
Divulgación de la Información	(F x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x MA = 1 x 5= 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Gerencia***

Tabla 43. Estimación de Riesgos en el Área de Gerencia

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(MPF x M = 1 x 3 = 3) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x M = 1 x 3 = 3) → Menor
Intercepción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Modificación de la Información	(MPF x M = 1 x 3 = 3) → Menor
Corrupción de la Información	(MPF x MB = 1 x 3 = 3) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x MA = 1 x 5 = 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Gestión Humana***

Tabla 44. Estimación de Riesgos en el Área de Gestión Humana

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(PF x M = 2 x 3 = 6) → Menor
Suplantación de la Identidad del Usuario	(MPF x M = 1 x 3 = 3) → Menor
Abuso de Privilegios de Acceso	(MPF x B = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x M = 1 x 3 = 3) → Menor
Intercepción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Modificación de la Información	(PF x M = 2 x 3 = 6) → Moderado
Corrupción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x MA = 1 x 5= 8) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Ginecobstetricia***

Tabla 45. Estimación de Riesgos en el Área de Ginecobstetricia

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x MB = 1 x 1 = 1) → Menor
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x B = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 2 x 2 = 4) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Menor
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Hospitalización***

Tabla 46. Estimación de Riesgos en el Área de Hospitalización

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x MB = 1 x 1 = 1) → Menor
Suplantación de la Identidad del Usuario	(PF x B = 2 x 2 =4) → Menor
Abuso de Privilegios de Acceso	(MPF x B = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 2 x 2 = 4) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(PF x MB = 2 x 1 = 2) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Laboratorio***

Tabla 47. Estimación de Riesgos en el Área de Laboratorio

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x B = 1 x 2 = 2) → Menor
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x B = 1 x 2 = 2) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(PF x B = 2 x 2 = 4) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(PF x MB = 2 x 1 = 2) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Observación***

Tabla 48. Estimación de Riesgos en el Área de Observación

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x B = 1 x 2 = 2) → Menor
Suplantación de la Identidad del Usuario	(MPF x MB = 1 x 1 = 1) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Modificación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Corrupción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x A = 1 x 4 = 4) → Menor
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Rips***

Tabla 49. Estimación de Riesgos en el Área de Rips

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Modificación de la Información	(PF x M = 2 x 3 = 6) → Moderado
Corrupción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(PF x MB = 2 x 1 = 2) → Menor
Ataque destructivo	(MPF x A = 1 x 4 = 4) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Siau***

Tabla 50. Estimación de Riesgos en el Área de Siau

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(PF x M = 2 x 3 = 6) → Moderado
Suplantación de la Identidad del Usuario	(MPF x B = 1 x 2 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x B = 1 x 2 = 2) → Menor
Intercepción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Modificación de la Información	(PF x M = 2 x 3 = 6) → Moderado
Corrupción de la Información	(PF x MB = 1 x 2 = 2) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(PF x MA = 1 x 5= 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Sistemas***

Tabla 51. Estimación de Riesgos en el Área de Sistemas

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(N x A = 3 x 4 = 12) → Grave
Suplantación de la Identidad del Usuario	(N x A = 3 x 4 = 12) → Grave
Abuso de Privilegios de Acceso	(N x A = 3 x 4 = 12) → Grave
Uso no Previsto	(MPF x A = 1 x 4 = 4) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x A = 1 x 4 = 4) → Menor
Intercepción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Modificación de la Información	(N x A = 3 x 4 = 12) → Grave
Corrupción de la Información	(PF x A = 2 x 4 = 8) → Moderado
Destrucción de la Información	(N x MA = 3 x 5 = 15) → Crítico
Divulgación de la Información	(PF x A = 2 x 4 = 8) → Moderado
Ataque destructivo	(MPF x A = 1 x 4= 4) → Menor
Indisponibilidad de Personal	(MPF x M = 1 x 3 = 3) → Menor

Fuente: El Autor

- ***Área de Subgerencia***

Tabla 52. Estimación de Riesgos en el Área de Subgerencia

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(MPF x MB = 1 x 1 = 1) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Modificación de la Información	(MPF x M = 1 x 3 = 3) → Menor
Corrupción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Destrucción de la Información	(MPF x A = 1 x 3 = 3) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Menor
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Telemática***

Tabla 53. Estimación de Riesgos en el Área de Telemática

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x A = 1 x 4 = 4) → Menor
Suplantación de la Identidad del Usuario	(MPF x A = 1 x 4 = 4) → Menor
Abuso de Privilegios de Acceso	(MPF x A = 1 x 4 = 4) → Menor
Uso no Previsto	(MPF x A = 1 x 4 = 4) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x A = 1 x 4 = 4) → Menor
Intercepción de la Información	(MPF x A = 1 X 4 = 4) → Menor
Modificación de la Información	(MPF x A = 1 x 4 = 4) → Menor
Corrupción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x M = 1 x 3 = 3) → Menor
Ataque destructivo	(MPF x A = 1 x 4= 4) → Menor
Indisponibilidad de Personal	(MPF x A = 1 x 4 = 4) → Menor

Fuente: El Autor

- ***Área de Terapia Física***

Tabla 54. Estimación de Riesgos en el Área de Terapia Física

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(MPF x MB = 1 x 1 = 1) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x B = 1 x 2 = 2) → Menor
Modificación de la Información	(MPF x M = 1 x 3 = 3) → Menor
Corrupción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x MA = 1 x 5= 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Tesorería***

Tabla 55. Estimación de Riesgos en el Área de Tesorería

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(MPF x M = 1 x 3 = 3) → Menor
Abuso de Privilegios de Acceso	(MPF x M = 1 x 3 = 3) → Menor
Uso no Previsto	(MPF x M = 1 x 3 = 3) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x M = 1 x 3 = 3) → Menor
Intercepción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Modificación de la Información	(PF x A = 2 x 4 = 8) → Moderado
Corrupción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(PF x M = 2 x 3 = 6) → Moderado
Ataque destructivo	(MPF x MA = 1 x 5 = 5) → Moderado
Indisponibilidad de Personal	(MPF x B = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Triage***

Tabla 56. Estimación de Riesgos en el Área de Triage

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 1 = 1) → Menor
Suplantación de la Identidad del Usuario	(MPF x MB = 1 x 1 = 1) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Modificación de la Información	(MPF x M = 1 x 3 = 3) → Menor
Corrupción de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x MB = 1 x 1 = 1) → Menor
Ataque destructivo	(MPF x MA = 1 x 5= 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Uci Adultos***

Tabla 57. Estimación de Riesgos en el Área de Uci Adultos

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(PF x MB = 2 x 1 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Modificación de la Información	(MPF x A = 1 x 4 = 4) → Menor
Corrupción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Ataque destructivo	(MPF x MA = 1 x 5= 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Uci Neonatal***

Tabla 58. Estimación de Riesgos en el Área de Uci Neonatal

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(PF x MB = 2 x 1 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Modificación de la Información	(MPF x A = 1 x 4 = 4) → Menor
Corrupción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Ataque destructivo	(MPF x MA = 1 x 5= 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

- ***Área de Uci Pediátrica***

Tabla 59. Estimación de Riesgos en el Área de Uci Pediátrica

AMENAZA	CLASE DE RIESGO
Manipulación de la Configuración	(MPF x M = 1 x 3 = 3) → Menor
Suplantación de la Identidad del Usuario	(PF x MB = 2 x 1 = 2) → Menor
Abuso de Privilegios de Acceso	(MPF x MB = 1 x 1 = 1) → Menor
Uso no Previsto	(MPF x MB = 1 x 1 = 1) → Menor
Difusión de Software Dañino	(MPF x A = 1 x 4 = 4) → Menor
Acceso no Autorizado	(MPF x MB = 1 x 1 = 1) → Menor
Intercepción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Modificación de la Información	(MPF x A = 1 x 4 = 4) → Menor
Corrupción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Destrucción de la Información	(MPF x A = 1 x 4 = 4) → Menor
Divulgación de la Información	(MPF x B = 1 x 2 = 2) → Menor
Ataque destructivo	(MPF x MA = 1 x 5= 5) → Moderado
Indisponibilidad de Personal	(MPF x MB = 1 x 1 = 1) → Menor

Fuente: El Autor

9.2. ESTABLECIMIENTO DE CONTROLES ADECUADOS PARA EL TRATAMIENTO DE LOS RIESGOS DE ACUERDO A LA NORMA NTC-ISO/IEC 27001

9.2.1. Objetivos de control y controles. Un Control es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable.[31]

A continuación, se listan los objetivos de control y controles que tratan los riesgos y debilidades encontradas en el sistema de información de la Clínica Laura Daniela

Se tiene como guía el anexo A de la norma ISO 27001, propone:

A.5 Política de seguridad

A.6 Organización de la información de seguridad

A.7 Gestión de activos

A.8 Seguridad de los recursos humanos

A.9 Seguridad física y del entorno

Quedando para el presente texto entonces:

A.10 Administración de las comunicaciones y operaciones

A.11 Control de accesos

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

A.13 Administración de los incidentes de seguridad

A.14 Administración de la continuidad de negocio

A.15 Marco legal y buenas prácticas

[31] **ISO-27001, LOS CONTROLES (Parte II),** Madrid, de 2006, Alejandro Corletti Estrada [Disponible en: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf

10. RESULTADOS DEL PROCESO DE AUDITORIA

La realización periódica de auditorías informáticas, representa para cada empresa la oportunidad de constatar la eficiencia y funcionalidad de cada una de las aplicaciones implementadas en el manejo de sus procesos internos. Todo esto se logra realizando entrevistas, encuestas y pruebas que contribuyan a evidenciar errores y falencias en los procesos informáticos llevados a cabo dentro de la organización.

Después de haber realizado encuestas y entrevistas al personal de labores que maneja la información procesada mediante la aplicación Krystalos en la Clínica Laura Daniela, y someter a la aplicación a una serie de pruebas se determinaron los siguientes resultados:

Aunque la aplicación Krystalos, presenta soluciones informáticas para la mayoría de los procesos llevados a cabo dentro de la Clínica Laura Daniela, éstas son solamente soluciones parciales, ya que no se ajustan en su totalidad a las necesidades puntuales de la entidad.

Los controles que posee la aplicación Krystalos, aunque presentan un grado muy representativo de utilidad y funcionalidad, no aplican en su mayoría para neutralizar algunos riesgos y errores trascendentales, generando muchas veces fallas en el procesamiento de la información.

La carencia de Políticas de Seguridad Informática en la Clínica Laura Daniela, ha imposibilitado un manejo organizado y eficiente del Sistema de Información, debido al uso inadecuado de algunas herramientas y procedimientos involucrados directamente con el manejo de los datos.

La falta de actualizaciones en algunos módulos, por cambios o modificaciones generadas desde el área contable, genera inconsistencias que repercuten en la integridad y confiabilidad de los datos manipulados mediante la aplicación Krystalos.

Algunos procesos involucrados con el censo y manejo de pacientes dentro de la Clínica Laura Daniela, se están viendo afectados por la falta de parámetros claros en la administración de pacientes en el área asistencial.

Existen claras falencias de diseño en algunos módulos de la aplicación Krystalos, donde es claramente notable que los desarrolladores pasaron por alto las posibles equivocaciones que podían cometer los usuarios en el momento de registrar e ingresar los datos al sistema.

El Manejo del Kárdex en la aplicación Krystalos, presenta deficiencias notables, puesto que la información reflejada en éste no coincide con las existencias en físico, generando inconsistencias en el momento de generar los reportes.

Con base a la Matriz de riesgos vs. Controles, podemos concluir que los riesgos más críticos son:

- ***R002 Limitaciones en la Trazabilidad de Documentos***
- ***R004 Falencias en el Proceso de Devoluciones en Compras***
- ***R006 Problemas con la Información del Censo de Pacientes***
- ***R007 Falta de Actualización en Cambios Generados Desde Contabilidad***
- ***R008 Dificultad para Reversar Procesos de Registro de Compras***

Por tal razón, se hace necesario que la Clínica Laura Daniela preste la adecuada atención a éstos, y realice una intervención oportuna implementando controles que contribuyan a minimizarlos, debido a que son los riesgos que presentan mayor probabilidad de ocurrencia.

CONCLUSIONES

Al finalizar este trabajo investigativo, en el cual se realizó un análisis detallado a los sistemas de información de la clínica Laura Daniela con énfasis en la aplicación Krystalos mediante técnicas y herramientas de auditoria, hemos podido concluir que:

La realización de la auditoria de seguridad informática al sistema de información de la clínica Laura Daniela en el marco de la norma NTC-ISO 27001 y el referente metodológico Magerit, es un importante avance para el desarrollo óptimo de sus procesos y el posicionamiento de la compañía frente a sus clientes, por la sensibilidad de la información que se maneja a su interior (Información de clientes, proveedores, productos y materias primas, etc.).

La clasificación y valoración de los activos informáticos permitió a la organización determinar el nivel de criticidad a la que están expuestos los activos dentro de una escala cualitativa de exposición al riesgo.

El análisis y gestión de riesgos, amenazas y vulnerabilidades al igual que la aplicación de las herramientas de petesting permitió conocer el nivel de exposición a la que se encuentra expuestos los activos informáticos en la clínica, esto con el fin de mitigarlas para que no se vea afectada la continuidad del negocio. Una vez se determinaron los riesgos, amenazas, su probabilidad de ocurrencia e impacto, se seleccionaron las salvaguardas o contramedidas más adecuadas para dar tratamiento a dichas amenazas.

Se recomendaron los controles y contramedidas de acuerdo a las recomendaciones de la norma NTC-ISO 27001:2013 lo que le permite a la empresa determinar las políticas y procedimientos más adecuados con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

La aplicación Krystalos, aunque suple los requerimientos en la mayoría de los procesos informáticos llevados a cabo en la Clínica Laura Daniela, existen fallas y errores durante su ejecución; que impiden un procesamiento integral y eficiente de los datos manejados por las diferentes áreas de esta entidad.

Los controles que presenta la aplicación Krystalos, no son suficientes para los riesgos presentados durante su ejecución, ya que en algunos casos éstos no

aplican, y en otros casos no realizan un proceso completo en la neutralización de riesgos.

Existen deficiencias en los procesos informáticos que involucran el censo de pacientes dentro de la Clínica Laura Daniela, debido a una parametrización inadecuada en la administración de pacientes en el área asistencial.

Existen fallas claras en el manejo de inventarios mediante la aplicación Krystalos, debido a que la información obtenida a partir de procedimientos que involucran Kárdex presenta muchas veces inconsistencias, generando confusión en el personal de labores y retraso en las actividades.

La aplicación Krystalos no permite realizar al usuario, un registro automatizado de los procedimientos concernientes a las devoluciones de las compras hechas por la entidad, generando así, inconsistencias relevantes en los procesos realizados por otras áreas de la empresa como: contabilidad y cuentas por pagar, las cuales dependen directamente de las actividades llevadas a cabo en el área de inventario.

Algunos módulos de la aplicación Krystalos que suministran información a otras áreas de la empresa, no reflejan las modificaciones y correcciones realizadas desde los módulos que reciben los datos inicialmente, generando inconsistencias en los procesos informáticos.

La implementación de políticas de seguridad informática en la Clínica Laura Daniela, contribuirán a mejorar notablemente los procesos involucrados con el manejo de los datos; obteniendo de esta manera, mayor organización y eficiencia en cada uno de estos procedimientos.

La falta de trazabilidad en algunos de los documentos procesados mediante la aplicación Krystalos, impide a los usuarios tener acceso a justificaciones que faciliten la toma de decisiones y contribuyan a un intercambio eficiente de la información manejada en la Clínica Laura Daniela.

Es evidente la falta de seguridad en el sitio web de la empresa, lo que significa que se deben implementar protocolos de seguridad a la misma y certificar dicha página aplicando procesos de encriptación que garanticen la integridad de la información.

RECOMENDACIONES

Teniendo en cuenta los resultados obtenidos a partir de la auditoría realizada a la aplicación en funcionamiento Krystalos, donde se pudieron evidenciar errores y fallas presentadas durante su ejecución; se hace necesario exponer algunas recomendaciones con el objetivo de mejorar los procesos informáticos en la Clínica Laura Daniela. Dentro de estas recomendaciones se destacan las siguientes:

- Debido a la continua actividad en algunas áreas de la Clínica Laura Daniela donde se maneja flujo constante de dinero, como lo son CAJA y FACTURACION, es necesario establecer en la aplicación Krystalos un control de tiempo para cada usuario, de tal manera, que solo se le habilite un intervalo de tiempo determinado de acuerdo a los turnos establecidos, para lograr mayor confidencialidad y seguridad en los procedimientos.

- Realizar periódicamente entrevistas y encuestas al personal directamente involucrado con el manejo de la aplicación Krystalos, con el objetivo de obtener información que revele fallas en los procedimientos, posibilitando de esta manera, la toma de decisiones por parte del área de Sistemas, y por consiguiente, contribuya al mejoramiento de las actividades informáticas dentro de la entidad

- Implementar en la aplicación Krystalos, reportes que permitan observar con claridad y a partir de notificaciones, los procesos históricos que involucren envío y recepción de documentación entre las diferentes áreas de la Clínica, de tal manera, que se pueda conocer en determinado caso, la trazabilidad completa de documentos cuando sea necesario.

- Es necesaria la puesta en marcha de un temporizador configurable, que permita regular los cambios o modificaciones en la información digitada por usuarios del Área Asistencial; de tal manera, que los médicos y enfermeras tengan establecido un tiempo determinado para agregar o cambiar información de su propio registro. Esto contribuirá a la eficiencia y oportunidad en los procedimientos.

- Al implementar el temporizador configurable para modificación de la información en la parte asistencial, se debe establecer un control que impida posteriormente cualquier registro de datos por parte del usuario y su línea de acción; es decir, al registrar datos un médico durante el tiempo establecido, solo se bloquearían

acciones correspondientes a la parte médica, quedando habilitada acciones por la parte especializada y de enfermería.

- Desarrollar una herramienta que posibilite la vinculación de pacientes a los costos generados por éstos durante los procedimientos que se le realicen, con el objeto de obtener registros detallados en los reportes correspondientes a los costos generados en el área asistencial de la Clínica Laura Daniela.

- Se hace necesario implementar un filtro comparativo en el proceso de registro de compras realizadas por La Clínica Laura Daniela, que inicie solicitando al usuario el ingreso al sistema el valor total de la factura, y a partir de éste, tener una referencia que permita detectar mediante comparaciones, errores o inconsistencias en el ingreso de la información; teniendo en cuenta los posibles errores que el usuario puede cometer al digitar las cantidades, impuestos y/o valores detallados en cada factura.

- Establecer herramientas que contribuyan a la actualización de los módulos afectados a partir de información modificada desde el área de contabilidad, permitiendo a cada usuario, obtener datos consecuentes y confiables al momento de acceder a la información desde cualquier módulo que involucre acciones contables.

- Con miras a mejorar el proceso censal de pacientes dentro de la Clínica Laura Daniela, se debe implementar en la aplicación Krystalos, una herramienta donde la administración de éstos sea asignada al departamento de enfermería, de tal manera, que cada enfermera sea responsable de llevar un registro actualizado de los pacientes que maneja dentro de su área, y sea la encargada de ingresar la información de éstos al sistema.

- Implementar la utilización de Tokens USB o firmas digitales encriptadas entre los usuarios de la aplicación Krystalos, con el fin de evitar el préstamo de claves a demás trabajadores de la institución o en su defecto el robo de identidad para acceder al sistema. Esto garantizará mayor seguridad y confidencialidad en el manejo de la información.

- Desarrollar o implementar herramientas que hagan posible un manejo adecuado y eficiente de los procesos involucrados con el área de inventarios dentro de la Clínica Laura Daniela, puesto que existen claras falencias en el manejo del Kárdex,

las devoluciones en compras y en la reversión o corrección por parte del usuario de los registros correspondientes a las compras realizadas por la entidad.

- Establecer políticas de seguridad informática, que contribuyan a un manejo eficiente de los procesos informáticos dentro de la Clínica Laura Daniela, y velar para que los usuarios den cumplimiento a cada uno de estos parámetros.

DIVULGACION

Los fines de este proyecto son principalmente académico, busca poner en práctica los conocimientos adquiridos en el transcurso de la especialización; No incluye información confidencial de la organización objeto de la auditoria, sin embargo, se incluye información referente a un proceso de auditoria en seguridad de la información en el periodo actual el cual puede diferir de los datos que reposan en la organización.

Los derechos de propiedad intelectual de este trabajo corresponden a la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD - COLOMBIA quien determinara las formas en las que este documento se puede compartir al público respetando su propiedad.

Sobre este trabajo pueden existir algunas restricciones de publicación que determinara la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD-COLOMBIA, en cualquier momento.

Este documento puede ser publicado en el repositorio institucional de la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD- COLOMBIA, para ser utilizado como referencia para otros trabajos de investigación en la Universidad o público general.

La UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD- COLOMBIA puede determinar en cualquier momento medios diferentes de publicación de este documento, revistas, artículos científicos, periódicos institucionales, libros, internet.

BIBLIOGRAFIA

ADACS. (2004). Asociación de Auditoría y Control de Sistemas de Información. Recuperado de: http://www.isaca.org/spanish/Pages/default.aspx.

AREVALO, D. (2014). Proyecto de norama tecnica colombiana NTC-ISO 27005. Recuperado de: https://fr.slideshare.net/danger-leinad/iso-27005espanol-34883875?cv=1

ARIAS, F. (2012). El proyecto de investigación, introducción a la metodología científica, Sexta edición, Editorial Epiteme Recuperado de: http://es.slideshare.net/paundpro/el-proyecto-de-investigacion-fidias-arias-2012.

AUDITOOL. NIA 320, La materialidad en la planeación y desarrollo de una auditoría. Aspectos Clave. Recuperado de: https://auditool.org/blog/auditoria-externa/331-la-materialidad-en-la-planeacion-y-desarrollo-de-una-auditoria.

AUDITORIASISTEMAS. (2014). Auditoria Sistemas. Auditoria informática. Recuperado de: http://auditoriasistemas.com/auditoria-informatica/.

AYALA, G., y GÓMEZ, J. (2011). Guia de buenas practicas de seguridad de la informacion en contextos de micro, pequeñas y medianas empresas de la region. Recuperado de: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2514/0058A973.pdf;jsessionid=A4EE857481BEAA5777D0F4526586611F?sequence=1.

BENÍTEZ, M. (2013). Gestion Integral. Políticas de Seguridad Informática. Recuperado de: http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf.

BORGHELLO, C. (2007). Escribiendo Políticas de Seguridad. Recuperado de: http://www.segu-info.com.ar/articulos/59-escribiendo-politicas-seguridad.htm. [2007]

CADME, C., y DUQUE, D. (2012). Auditoria de seguridad informatica ISO 27001 para la empresa de alimentos Cia. Ltda. Recuperado de: http://dspace.ups.edu.ec/bitstream/123456789/2644/16/UPS-CT002441.pdf.

CCM. (2017). Introducción a la seguridad informática. Recuperado de : . http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica.

CIE. Clínica Integral de Emergencia. Misión y Visión. Recuperado de: http://www.clinicaintegral.com.co/nosotros/misi%C3%B3n-y-visi%C3%B3n.html

CLÍNICA INTEGRAL DE EMERGENCIAS. Servicio humanizado por vocación. Recuperado de: http://www.clinicaintegral.com.co/

CONGRESO DE COLOMBIA. (1999). LEY 527. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276.

COOK, J.W. (1978). Auditoria, Filosofia y Tecnica/John W. Cook, Gary M. Winkle; Traducido por: M.G.R. DE V. DE Paredes. Mexico: Eudeba.

DEFINICIONABC. Definición de Base de datos. Recuperado de: http://www.definicionabc.com/tecnologia/base-de-datos.php. [s.f.]

DEGERENCIA. Qué es Tecnología de Información. Recuperado de: http://www.degerencia.com/tema/tecnologia_de_informacion. [s.f.]

DEL HIERRO, P., y TRUJILLO., F. (2012). Auditoria del sistema informatico del Hospital del sus "Enrique Garces". Recuperado de: http://bibdigital.epn.edu.ec/bitstream/15000/4484/1/CD-4095.pdf.

FCEIA. (2011). Auditoría Informática. Recuperado de: http://www.fceia.unr.edu.ar/asist/intro-aa-t.pdf.

FLORES, A. Metodología de gestión para las micro, pequeñas y medianas empresas en Lima Metropolitana. CAPÍTULO VII. Sistema de Información. Recuperado de: http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/empre/flores_ka/cap07.pdf. [s.f.]

GARCIA, C. (2012). Establecimiento del sistema de seguridad de información en SFG bajo los estándares de la norma ISO 27001: 2005. Recuperado de: http://repository.ean.edu.co/bitstream/handle/10882/2532/GarciaCamilo2012.pdf;jsessionid=6637DDAE1090F42CEAFF7FEF33FFF29D?sequence=1.

GIROUX & TREMBLAY. (2004). Metodologia de las ciencias humanas, La investigación en acción, Primera edición en español 2004, Editorial Fondo de cultura económica. Recuperado de: https://imas2010.files.wordpress.com/2010/06/metodologia-de-las-cchh-s-giroux-g-tremblay.pdf

GRANADOS, G. (2014). Información Activo valioso para las empresas. Recuperado de: http://www.visionindustrial.com.mx/industria/desarrollo-industrial-3020/informacion-activo-valioso-para-las-empresas.

HURTADO, (2000). *Metodología de la investigación holística.* IUTP. Sypal. Caracas MARTINEZ B., C. (1998). *Estadística y muestreo.* Ecoediciones. Colombia.

ISO-27001, LOS CONTROLES (Parte II), Madrid, de 2006, Alejandro Corletti Estrada. Recuperado de: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf

LEY 1273 DE 2009. Ministerio de las TIC. Recuperado de: http://www.mintic.gov.co/portal/604/w3-article-3705.html

LÓPEZ, H. (2009). Archivos Auditoría En Sistemas. Recuperado de: http://archivosauditoria.blogspot.com.co/.

LÓPEZ, E. (2012). ¿Qué es la Auditoria de sistemas de información? Universidad veracruzana. Recuperado de: http://www.uv.mx/personal/artulopez/files/2012/10/07-Auditoria-de-SI.pdf.

MHEDUCATION. La auditoría: concepto, clases y evolución. Recuperado de: http://assets.mheducation.es/bcv/guide/capitulo/8448178971.pdf. [s.f.]

MUÑOZ, C. (2002). Auditoría en sistemas. México : Pearson Educación.

PARRA, J. (2003). Guía de Muestreo. Maracaibo. LUZ.

PIATTINI, M., y DEL PESO , E. (2003). Auditoría Informática, un enfoque práctico. . ISbn: 958-682-455-1 : Alfaomega-Rama.

SABINO, C. (2007). El proceso de investigación, Caracas, Editorial Panapo, Recuperado de: http://es.slideshare.net/male2712/sabino-carlos-el-proceso-de-investigacion.

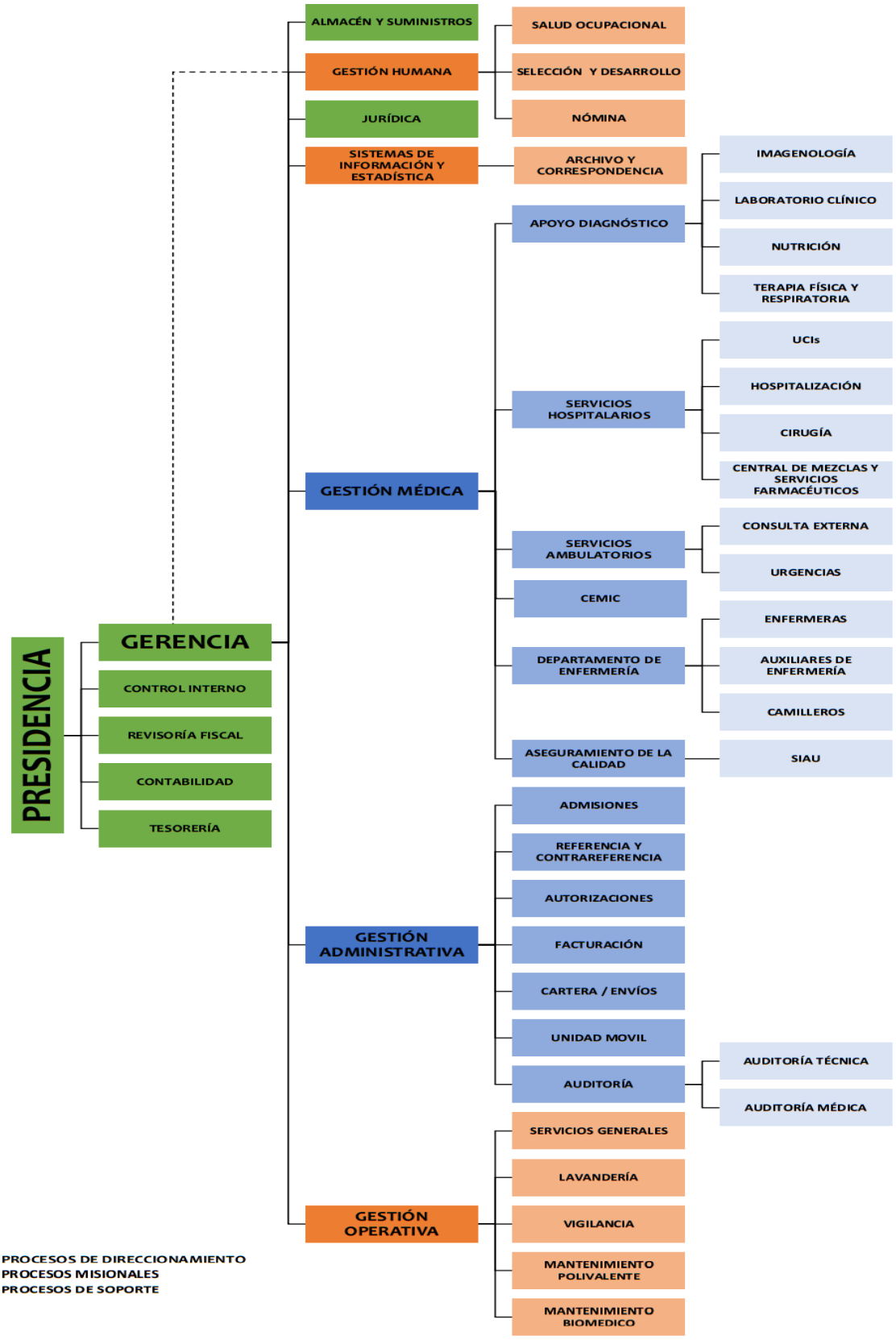
SAMPIERI. H. (1998). Metodologia de la investigación, Editorial McGraw-Hill. Recuperado de: http://www.univo.edu.sv:8081/tesis/021552/021552_Cap3.pdf [1998]

TAMAYO & TAMAYO. (2000). El proceso de la investigación científica, Cuarta edición, Editorial Limusa. Recuperado de: http://es.slideshare.net/sarathrusta/el-proceso-de-investigacion-cientifica-mario-tamayo-y-tamayo1

TAMAYO & TAMAYO. (1997). El proceso de la investigación científica, tercera edición, Editorial Limusa.

UNIVERSIDAD DEL CAUCA. Aspectos Organizacionales de los Sistemas de Información. 1. Conceptos Básicos de Sistemas de Información. Recuperado de: http://fccea.unicauca.edu.co/old/siconceptosbasicos. [s.f.]

ANEXO A. Sistema Organizacional Clínica Laura Daniela



ANEXO B. Informe general de la auditoria

INTRODUCCION

El presente informe pretende dar a conocer los resultados obtenidos tras la realización de la investigación descriptiva y aplicada puesto que busca especificar propiedades, características y rasgos importantes de cualquier fenómeno y proponer un “plan de acción” o intervenir eficazmente en una situación dada que se analice dentro de la empresa CLINICA LAURA DANIELA con el objetivo de emitir un informe que pueda ser presentado a las directivas de la empresa, para que el gerente lo evalué junto con sus trabajadores y así tomen decisiones encaminadas a corregir las deficiencias encontradas.

OBJETIVOS DE LA AUDITORIA

OBJETIVO GENERAL

Analizar detalladamente el sistema de información actual, con el fin de emitir un informe general acerca de su funcionamiento.

OBJETIVOS ESPECÍFICOS

- Analizar y evaluar todas las evidencias necesarias para poder determinar si el sistema de información es seguro, eficaz y confiable.

- Seleccionar los controles que ayuden a minimizar los riesgos, amenazas y vulnerabilidades que presente el sistema de información.

- Determinar los riesgos que atentan contra la integridad del Sl.

- Presentar una guía de políticas y prácticas de seguridad de la información.

- Presentar un informe y que sirva de apoyo a la administración en la toma de cualquier decisión que contribuya al mejoramiento de los procesos realizados por el SC.

Valledupar, junio del 2017

Doctor
JAIME ARCE
Gerente clínica Laura Daniela
Ing. Edgardo Martínez

ASUNTO: INFORME DE AUDITORÍA AL SISTEMA DE INFORMACIÓN EN LA EMPRESA CLÍNICA LAURA DANIELA

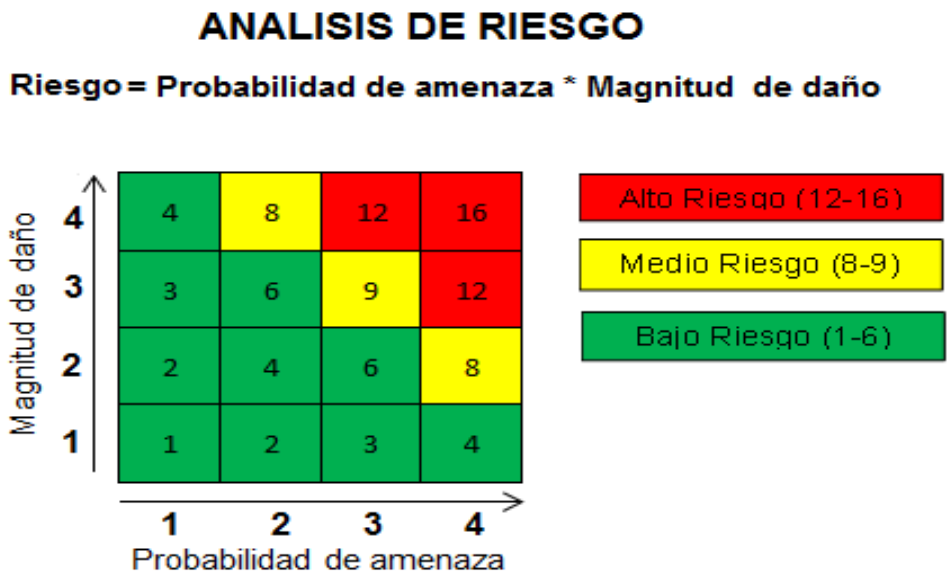
Respetado Señor:

En cumplimiento con los objetivos propuestos en el plan de auditoría al sistema de información, se evaluaron los diferentes activos de la empresa.

Para la evaluación de los riesgos se utilizó una matriz o tabla “para relacionar el valor del activo y la probabilidad de ocurrencia de la amenaza, teniendo en cuenta los aspectos de vulnerabilidad”.

El valor del activo se determinó teniendo en cuenta “el costo en que se incurre debido a la perdida de confidencialidad, integridad y disponibilidad como resultado de un incidente”.

FIGURA 1. Análisis de riesgo



Es decir, se determinó el valor del activo considerando el impacto que tendría en la empresa si el mismo estuviera expuesto a una amenaza inminente. Se le asignaron los siguientes valores a los activos:

Tabla 1. **Valor del activo**

ACTIVO	HARDWARE	SOFTWARE	RED	PERSONAL	LUGAR	ORGANIZACIÓN
VALOR DEL ACTIVO	4	4	4	4	4	4

Fuente: El Autor

Para determinar la probabilidad de ocurrencia de una amenaza se realizó una encuesta por cada activo, teniendo en cuenta las posibles vulnerabilidades que se pueden presentar en una empresa, las cuales así mismo se relacionan con sus respectivas amenazas. El valor de probabilidad de ocurrencia que se presenta en las tablas resulta de la siguiente escala promediada con la cantidad de personas encuestadas:

Tabla 2. Valor cualitativo y cuantitativo de la vulnerabilidad (elaboración propia)

VALOR CUALITATIVO DE LA VULNERABILIDAD	VALOR CUANTITATIVO DE LA VULNERABILIDAD
EXCELENTE	1
BUENO	2
REGULAR	3
BAJA	4
NO CUMPLE	5

Fuente: El Autor

Finalmente, para evaluar el riesgo se calcula la medida del mismo multiplicando el valor del activo por la probabilidad de ocurrencia. La medida del riesgo se clasifica en la siguiente tabla:

Tabla 3. Medida del riesgo basado en el análisis de riesgo

MEDIDA DEL RIESGO	CLASIFICACIÓN DE LA AMENAZA
1-6	**BAJO RIESGO**
8-9	**MEDIO RIESGO**
12-16	**ALTO RIESGO**

Fuente: El Autor

A continuación, se detallan los diferentes activos con su respectiva evaluación de riesgos:

1. ACTIVO: HARDWARE

Tabla 4. Evaluación de riesgo de hardware

N°	Descriptor de la amenaza (a)	Consecuencia (valor del activo) (b)	Probabilidad de ocurrencia de la amenaza (c)	Medida del riesgo (d)	Clasificación de la amenaza (e)
1	Hurto de equipos	4	2	8	Medio Riesgo (8-9)
2	Destrucción del equipo o los medios.	4	2	8	Medio Riesgo (8-9)
3	Mal funcionamiento del equipo.	4	2	8	Medio Riesgo (8-9)
4	Incumplimiento en la disponibilidad del personal	4	2	8	Medio Riesgo (8-9)
5	Perdida de suministro de energía	4	2	8	Medio Riesgo (8-9)
6	Hurto de medios o documentos.	4	1	4	Bajo riesgo (1-6)
7	Uso no autorizado del equipo.	4	3	12	Alto riesgo (12-16)
8	Polvo, corrosión, congelamiento.	4	2	8	Medio Riesgo (8-9)
9	Error en el uso.	4	2	8	Medio Riesgo (8-9)
10	Falla del equipo.	4	2	8	Medio Riesgo (8-9)

Fuente: El Autor

El resultado final del análisis de riesgo del activo en hardware un promedio del 80% de las amenazas anteriormente mencionadas están en un nivel de calificación medio en un rango de (8-9), un 10% de las amenazas se considera en un nivel bajo en un rango de (1-6), y un 10% de las amenazas se considera en un nivel alto en un rango de (12-16) para un total del 100%.

De las amenazas en el activo hardware podemos concluir que se maneja una taza de riesgo medio, por lo tanto podría producirse daño a la información.

2. ACTIVO: SOFTWARE

Tabla 5. Evaluación de riesgo de software

N°	Descriptor de la Amenaza (a)	Consecuencia (valor del activo) (b)	Probabilidad de ocurrencia de la amenaza (c)	Medida del riesgo (d)	Clasificación de la amenaza (e)
1	Mal funcionamiento del software.	4	2	8	Medio Riesgo (8-9)
2	Uso no autorizado del equipo	4	2	8	Medio Riesgo (8-9)
3	Procesamiento ilegal de los datos.	4	2	8	Medio Riesgo (8-9)
4	Abuso de los derechos	4	2	8	Medio Riesgo (8-9)
5	manipulación con software	4	2	8	Medio Riesgo (8-9)
6	Falsificación de derechos.	4	2	8	Medio Riesgo (8-9)
7	Acceso no autorizado al sistema,	4	2	8	Medio Riesgo (8-9)
8	Terrorismo.	4	2	8	Medio Riesgo (8-9)
9	Detección de la posición.	4	2	8	Medio Riesgo (8-9)
10	Saturación al sistema información	4	2	8	Medio Riesgo (8-9)
11	Piratería	4	2	8	Medio Riesgo (8-9)
12	Espionaje	4	2	8	Medio Riesgo (8-9)
13	otros ataques informáticos	4	2	8	Medio Riesgo (8-9)
14	Error en el uso	4	2	8	Medio Riesgo (8-9)
15	Datos provenientes de fuentes no confiables	4	2	8	Medio Riesgo (8-9)
16	uso de software falso o copiado	4	2	8	Medio Riesgo (8-9)
17	Pérdida de suministro de energía,	4	2	8	Medio Riesgo (8-9)
18	falla del equipo de telecomunicaciones	4	2	8	Medio Riesgo (8-9)
19	Hurto de medios y documentos	4	2	8	Medio Riesgo (8-9)
20	intrusión en el sistema, manipulación del sistema	4	2	8	Medio Riesgo (8-9)
21	suplantación de identidad	4	2	8	Medio Riesgo (8-9)
22	Acceso no autorizado al sistema, crimen por computador	4	2	8	Medio Riesgo (8-9)

Fuente: El Autor

En el resultado final del análisis de riesgo del activo en software un promedio del 100% de las amenazas anteriormente mencionadas se encuentran en un nivel de calificación medio en un rango de (8-9), con lo que podemos concluir que este activo maneja una taza de riesgo medio, por lo tanto, podría producirse daño a la información.

4. ACTIVO: RED

Tabla 6. Evaluación de riesgo de red

N°	Descriptor de la amenaza (a)	Consecuencia (valor del activo) (b)	Probabilidad de ocurrencia de la amenaza (c)	Medida del riesgo (d)	Clasificación de la amenaza (e)
1	Negación de acciones	4	2	8	Medio Riesgo (8-9)
2	Mal funcionamiento del equipo	4	2	8	Medio Riesgo (8-9)
3	Falla del equipo	4	2	8	Medio Riesgo (8-9)
4	Mal funcionamiento del software	4	2	8	Medio Riesgo (8-9
5	Manipulación con hardware	4	3	12	Alto riesgo (12-16)
6	Uso no autorizado del equipo	4	2	8	Medio Riesgo (8-9)
7	Incumplimiento en el mantenimiento del sistema de información.	4	2	8	Medio Riesgo (8-9)
8	Error en el uso.	4	2	8	Medio Riesgo (8-9)
9	Divulgación ilegal de la información	4	2	8	Medio Riesgo (8-9)
10	Abuso de derechos	4	2	8	Medio Riesgo (8-9)
11	Destrucción de la información	4	3	12	Alto riesgo (12-16)
12	Polvo, fuego, contaminación, corrosión, congelamiento o daños por agua.	4	3	12	Alto riesgo (12-16)
13	Fenómenos sísmicos, volcánicos, meteorológicos, etc.	4	4	16	Alto riesgo (12-16)

Fuente: El Autor

En el resultado final del análisis de riesgo del activo en red un promedio del 70% es de las amenazas anteriormente mencionadas y se encuentran en un nivel de calificación medio en un rango de (8-9), y un 30% de las amenazas se considera en un nivel alto en un rango de (12-16), para un total del 100% de las amenazas en el activo en red. Lo que nos lleva a concluir que este activo se maneja en una taza de riesgo media, por lo tanto podría producirse daño a la información.

4. ACTIVO: PERSONAL

Tabla 7. Evaluación de riesgo de Personal

N°	Descriptor de la amenaza (a)	Consecuencia (valor del activo) (b)	Probabilidad de ocurrencia de la amenaza (c)	Medida del riesgo (d)	Clasificación de la amenaza (e)
1	Incumplimiento en la disponibilidad del personal	4	2	8	Medio Riesgo (8-9)
2	Error en el uso	4	3	12	Alto riesgo (12-16)
3	Mal funcionamiento del software	4	3	12	Alto riesgo (12-16)
4	Uso no autorizado del equipo	4	3	12	Alto riesgo (12-16)
5	Accidentes importantes	4	3	12	Alto riesgo (12-16)
6	Falla En El Suministro De Aire Acondicionado	4	2	8	Medio Riesgo (8-9)

Fuente: El Autor

En el resultado final del análisis de riesgo del activo en personal un promedio del 67% es de las amenazas anteriormente mencionadas con un nivel de calificación alto en un rango de (12-16), y un 33% de las amenazas se considera en un nivel medio en un rango de (8-9), para un total del 100% de las amenazas en el activo en personal. Lo que nos lleva a concluir que este activo se maneja en una taza de riesgo alto, por consiguiente, la empresa corre un alto riesgo de daño a la información.

5. ACTIVO: LUGAR

Tabla 8. Evaluación de riesgo de lugar

N°	Descriptor de la amenaza (a)	Consecuencia (valor del activo) (b)	Probabilidad de ocurrencia de la amenaza (c)	Medida del riesgo (d)	Clasificación de la amenaza (e)
1	Accidente importante	4	3	12	Alto riesgo (12-16)
2	Destrucción del equipo o los medios	4	3	12	Alto riesgo (12-16)
3	Perdida de suministro de energía	4	2	8	Medio Riesgo (8-9)
4	Incumplimiento en el mantenimiento del sistema de información	4	2	8	Medio Riesgo (8-9)
5	Error en uso	4	2	8	Medio Riesgo (8-9)
6	Falla en el sistema de suministro de aire acondicionado	4	3	12	Alto riesgo (12-16)
7	Fenómenos sísmicos	4	4	16	Alto riesgo (12-16)
8	Inundaciones	4	4	16	Alto riesgo (12-16)
9	Fenómenos climáticos	4	3	12	Alto riesgo (12-16)
10	Fuego	4	4	16	Alto riesgo (12-16)
11	Hurto de medios o documentos	4	3	12	Alto riesgo (12-16)
12	Mal funcionamiento del equipo	4	2	8	Medio Riesgo (8-9)
13	Incumplimiento en la disponibilidad del personal	4	3	12	Alto riesgo (12-16)
14	Abuso de los derechos	4	3	12	Alto riesgo (12-16)

Fuente: El Autor

El resultado final del análisis de riesgo del activo en lugar arroja que un promedio del 72% de las amenazas anteriormente mencionadas están en un nivel de calificación alto en un rango de (12-16), y un 28% de las amenazas se considera en un nivel medio en un rango de (8-9), para un total del 100% de las amenazas en el activo en lugar. Lo que nos da a concluir que este activo se maneja en una taza de riesgo alto, por consiguiente, la empresa corre un alto riesgo de daño a la información.

6. ACTIVO: ORGANIZACIÓN

Tabla 9. Evaluación de riesgo de organización

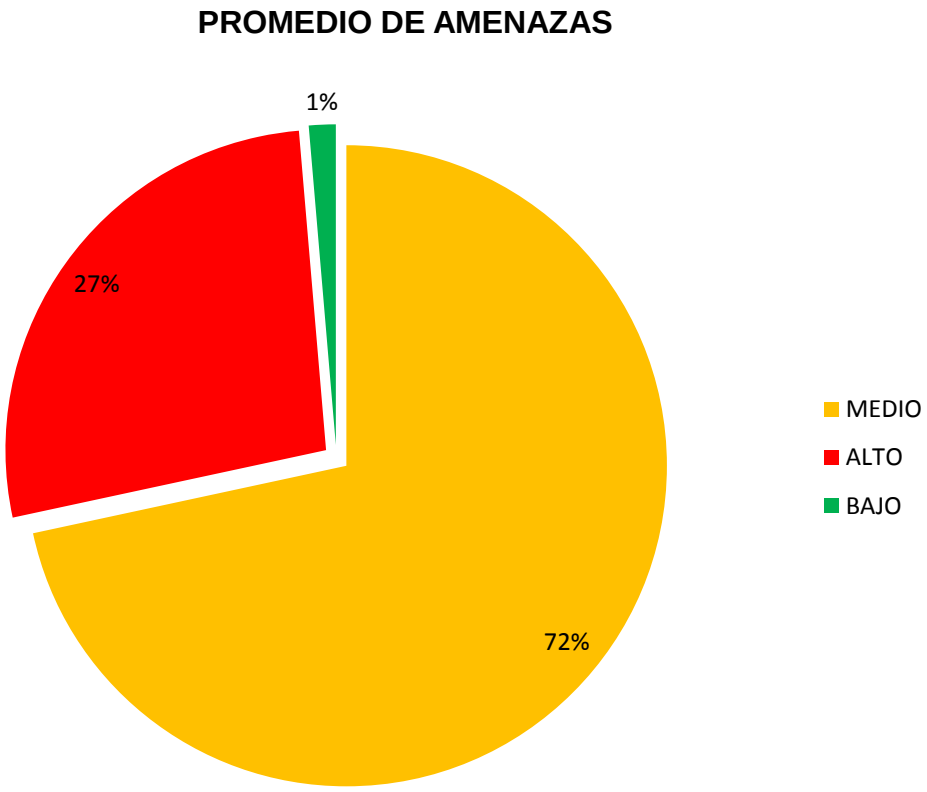
N°	Descriptor de la amenaza (a)	Consecuencia (valor del activo) (b)	Probabilidad de ocurrencia de la amenaza (c)	Medida del riesgo (d)	Clasificación de la amenaza (e)
1	Abuso de los derechos	4	2	8	Medio Riesgo(8-9)
2	Incumplimiento en el mantenimiento del sistema de información	4	3	12	Alto riesgo (12-16)
3	Corrupción de datos	4	2	8	Medio Riesgo (8-9)
4	Falla del equipo	4	2	8	Medio Riesgo (8-9)
5	Error en el uso	4	2	8	Medio Riesgo (8-9)
6	Procesamiento ilegal de datos	4	2	8	Medio Riesgo (8-9)
7	Hurto de equipo	4	2	8	Medio Riesgo (8-9)
8	Hurto de medios o documentos	4	2	8	Medio Riesgo(8-9)
9	Uso no autorizado del equipo	4	2	8	Medio Riesgo (8-9)

Fuente: El Autor

El resultado final del análisis de riesgo del activo en organización arroja que un promedio del 90% de las amenazas anteriormente mencionadas están en un nivel de calificación medio en un rango de (8-9), y un 10% de las amenazas se considera en un nivel alto en un rango de (12-16), para un total del 100% de las amenazas en el activo en organización. Lo que nos da a concluir que este activo se maneja en una taza de riesgo medio, por consiguiente, en la empresa podría producirse un daño a la información.

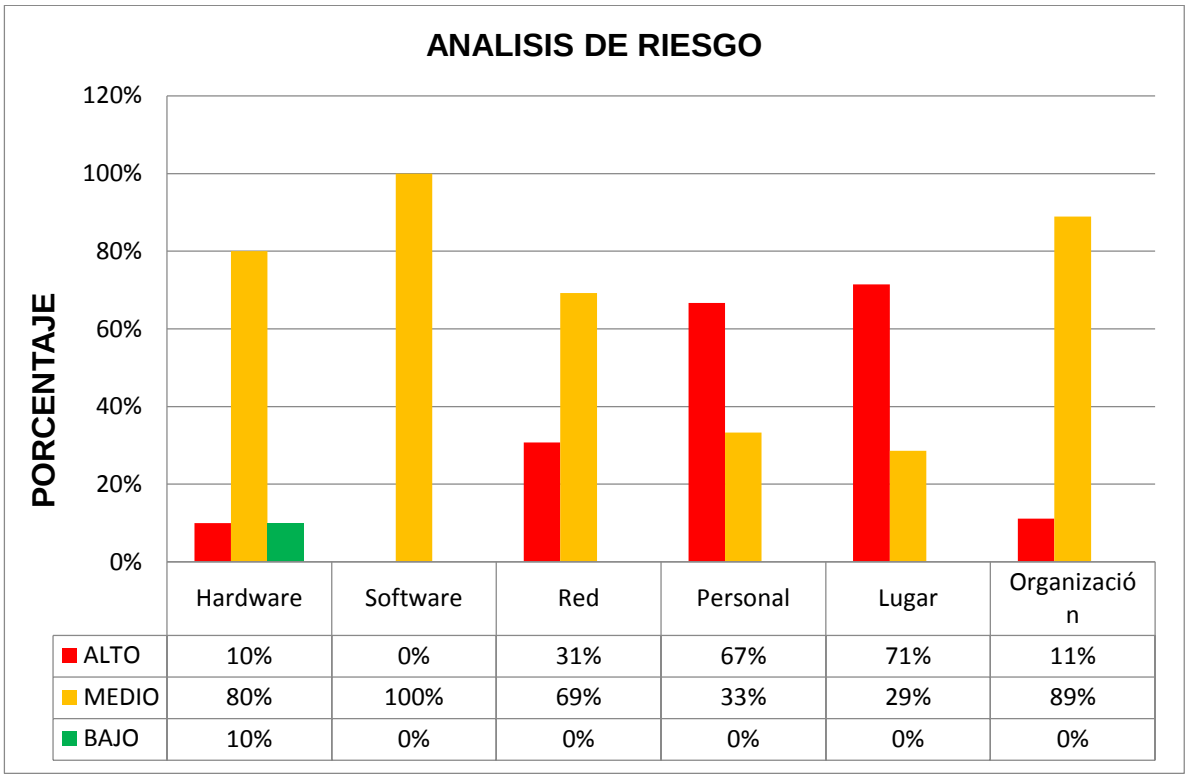
PROMEDIO ESTADÍSTICO DEL ANÁLISIS DE RIESGO

Grafica 1. Promedio de amenazas



La Grafica 1, está relacionada con las amenazas y probabilidad de ocurrencia de las mismas. De un total de 74 amenazas evaluadas entre los 6 activos (red, hardware, software, organización, lugar y personal), el 72% corresponde a las amenazas clasificadas en un riesgo medio de probabilidad de ocurrencia, el 27% corresponde a amenazas clasificadas en riesgo alto y solo el 1% a amenazas en riesgo bajo. Lo que indica, que 99% de las amenazas identificadas están entre alto y mediano riesgo, y que la empresa debe trabajar porque los activos de la empresa se encuentren en una condición segura ante la presencia de probabilidad de ocurrencias que incurren las amenazas en la empresa.

Grafica 2. Análisis del riesgo general por cada activo



	Hardware	Software	Red	Personal	Lugar	Organización
ALTO	10%	0%	31%	67%	71%	11%
MEDIO	80%	100%	69%	33%	29%	89%
BAJO	10%	0%	0%	0%	0%	0%

El análisis de los riesgos reflejado en la Grafica 2 arroja detalladamente que en la mayoría de los activos la probabilidad de ocurrencia de sus amenazas está en un nivel medio, es el caso de hardware, red y organización, de hecho, en el activo software todas las amenazas clasifican en nivel medio de ocurrencia o impacto.

Por otra parte, los activos lugar y personal manejan en mayor frecuencia riesgos altos de ocurrencia por las vulnerabilidades y debilidades en el tratamiento del sistema de información en estos ámbitos.

Esta estadística es radical para el enfoque en la toma de decisiones por parte de la gerencia, pues refleja el estado actual de la empresa.

La auditoría se efectuó conforme a las Normas y Procedimientos de Auditoría Generalmente aceptados y por consiguiente incluye la obtención y análisis de la información sobre el Sistema de información, sobre su entorno a través de observaciones, entrevistas, pruebas, análisis de documentos, operatividad del sistema, evaluación de los procedimientos y controles.

CONCLUSIONES

Como resultado de la auditoría al sistema de información CLINICA LAURA DANIELA. Se pudo determinar que es una empresa mediana con miras a extenderse, y que a corto plazo debe velar por el mejoramiento de sus condiciones y por la revisión de debilidades puntuales tales como: a nivel de uso no autorizado de equipos, control en la manipulación de las redes de comunicaciones, prevención ante siniestros de origen natural, y poca capacitación de personal. Todas y cada una de las anteriores son amenazas evaluadas, y a las cuales es necesario hacerles un control para disminuir los riesgos. Sin duda alguna la mayor debilidad del sistema de información es la ausencia de políticas y prácticas de seguridad planteadas por la administración de la empresa que regulen el comportamiento de los usuarios del sistema.

Por otra parte, hay riesgos medios que deben ser minimizados ante la presencia de amenazas, esto a través del tratamiento de la intrusión en el sistema, la manipulación del sistema, el uso de software falso o copiado, entre otros.

RECOMENDACIONES

Las recomendaciones finales que se resaltan de esta investigación después de haber evaluado todo el sistema y de haber encontrado todas estas fallas tanto en el sistema como en la empresa en general son las siguientes:

Se debe establecer, documentar y revisar la política de control de acceso, para asegurar que sólo se permite el acceso a personal autorizado.

Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.

Velar por el mantenimiento y mejor organización del cuarto de telecomunicaciones y el resto de la red de acuerdo a los estándares para cableado estructurado.

Se recomienda que se lleve a cabo una revisión periódica de las amenazas y riesgos, puesto que la tecnología está en constante cambios y avance, los cuales deben ser controlados para evitar futuros problemas.

Mejorar las condiciones preventivas ante riesgos laborales e incidentes de tipo natural, esto a través de asesorías con empresas de salud ocupacional, capacitación del personal y adecuación de salidas de emergencia y planes de contingencia.

Formalizar la realización, socialización y control de las políticas de seguridad entre los usuarios del sistema de información, así como la revisión periódica de las mismas por parte de la gerencia.

Expresamos nuestro agradecimiento por la colaboración recibida y gran disposición por parte de los funcionarios de la empresa CLINICA LAURA DANIELA.

Cordialmente,

_____

NEHEMIAS SARABIA DÍAZ

ANEXO C. INFORME DE AUDITORIA DE VULNERABILIDADES DEL SITIO WEB DE LA CLINICA INTEGRAL DE EMERGENCIAS LAURA DANIELA

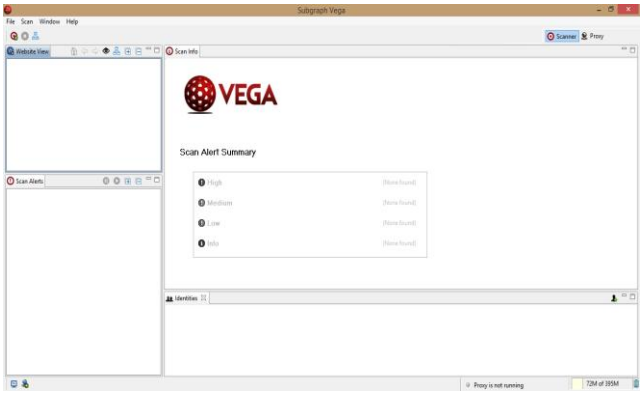
La seguridad en los sistemas de información de las empresas tiene un papel muy relevante para el desempeño de las mismas, es por ello que los sistemas deben estar protegidos ante cualquier posibilidad de ataque o ataque real al que puedan ser sometidos, esto se logra ideando estrategias de bloqueo a dichos ataques pero para poder crearlas primeramente se deben estudiar las vulnerabilidades que poseen dichos sistemas, por esta razón, existen múltiples técnicas y herramientas de análisis que permiten realizar estudios a fondo a los sistemas descubriendo en el acto los puntos débiles que poseen los sistemas, al tener identificadas estas vulnerabilidades se pueden idear todo tipo de mecanismos de defensas para contrarrestar cualquier tipo de ataques.

Con objetivo de identificar las vulnerabilidades presentes en *el sistema web de la Clínica Integral de Emergencias Laura Daniela* se realizaron Pruebas de Penetración.

DESCRIPCION DE HERRAMIENTAS

- **Vega Vulnerability Scanner:** Vega es un escáner de Vulnerabilidades de código abierto para probar la seguridad de aplicaciones web, en la cual puede ayudarle a encontrar y validar las Inyecciones SQL, Cross-Site Scripting (XSS), Shell Injection, Local File Inclusion, Integer Overflow y otras vulnerabilidades.

Vega incluye un escáner automatizado para pruebas rápidas y también un Proxy para proteger nuestra IP cuando realizamos alguna auditoria web. Vega fue desarrollado por Subgraph en Montreal.



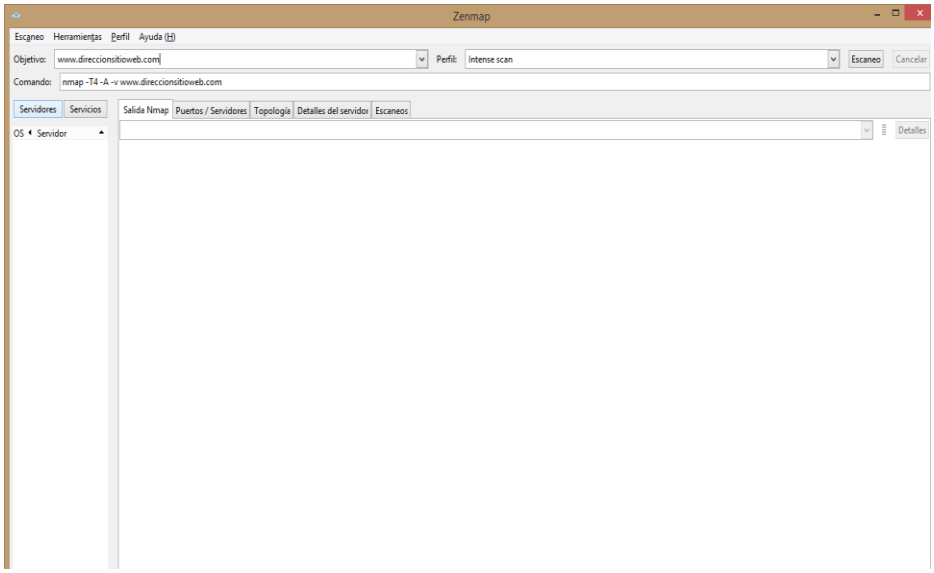
Fuente: Aplicación Vega

NMAP Security Scanner: Programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Este software posee varias funciones para sondear redes de computadores, incluyendo detección de equipos, servicios y sistemas operativos. Estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Además, durante un escaneo, es capaz de adaptarse a las condiciones de la red incluyendo latencia y congestión de la misma.

Entre las caracterizticas de esta herramienta encontramos:

- Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo, listando aquellas que responden ping.1
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como fingerprinting).
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.



Fuente: Aplicación Vega

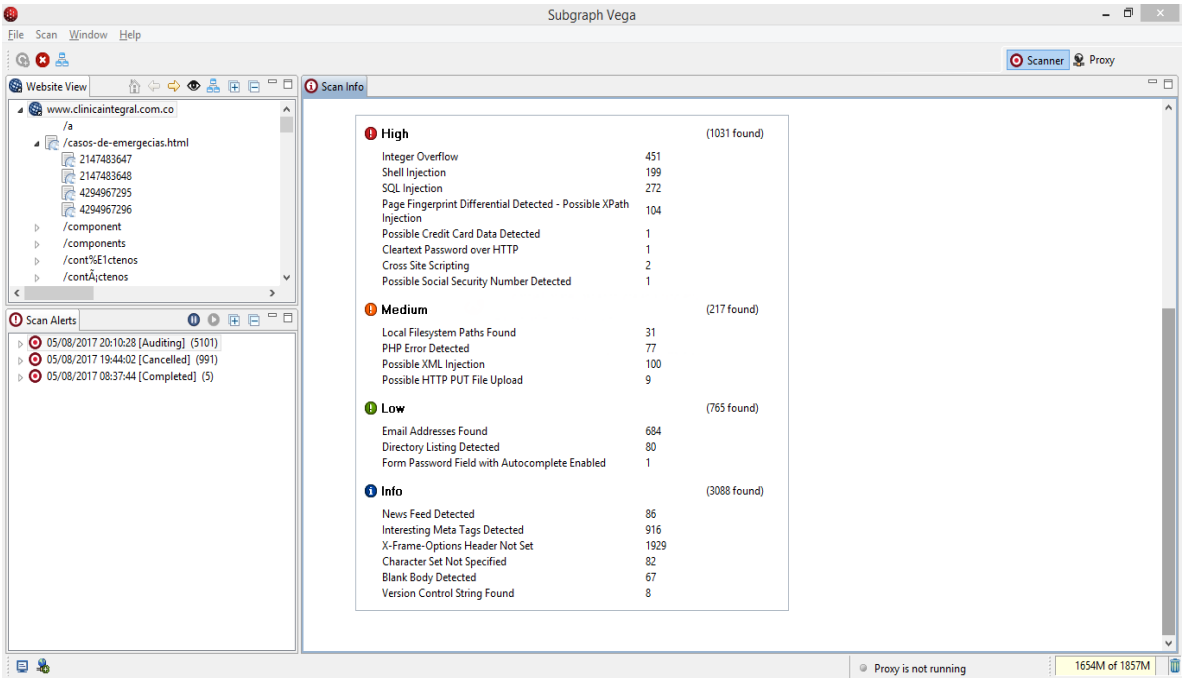
RESULTADO DE PRUEBAS CON VEGA VULNERABILITY SCANNER

Se realizó la prueba de penetración del sistema obteniendo los siguientes resultados de vulnerabilidades halladas de Alto, Mediano y Bajo impacto. Además de obtener el número y tipo de vulnerabilidades se explica el impacto que estás tienen en el sistema y cuál es la recomendación para solucionar dichas vulnerabilidades.

RESULTADO DE ANÁLISIS DE VULNERABILIDADES VEGA VULNERABILITY SCANNER	
TIPO DE RIESGO	*CANTIDAD RIESGOS ENCONTRADOS*
ALTO	1031
MEDIANO	217
BAJO	765
TOTAL	**2013**

Fuente: El Autor

Se encontraron vulnerabilidades clasificados en los siguientes tipos tal como se detalla en la siguiente imagen capturada del resultado de análisis de la prueba realizada en el software.



Fuente: Aplicación Vega

A continuación, se explican algunas de las vulnerabilidades más importantes de las encontradas y clasificadas en riesgo alto, mediano y bajo.

- **ALTO RIESGO**

SQL INJECTION

En el análisis realizado se encontraron al menos 272 elementos de código del sistema en donde existe vulnerabilidad de este tipo.

El SQL Injection es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

Se produce una inyección SQL cuando, se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.

Este tipo de intrusión normalmente es de carácter malicioso, dañino o espía, por tanto, es un problema de seguridad informática, y debe ser tomado en cuenta por el programador de la aplicación para poder prevenirlo.

La intrusión ocurre durante la ejecución del programa vulnerable, ya sea, en computadores de escritorio o bien en sitios Web, en este último caso obviamente ejecutándose en el servidor que los aloja. La vulnerabilidad se puede producir automáticamente cuando un programa inserta una sentencia SQL en tiempo de ejecución, o bien durante la fase de desarrollo.

Al ejecutarse la consulta en la base de datos, el código SQL inyectado también se ejecutará y podría hacer un sinnúmero de cosas, como insertar registros, modificar o eliminar datos, autorizar accesos e, incluso, ejecutar otro tipo de código malicioso en el computador.

EJEMPLO TOMADO DEL ANÁLISIS

Classification	**Input Validation Error**
Resource	**http://www.clinicaintegral.com.co/**
Parameter	**Format**
Method	**GET**
Detection Type	**Blind Arithmetic Evaluation Differential**
Risk	**High**

Fuente: Aplicación Vega

SOLICITUD QUE CONTIENE VULNERABILIDAD

GET /?format=feed%200%200%20-%20-&type=atom

CODIGO QUE CONTIENE SOLICITUD

```
<!doctype html>
<html lang="en">
   <head>
      <meta charset="utf-8">
      <meta http-equiv="X-UA-Compatible" content="IE=edge">
      <title>500: Internal Error - HostGator</title>
      <meta name="description" content="">
      <meta name="viewport" content="width=device-width, initial-scale=1">
      <link rel="shortcut icon" type="image/x-icon" href="/img-sys/favicon.ico" />
 ...
```

Fuente: Aplicación Vega

DISCUSION

Vega ha detectado una posible vulnerabilidad de inyección SQL. Estas vulnerabilidades están presentes cuando se suministra desde el exterior una

entrada para construir una consulta SQL. Si no se toman precauciones, la entrada suministrada externamente (normalmente un parámetro GET o POST) puede modificar la cadena de consulta que realiza acciones de arranque. Estas acciones incluyen obtener lectura no autorizada o el acceso de escritura a los datos almacenados en la base de datos, así como modificar la lógica de la aplicación.

IMPACTO

- Estas vulnerabilidades pueden ser explotadas por atacantes remotos para obtener acceso de lectura o escritura no autorizado a la base de datos subyacente.

- La explotación de vulnerabilidades de inyección de SQL también puede permitir ataques contra la lógica de la aplicación.

- Los atacantes pueden obtener acceso no autorizado al servidor que aloja la base de datos.

SOLUCION

- El desarrollador debe revisar la solicitud y la respuesta contra el código para comprobar manualmente si existe una vulnerabilidad.

- La mejor defensa contra vulnerabilidades de inyección SQL es usar comandos parametrizados.

- Desinfectar las entradas puede evitar estas vulnerabilidades. Deben filtrarse las variables de tipo cadena de caracteres de escape, y los tipos numéricos deben controlarse para asegurar que sean válidos.

- Uso de procedimientos almacenados puede simplificar las consultas complejas y permitir la configuración de control de acceso más estricto.

- Controles de acceso a la configuración de la base de datos pueden limitar el impacto de las vulnerabilidades explotadas. Se trata de una estrategia de mitigación que se puede emplear en ambientes donde el código no es modificable.

- Mapeo objeto-relacional elimina la necesidad de SQL.

SHELL INJECTION:

Se registraron 199 elementos de código con vulnerabilidad de este tipo.

Vulnerabilidades de inyección de comandos ocurren a menudo cuando inadecuadamente higienizados datos externamente suministrados como parte de un comando del sistema ejecutado por un intérprete de comandos o shell. Vulnerabilidades como estos pueden ser explotadas mediante el uso de metacaracteres de shell para ejecutar comandos adicionales que no estaban destinados a ser ejecutadas por el desarrollador de aplicaciones. La función de system() y derivados, a menudo son responsables, ya que estas funciones son muy fáciles de usar. Estas vulnerabilidades pueden conceder acceso remoto a los atacantes, si explota con éxito.

EJEMPLO TOMADO DEL ANÁLISIS

Classification	Information
Resource	**/component/k2/**
Parameter	**Option**
Method	**POST**
Risk	**High**

Fuente: Aplicación Vega

COMANDO REQUERIDO

POST /component/k2/ [searchword=Buscar... task=search option=com_search"`true`" Itemid=0]

IMPACTO

- Atacante puede ser capaz de ejecutar comandos en el servidor.
- Explotación puede causar acceso remoto no autorizado.

SOLUCION

- Los desarrolladores deberían examinar el código correspondiente a la página en detalle para determinar si la vulnerabilidad existe.

- Debe evitarse la ejecución de comandos del sistema como con system() a través de un intérprete de comandos o Shell.

- Si es absolutamente necesario, el desarrollador debe tener especial cuidado con validar la entrada antes de que pase al intérprete de comando o Shell.

➢ **Possible Social Security Number Detected:**

Vega ha detectado un patrón numérico que empareja la estructura del número de seguro social en el contenido escaneado. Esto podría ser un falso positivo contra un patrón con las mismas características.

EJEMPLO DEL ANÁLISIS

Classification	**Information**
Risk	**High**

Fuente: Aplicación Vega

COMANDO REQUERIDO QUE CONTIENE LA VULNERABILIDAD

GET /index.php?option=com_contentmap&view=smartloader&type=json&filename=articlesmarkers&source=articles&owner=module&id=170%0A%20-->">'>'"&Itemid=245

CÓDIGO FUENTE CON SOLICITUD

462175302
471482865

Fuente: Aplicación Vega

IMPACTO

- Divulgación no autorizada de esta información podría conducir a fraude o robo de identidad.
- La divulgación no autorizada podría también conducir a sanciones reglamentarias.

SOLUCIÓN

- Esto debe ser investigado para identificar la naturaleza de los datos que el análisis ha detectado. La causa de la revelación podría ser datos de prueba, una base de datos de archivo plano o la activación de algunas vulnerabilidades inesperadas.

➢ **Possible Credit Card Data Detected:**

Vega ha detectado una secuencia de dígitos que tienen características similares a números de tarjeta de crédito. Esto debe revisarse cuidadosamente (se puede hacer mediante un examen de respuesta del servidor).

EJEMPLO TOMADO DEL ANÁLISIS

Classification	Personally Identifiable Information (PII)
Resource	**/templates/vina_medical/css/bootstrap-responsive.min.css**
Risk	**High**

Fuente: Aplicación Vega

COMANDO QUE CONTIENE LA VULNERABILIDAD

GET /templates/vina_medical/css/bootstrap-responsive.min.css

INFORMACIÓN OBTENIDA A PARTIR DEL ANÁLISIS

36370249136206

Fuente: Aplicación Vega

IMPACTO

- Vega ha detectado una secuencia de dígitos que tienen algunas de las propiedades de los números de tarjeta de crédito.

- La divulgación no autorizada de esta información podría conducir a fraude o robo de identidad.

- La divulgación no autorizada podría también conducir a sanciones reglamentarias.

SOLUCIÓN

- Esto debe ser investigado para identificar la naturaleza de los datos que el patrón de detección.

- La causa de una revelación podría ser datos de prueba, una base de datos de archivo plano o la activación de algunas vulnerabilidades inesperadas.

➢ **Page Fingerprint Differential Detected - Possible XPath Injection:**

Existen 104 elementos detectados en el análisis con posible vulnerabilidad de este tipo.

Vega ha detectado una huella de la página de respuesta en relación con una solicitud de inyección XPath. Esto significa que el contenido de la página de respuesta devuelto por la aplicación web tiene una firma diferente a una petición ordinaria, que puede indicar la existencia de una vulnerabilidad de inyección XPath. La huella de página diferente puede incluir mensajes de error o indicar un cambio de estado en la aplicación en respuesta a la tentativa de inyección XPath.

Los desarrolladores deben examinar el contenido de la respuesta y el código subyacente para verificar si es o no una vulnerabilidad presente. Si la vulnerabilidad existe y no se toman las precauciones, según la naturaleza de la consulta XPath afectada, esta vulnerabilidad podría permitir que atacantes omitir autenticación o ganar acceso no autorizado a datos XML.

EJEMPLO TOMADO DEL ANÁLISIS

Classification	Error Message
Resource	**/component/search/**
Parameter	**areas[]**
Method	**POST**
Detection Type	**XPath 2.0 Blind Injection Differential Checks**
Risk	**High**

Fuente: Aplicación Vega

COMANDO REQUERIDO CON POSIBLE VULNERABILIDAD

POST /component/search/ [searchword=Buscar... Search=vega task=search searchphrase=all searchphrase=any searchphrase=exact ordering=1 areas[]=on areas[]=on areas[]=on areas[]=e' or 1 eq 1 or 'a' = 'a areas[]=on areas[]=on areas[]=on limit=1]

IMPACTO

- Vega ha detectado una huella diferente respuesta en relación con un intento de inyección XPath.

- Esto puede indicar una vulnerabilidad de inyección XPath, aunque esto no está confirmado.

- Si esto es debido a una vulnerabilidad de XPath, dependiendo de la naturaleza de la consulta XPath, explotación podría permitir que atacantes omitir autenticación o ganar acceso no autorizado a datos XML.

SOLUCION

- Para evitar este tipo de vulnerabilidad, el desarrollador debe considerar adoptar el uso de declaraciones XPath precompiladas u opciones de parametrización de consultas.

➢ **Cross Site Scripting:**

Cross-site scripting (XSS) es una clase de vulnerabilidades que afectan a las aplicaciones web que pueden resultar en controles de seguridad implementados en los navegadores que se eluden. Cuando un navegador visita una página de un sitio web, el código de script que se origina en el dominio del sitio web puede acceder y manipular el DOM (modelo de objeto de documento), una representación de la página y sus propiedades en el navegador. Código de script de otro sitio web no puede. Esto se conoce como "la misma política de origen", un control crítico en el modelo de seguridad del navegador. Las vulnerabilidades de secuencias de comandos entre sitios se producen cuando la falta de validación de entrada permite a los usuarios inyectar código de secuencia de comandos en el sitio web de destino de manera que se ejecute en el explorador de otro usuario que visite el mismo sitio web. Esto evadiría la política del mismo origen del navegador porque el navegador no tiene forma de distinguir el código de script auténtico de no auténtico, aparte de su origen.

EJEMPLO TOMADO DEL ANÁLISIS

Classification	Input Validation Error
Resource	**/component/users/2147483647.html**
Parameter	**Return**
Method	**GET**
Risk	**High**

Fuente: Aplicación Vega

COMANDO CON POSIBLE VULNERABILIDAD

GET/component/users/2147483647.html?return=aHR0cDovL3d3dy5jbGluaWNhaW50ZWdyYWwuY29tLmNvL21lZGlhL2syL2Fzc2V0cy9qcy9pbmRleC5waHA/b3B0aW9uPWNvbV9rMiZ2aWV3PW1lZGlhJnR5cGU9YXR0YWNobWVudCZ0bXBsPWNvbXBvbmVudCZmaWVsZElEPWsyQWN0aXZlQXR0YWNobWVudA==-->">'>'"

IMPACTO

El impacto preciso depende en gran medida de la aplicación.

- XSS es generalmente una amenaza para las aplicaciones web que tienen usuarios autenticados o son sensibles a la seguridad.

- El código malicioso puede manipular el contenido del sitio, cambiando su aspecto y / o función para otro usuario. Esto incluye modificar el comportamiento de la aplicación web (como redireccionar formularios, etc.).

- El código también puede ser capaz de realizar acciones dentro de la aplicación sin el conocimiento del usuario.

- El código de secuencia de comandos también puede obtener y retransmitir valores de cookies si no se han establecido HttpOnly.

SOLUCION

- El desarrollador debe identificar la manera en que los datos no confiables se envían al cliente sin filtrar adecuadamente.

- Hay varias técnicas específicas de lenguaje / plataforma para filtrar datos no fiables.

- Las reglas generales para prevenir XSS se pueden encontrar en la hoja de trucos recomendada para la prevención de XSS de OWASP.

- Obtener y retransmitir valores de cookie si no se han establecido HttpOnly.

- **MEDIADO RIESGO**

➢ **Local Filesystem Paths Found:**

Vega ha detectado una posible ruta absoluta del sistema de archivos (es decir, una que no es relativa a la raíz de la web). Esta información es sensible, ya que puede revelar cosas sobre el entorno del servidor a un atacante. Conocer el diseño del sistema de archivos puede aumentar las posibilidades de éxito de los ataques ciegos. Las rutas completas del sistema se encuentran muy a menudo en la salida de errores. Esta salida nunca debe ser enviada a los clientes en los sistemas de producción. Debe ser redireccionado a otro canal de salida (como un registro de errores) para su análisis por los desarrolladores y administradores del sistema.

EJEMPLO TOMADO DEL ANÁLISIS

Classification	Information
Resource	**/index.php**
Risk	Medium

Fuente: Aplicación Vega

COMANDO REQUERIDO CON POSIBLE VULNERABILIDAD

GET /index.php?option=com_contentmap&view=smartloader&type=js&filename=map-->">'>'"&owner=module&id=170&Itemid=245

CONTENIDO DEL CÓDIGO

```
/lib/php /opt/php
```

Fuente: Aplicación Vega

IMPACTO

- Vega ha detectado lo que pueden ser rutas absolutas del sistema de archivos en el contenido escaneado.

- La revelación de estas rutas revela información sobre el diseño del sistema de archivos.

- Esta información puede ser sensible, su divulgación puede aumentar las posibilidades de éxito de otros ataques.

SOLUCIÓN

- Las trayectorias absolutas se encuentran a menudo en la salida del error.

- Tanto los administradores del sistema como los desarrolladores deben estar informados, ya que el problema puede deberse a un error de aplicación o una configuración incorrecta del servidor.

- La salida de error que contiene información confidencial, como rutas de sistema absolutas, no se debe enviar a clientes remotos en servidores de producción.

- Esta salida se debe enviar a otro flujo de salida, como un registro de errores.

➢ **PHP Error Detected**

Se ha detectado firmas en contenido escaneado que coinciden con páginas de error comunes de PHP. Estas páginas se generan automáticamente cuando ocurre un error y pueden generar información útil en ataques más sofisticados. Se recomienda que la salida de errores no se envíe al cliente en sistemas de producción.

EJEMPLO TOMADO DEL ANÁLISIS

Classification	Information
Resource	**/index.php**
Risk	Medium

Fuente: Aplicación Vega

COMANDO REQUERIDO DONDE EXISTE POSIBLE VULNERABILIDAD

GET /index.php?option=com_contentmap&view=smartloader&type=json&filename=articlesmarkers&source=articles&owner=module&id=170%0A%20-->">'>'"&Itemid=245

CODIGO

```
<b>Warning</b>: session_start(): Trying to destroy uninitialized session in <b>/home4/ab92565/public_html/libraries/joomla/session/session.php</b> on line <b>
```

Fuente: Aplicación Vega

IMPACTO

- Vega ha detectado la firma de una página de error de PHP.

- Las páginas de error generadas automáticamente pueden transmitir información confidencial.

- La información filtrada puede incluir los niveles de revisión de software, los parámetros de configuración y la estructura de la base de datos o del sistema de archivos.

SOLUCIÓN

- El manual de PHP recomienda desactivar "display_errors" en los servidores expuestos a Internet. Para PHP 5.2.4 o superior, la configuración "display_errors" en el archivo de configuración "php.ini" debería establecerse en "stderr" (flujo de salida de error), en lugar de "stdout" (flujo de salida enviado a los clientes). Para versiones anteriores, "display_errors" es un tipo booleano, y se puede establecer en "False" para deshabilitar. La configuración también se puede desactivar en tiempo de ejecución utilizando ini_set () desde un script PHP.

➢ **Possible HTTP PUT File Upload**

El método HTTP PUT fue diseñado para permitir que los clientes HTTP almacenen recursos en un servidor HTTP. En las implementaciones, esto suele significar capacidad de carga de archivos. Como el HTTP RFC establece que un servidor debería sobrescribir los recursos preexistentes ubicados en el URI de una petición PUT, podría ocurrir una pérdida de integridad del sistema o de la aplicación si se realizara tal solicitud.

EJEMPLO TOMADO DEL ANÁLISIS

Classification	Configuration
Resource	http://www.clinicaintegral.com.co/component/PUT-putfile
Parameter	**Return**
Method	**PUT**
Risk	**Medium**

Fuente: Aplicación Vega

COMANDO REQUERIDO CON POSIBLE VULNERABILIDAD

PUT /component/PUT-putfile

IMPACTO

- Las subidas arbitrarias de archivos podrían afectar la integridad de la aplicación o del sistema.
- Esto podría ocurrir si un atacante sobrescribiera un recurso preexistente en el servidor.

SOLUCIÓN

- Los parámetros de configuración del servidor deben revisarse para identificar y deshabilitar la configuración incorrecta.

Apache permite que métodos como PUT y DELETE se restrinjan usando la directiva LIMIT.

➢ **Possible XML Injection**

Vega ha detectado una posible vulnerabilidad de inyección XML. La inyección de XML puede ocurrir cuando los datos suministrados externamente que no han sido suficientemente validados se utilizan para crear un documento XML. Es posible que estos datos corrompan la estructura de los documentos. Las posibles consecuencias dependen del documento XML y de su uso.

EJEMPLO TOMADO DEL ANÁLISIS

Classification	**Input Validation Error**
Resource	**/component/users/**
Parameter	**Username**
Method	**POST**
Risk	Medium

Fuente: El Autor

COMANDO REQUERIDO CON POSIBLE VULNERABILIDAD

POST /component/users/ [username=vega>'>"> password=vega return=aHR0cDovL3d3dy5jbGluaWNhaW50ZWdyYWwuY29tLmNvL21lZGlhL2syL2Fzc2V0cy9qcy9pbmRleC5waHA/b3B0aW9uPWNvbV9rMiZ2aWV3PW1lZGlhJnR5cGU9YXR0YWNobWVudCZ0bXBsPWNvbXBvbmVudCZmaWVsZElEPWsyQWN0aXZlQXR0YWNobWVudAunamc= 044716256f014353da1c96947845ca26=1]

IMPACTO

- Vega ha detectado que es posible corromper la estructura de un documento XML del lado del servidor.

- Esto podría afectar la lógica de la aplicación, dependiendo de cómo se utilice el documento XML.

- Una vulnerabilidad de inyección de XML puede conducir a una pérdida de integridad de los datos utilizados o almacenados por la aplicación. XML puede ser un vector de inyección que ignore los filtros de contenido (por ejemplo, incluyendo javascript en una sección CDATA).

SOLUCIÓN

- Los desarrolladores deben investigar el código para verificar manualmente que existe una vulnerabilidad de inyección XML.

- Los caracteres que se pueden interpretar como XML deben ser filtrados.

RIESGO BAJO

➢ **Directory Listing Detected:**

Listado del contenido del directorio cuando no hay ningún archivo de índice presente en una configuración errónea común. El contenido del directorio puede proporcionar información útil a un atacante, especialmente si hay archivos que no están destinados a ser accesibles, como código fuente o copias de seguridad. La lista de directorios también puede proporcionar información útil sobre los hábitos de la administración de servidores y / o desarrolladores web, como la convención de nomenclatura de archivos, que podría usarse para aumentar el éxito probable de ataques de fuerza bruta u otros.

EJEMPLO TOMADO DEL ANÁLISIS

Classification	**Configuration Error**
Resource	**/plugins/system/jcemediabox/**
Risk	Low

Fuente: Aplicación Vega

COMANDO REQUERIDO CON POSIBLE VULNERABILIDAD

GET /plugins/system/jcemediabox/

CODIGO

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /plugins/system/jcemediabox</title>
 </head>
 <body>
<h1>Index of /plugins/system/jcemediabox</h1>
<ul><li><a href="/plugins/system/"> Parent Directory</a></li>
<li><a href="addons/"> addons/</a></li>
<li><a href="css/"> css/</a></li>
<li><a href="elements/"> elements/</a></li>
<li><a href="img/"> img/</a></li...
```

Fuente: Aplicación Vega

IMPACTO

- El servidor emite el contenido de los directorios. Esto podría exponer archivos no destinados a la recuperación del usuario (antiguos archivos htaccess, copias de seguridad, código fuente).

- La lista de directorios también puede proporcionar información útil sobre el diseño y las características del sistema, como las convenciones de nomenclatura utilizadas por los desarrolladores y administradores.

- Esta información puede aumentar la probabilidad de éxito de los ataques ciegos y la adivinación de la fuerza bruta.

SOLUCION

- Para Apache, realice una de las acciones siguientes: agregue "IndexIgnore *" al archivo .htaccess del directorio o, alternativamente, quite "Índices" de la línea

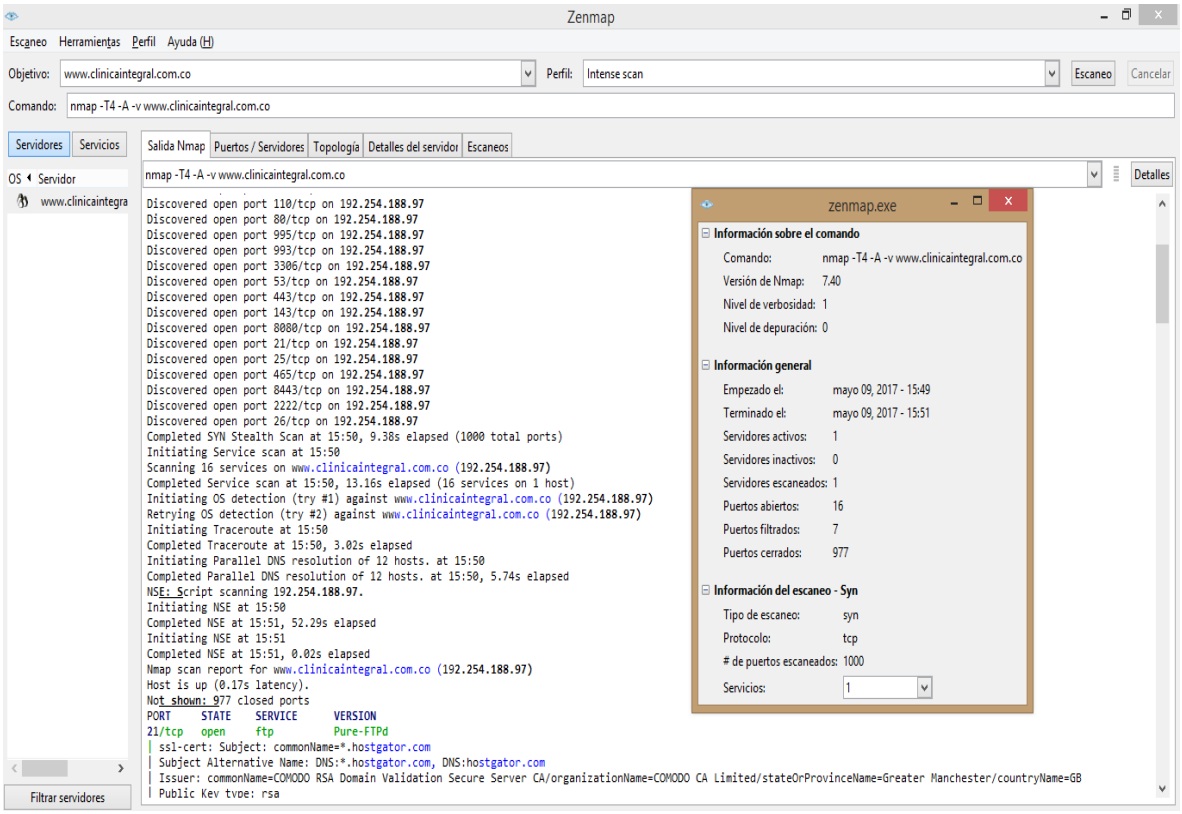
"Opciones Todos los índices FollowSymLinks MultiViews" en el archivo de configuración de Apache.

• Para lighttpd, cambie "dir-listing.activate =" enable "" a "dir-listing.activate =" disable "" en su archivo de configuración de lighttpd.

RESULTADOS DE PRUEBAS CON NMAP

Con el análisis realizado con esta herramienta se obtuvieron resultados acerca del listado de puertos abiertos en el sistema (que pueden ser usados por atacantes como puerta de entrada trasera para ingresar al sistema), la topología de la red, información posible acerca del sistema operativo y demás información acerca del servidor y la respectiva dirección IP del sistema.

A continuación, se anexan los captures con la respectiva información obtenida.

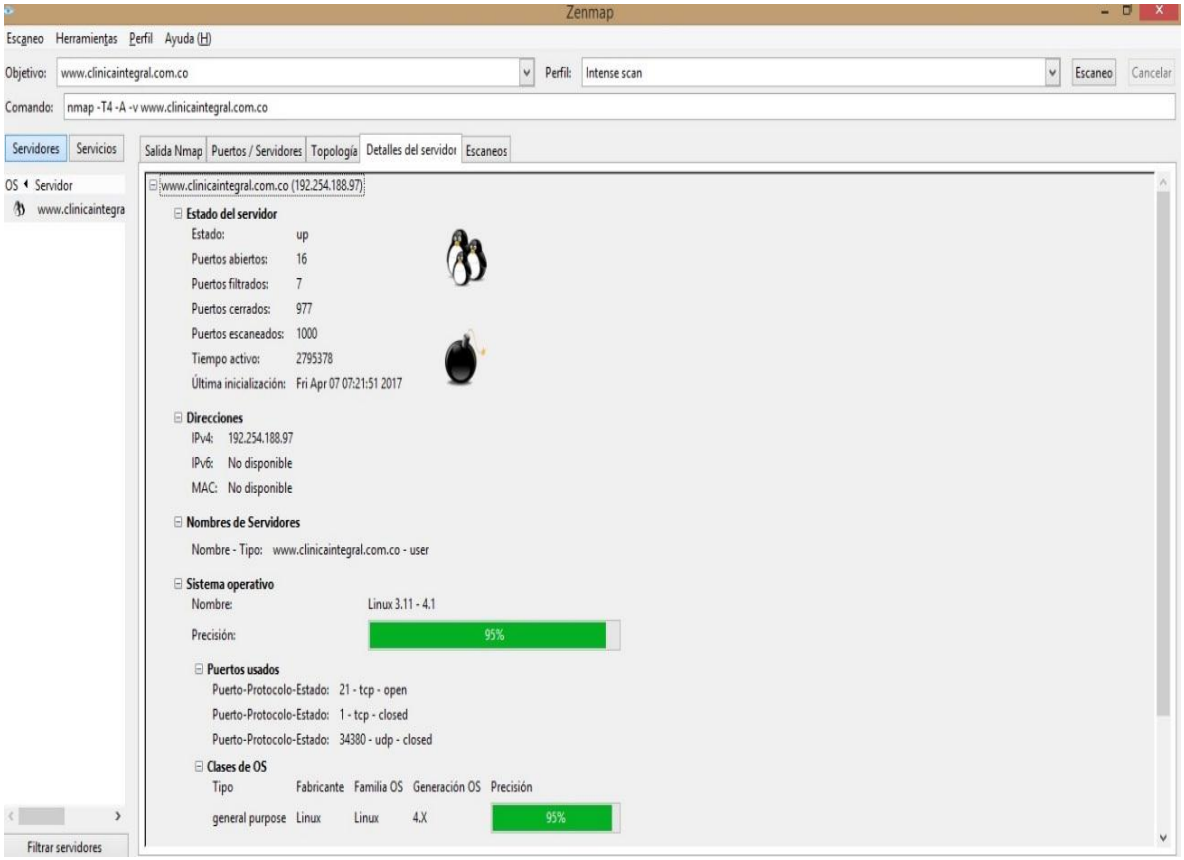


Fuente: Aplicación nmap

NOTA: Como se muestra en el capture tan solo se usó la dirección web del sitio para realizar el análisis y obtener toda la información detallada en adelante.

POSIBLE INFORMACIÓN ACERCA DEL SERVIDOR

Se obtuvo información con una precisión del 95% en lo que respecta a la detección del sistema operativo usado por el servidor donde está alojado el sistema web objeto del análisis.

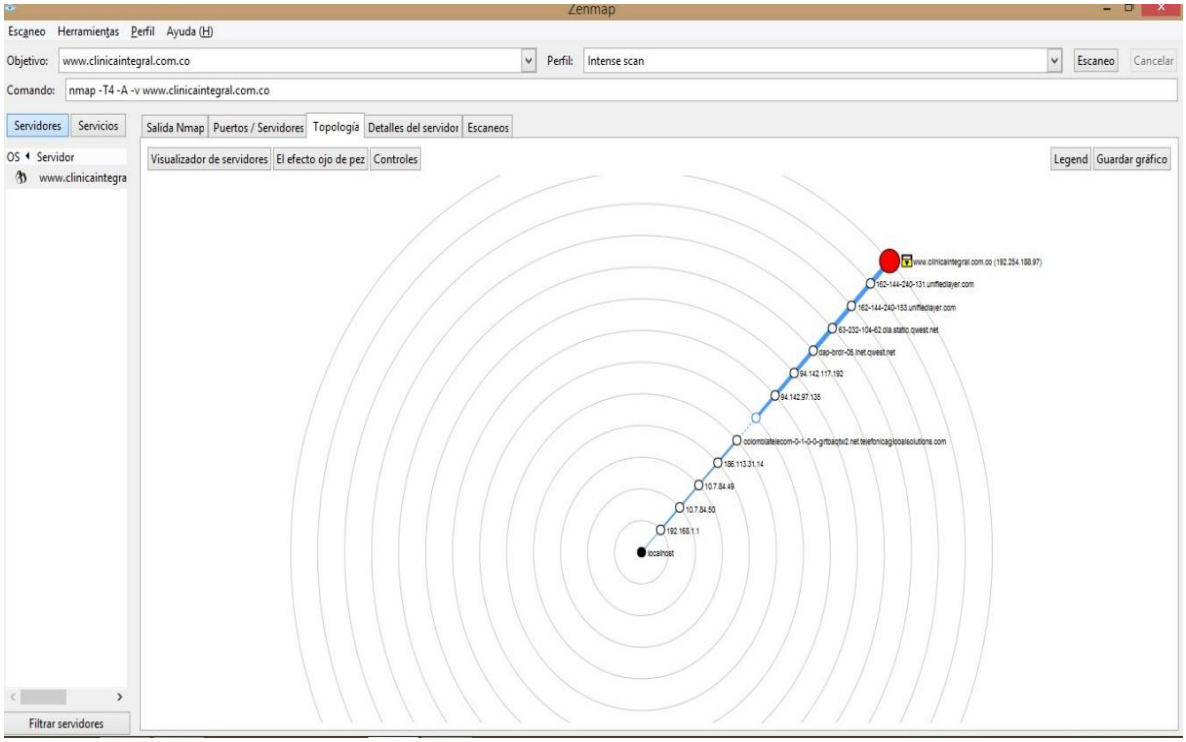


Fuente: Aplicación nmap

Como se puede observar a través del análisis con la herramienta se obtuvo una precisión del 95% que el posible sistema operativo usado por el servidor es de la familia de OS Linux Generación 4.x

TOPOLOGIA DE LA RED

Se pudo obtener que la Topología de la Red en donde está alojado el sistema web.



Fuente: Aplicación nmap

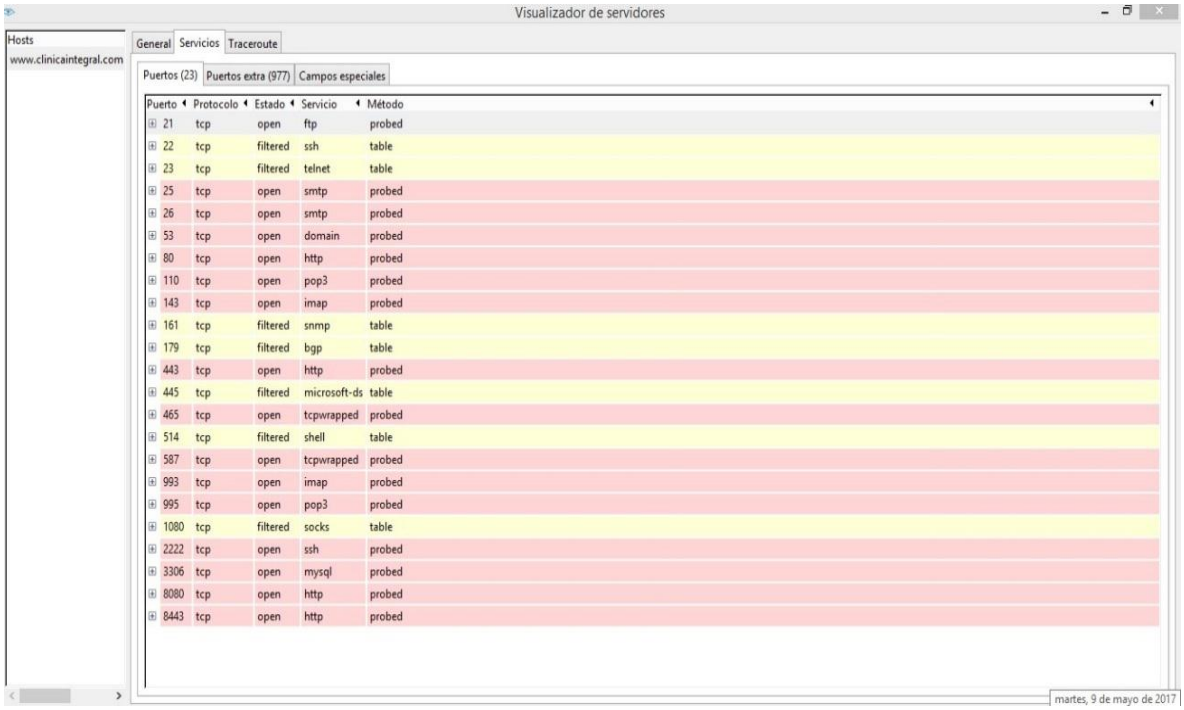
Gracias a la topología se pudo obtener la dirección IP del servidor en donde está alojado el sistema; siendo la IP 192.254.188.97 la dirección del dominio www.clinicaintegral.com.co

PUERTOS ABIERTOS

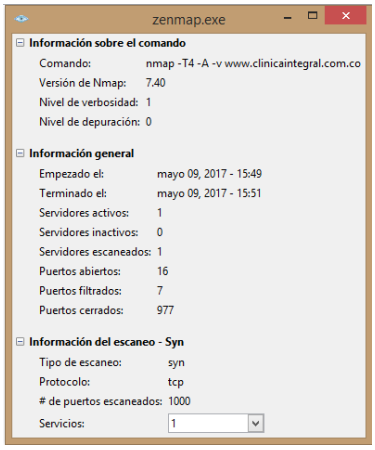
Gracias al análisis realizado por la herramienta se pudo obtener un listado puertos abiertos en el sistema y el tipo de protocolo que los utiliza.

Desde el punto de vista de seguridad, es recomendable permitir el acceso sólo a los servicios que solo son necesarios, pues cualquier servicio expuesto a Internet es un punto de acceso potencial para intrusos. Por otra parte, es recomendable bloquear aquellos puertos que no se estén siendo usados para no dar facilidades a los hackers quienes hacen escaneos aleatorios de IPs y puertos por Internet, intentando identificar las características de los sistemas conectados, y creando bases de datos con estas.

A continuación, listado de puertos abiertos obtenidos a partir del análisis.



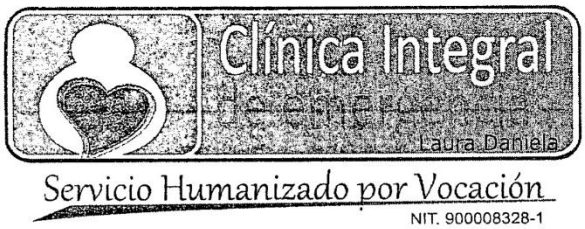
Fuente: Aplicación nmap



Fuente: Aplicación nmap

De este analisis se pudo determinar que existen 16 puertos abiertos que pueden ser explotados por hackers informáticos como puerta de ingreso para obtener información del sistema, por lo que se deben tomar las medidas correctivas al respecto.

ANEXO D. Carta de Autorización para realizar la Investigación



Valledupar 28 de marzo 2017

Señor
NEHEMIAS SARABIA DIAZ
Estudiante Especialización en Seguridad Informática
Universidad Nacional Abierta y a Distancia UNAD
Ciudad.

ASUNTO: autorizacion de ingreso

Por medio de la presente y de a cuerdo con su solicitud, se autoriza el ingreso a la institución al antes mencionado, para realizar investigación academica titulado **AUDITORIAS AL SISTEMAS DE INFORMACION DE LA CLINICA LAURA DANIELA**, bajo la supervicion del Ingeniero Carlos Mena Medina.

Gracias por la tencion prestada.

Coordialmenrte,

LINA TATIANA FERNANDEZ BARBOSA
Coordinadora de Gestión Humana.

03/04/17.

CARRERA 19 N0 14 -47 BARRIO SAN VICENTE PBX 5803535-5803636 EXT 107
E- mail: gestionhumanacld@gmail.com
VALLEDUPAR-CESAR

ANEXO E. Formato de Encuesta

ENCUESTA A REALIZAR AL PERSONAL QUE MANEJA EL SISTEMA DE INFORMACION KRYSTALOS EN LA CLINICA LAURA DANIELA

Objetivo: Determinar los diferentes riesgos que atentan contra la integridad del Sistema de Información KRYSTALOS.

CARGO: _____

Señale con una X los riesgos que usted considere que presenta el Sistema de Información Krystalos.

Emisión de datos incorrectos _____

Perdida de información _____

Sustracción de información _____

Divulgación de datos confidenciales _____

Inconsistencia de los datos procesados _____

Faltas en la emisión de reportes _____

Información desactualizada referente a los usuarios _____

Lentitud en los módulos de captura y procesamiento _____

Falta de filtros y consultas detalladas en la Base de Datos _____

Cruce de tablas _____

Faltas en la comunicación con el servidor en la Base de Datos _____

Fácil acceso de intrusos al sistema _____

Fallas en el hardware _____

Fallas en las conexiones eléctricas _____

Ausencia de políticas de seguridad _____

Inexistencia de fuentes del sistema _____

Falta de actualización o reingeniería del sistema _____

Ausencia del soporte y mantenimiento a equipos _____

Mencione que otros riesgos afectan el Sistema de Información Krystalos aparte de los señalados en el primer inciso.

_____

_____

_____

_____

ANEXO F. Formato de Entrevista 1

ENTREVISTA A REALIZAR AL PERSONAL QUE MANEJA EL SISTEMA DE INFORMACION KRYSTALOS EN LA CLINICA LAURA DANIELA

Objetivo: Determinar el funcionamiento general del sistema de información KRYSTALOS.

1. ¿Considera que todos los datos enviados y emitidos por la aplicación KRYSTALOS son válidos y confiables?

SI_____ NO_____ ALGUNOS_____

2. ¿El sistema de información KRYSTALOS valida todas las entradas de datos ingresadas por el usuario?

SI_____ NO_____ ALGUNOS_____

3. ¿Contiene KRYSTALOS una interfaz amigable para el usuario?

SI_____ NO_____ UN POCO _____

4. ¿Se le brinda la capacitación adecuada, completa y oportuna a las personas que ingresan a manejar el software dentro de la empresa?

SI_____ NO_____ ALGUNAS VECES_____

5. ¿Se encuentran con frecuencia errores de procedimiento dentro del programa KRYSTALOS?

SI_____ NO_____ ALGUNAS VECES_____

6. ¿Existen procedimientos para comparar las entradas con las salidas emitidas o procesadas por el sistema?

SI_____ NO_____ ALGUNOS_____

7. ¿Los errores e inconsistencias de las entradas y las salidas se prevén con procedimientos de control que aseguran la efectiva detección y posterior corrección de los datos?

SI_____ NO_____ ALGUNOS_____

8. ¿La empresa ha tomado medidas para eliminar los errores emitidos por KRYSTALOS?

SI_____ NO_____ ALGUNOS_____

9. ¿El sistema envía mensajes de error o advertencia cuando ocurre un mal procedimiento efectuado por el usuario?

SI_____ NO_____ ALGUNAS VECES_____

10. ¿Se corrigen errores de procedimiento antes de generar los archivos planos y enviar cuentas de cobro a las entidades que se les prestan servicios?

SI_____ NO_____ ALGUNOS_____

11. ¿Están debidamente documentados todos los módulos que posee KRYSTALOS?

SI_____ NO_____ ALGUNOS_____

12. ¿Las entradas de datos al software KRYSTALOS se hacen desde terminales debidamente autorizadas?

SI_____ NO_____ ALGUNOS_____

ANEXO G. Formato de Entrevista 2

ENTREVISTA A REALIZAR AL PERSONAL QUE MANEJA EL SISTEMA DE INFORMACION KRYSTALOSEN LA CLINICA LAURA DANIELA

Objetivo: Determinar el grado de importancia que tiene la implementación de la herramienta KRYSTALOS en la optimización de los procesos en la Clínica Laura Daniela de Valledupar.

1. ¿Conoce usted en general el funcionamiento del software que maneja?

SI_____ NO_____

2. ¿Cómo funcionario de la Clínica Laura Daniela considera que es importante contar con un sistema de información para optimizar los procesos que aquí se realizan?

SI_____ NO_____

¿Por qué?

_____

_____

_____

3. ¿Ha detectado usted fallas en la aplicación?

SI_____ NO_____ ALGUNAS VECES_____

4. ¿Considera usted que algunas de las fallas presentadas en el aplicativo se debe a la falta de cuidado al momento de ingresar la información?

SI_____ NO_____ ALGUNAS VECES_____

¿Cuáles?

_____

_____

5. ¿Identifica los errores que comete al ingresar datos al sistema de información y los corrige?

SI_____ NO_____ ALGUNAS VECES_____

¿Por qué?

_____

_____

_____

6. ¿Cree usted que la realización de una auditoria al sistema d información que maneja actualmente es necesaria?

SI_____ NO_____ ALGUNAS VECES_____

¿Por qué?

_____

_____

_____

7. ¿Qué sugerencias propone usted para mejorar el funcionamiento de la aplicación KRYSTALOS en la Clínica Laura Daniela?

_____

_____

_____

ANEXO H. Formato de Encuesta 2

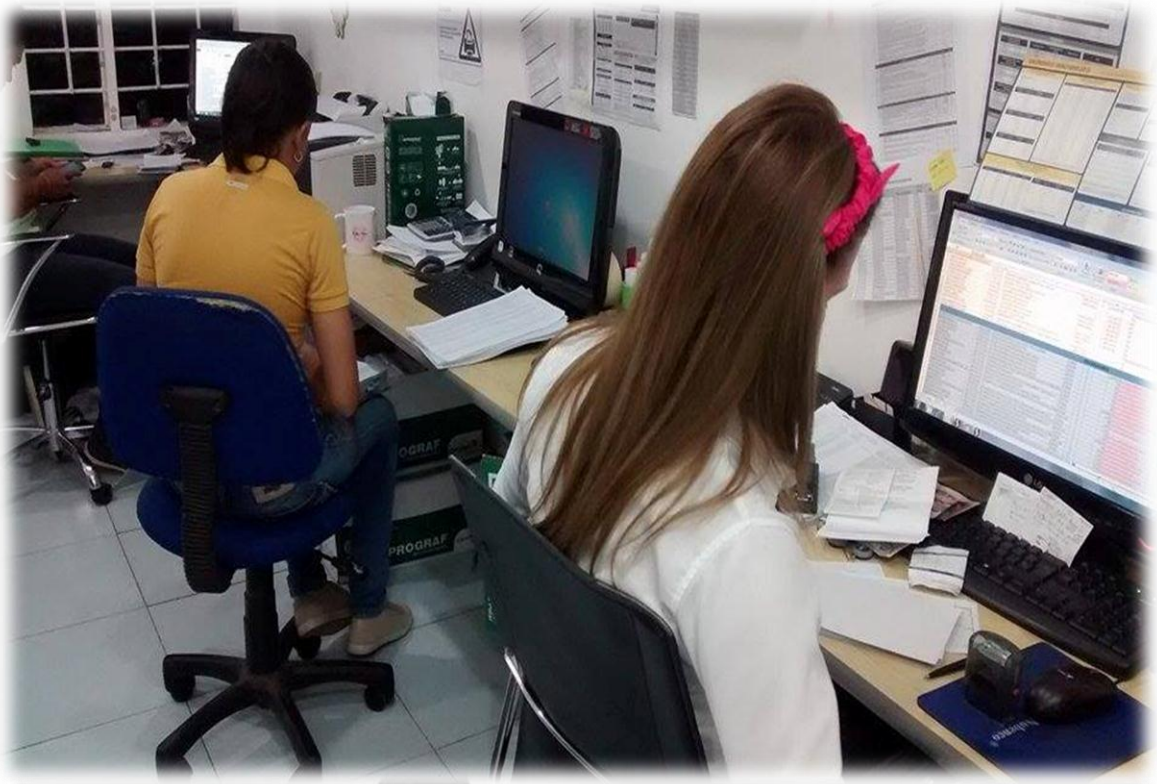
CUESTIONARIO DE PREGUNTAS A REALIZAR A LOS FUNCIONARIOS DEL AREA DE SISTEMAS DE LA CLINICA LAURA DANIELA MARQUE CON UNA X LA RESPUESTA QUE USTED CONSIDERE ACERTADA

PREGUNTAS	SI	NO	N/A
1. ¿Se han adoptado medidas de seguridad en el sistema de información KRYSTALOS?			
2. ¿Existe una persona responsable de la seguridad del sistema de información?			
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?			
4. ¿Existe personal de vigilancia en la Clínica Laura Daniela de Valledupar?			
5. ¿Existe una clara definición de funciones entre los puestos clave?			
6. ¿Se controla el trabajo fuera de horario?			
7. ¿Se registran las acciones de los operadores para evitar que realicen algunas acciones que puedan causar daños en los sistemas?			
8. ¿Se han adoptado políticas de seguridad en el manejo de contraseñas a los encargados de manejar el sistema de información?			
9. ¿Se permite a los programadores, analistas y operadores acceder a los archivos y programas?			
10. ¿Se han instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?			
11. ¿Se ha auditado alguna vez el centro de cómputo?			
12. ¿Son controladas las visitas y demostraciones en el centro de cómputo?			

13. ¿Se registra el acceso al departamento de cómputo por parte de personas ajenas a la dirección de informática?			
14. ¿Se vigila la moral y comportamiento del personal de la dirección de información con el fin de mantener una buena imagen y evitar un posible fraude?			
15. ¿La empresa dispone de extintores en el área de sistemas?			
16. ¿Se aplican políticas de seguridad en el área de cómputo?			
17. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?			
18. ¿Existe departamento de auditoria interna en la empresa?			
19. ¿Se auditan los sistemas en operación?			
20. ¿Se mantienen un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos?			
21. ¿Los operadores del equipo central están entrenados para recuperar o restaurar información en caso de destrucción de archivos?			
22. ¿Se han contratado pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación?			
23. ¿Existen políticas de seguridad que garanticen el buen funcionamiento del sistema de información?			
24. ¿Se hacen monitoreo constantes al sistema de información?			

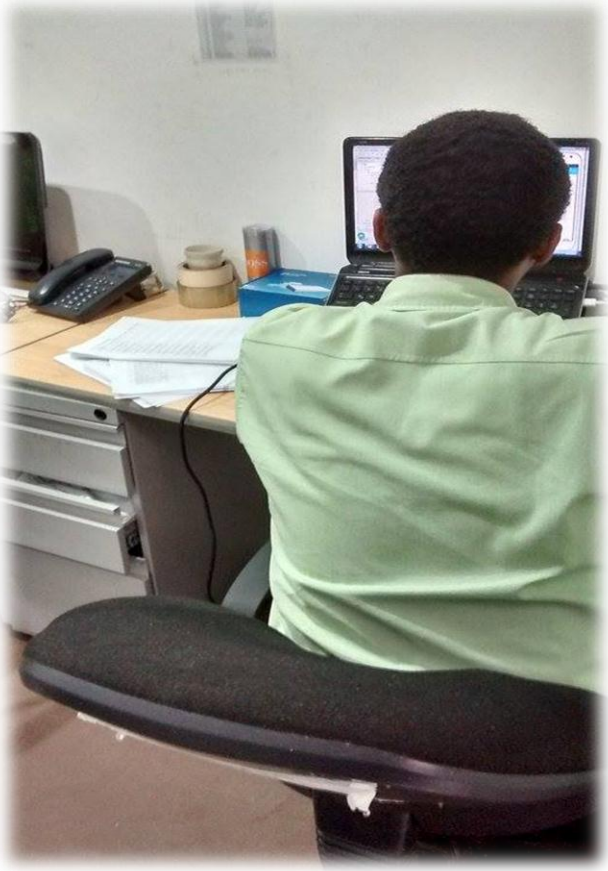
ANEXO I. Evidencias Fotográficas

Area de Facturación



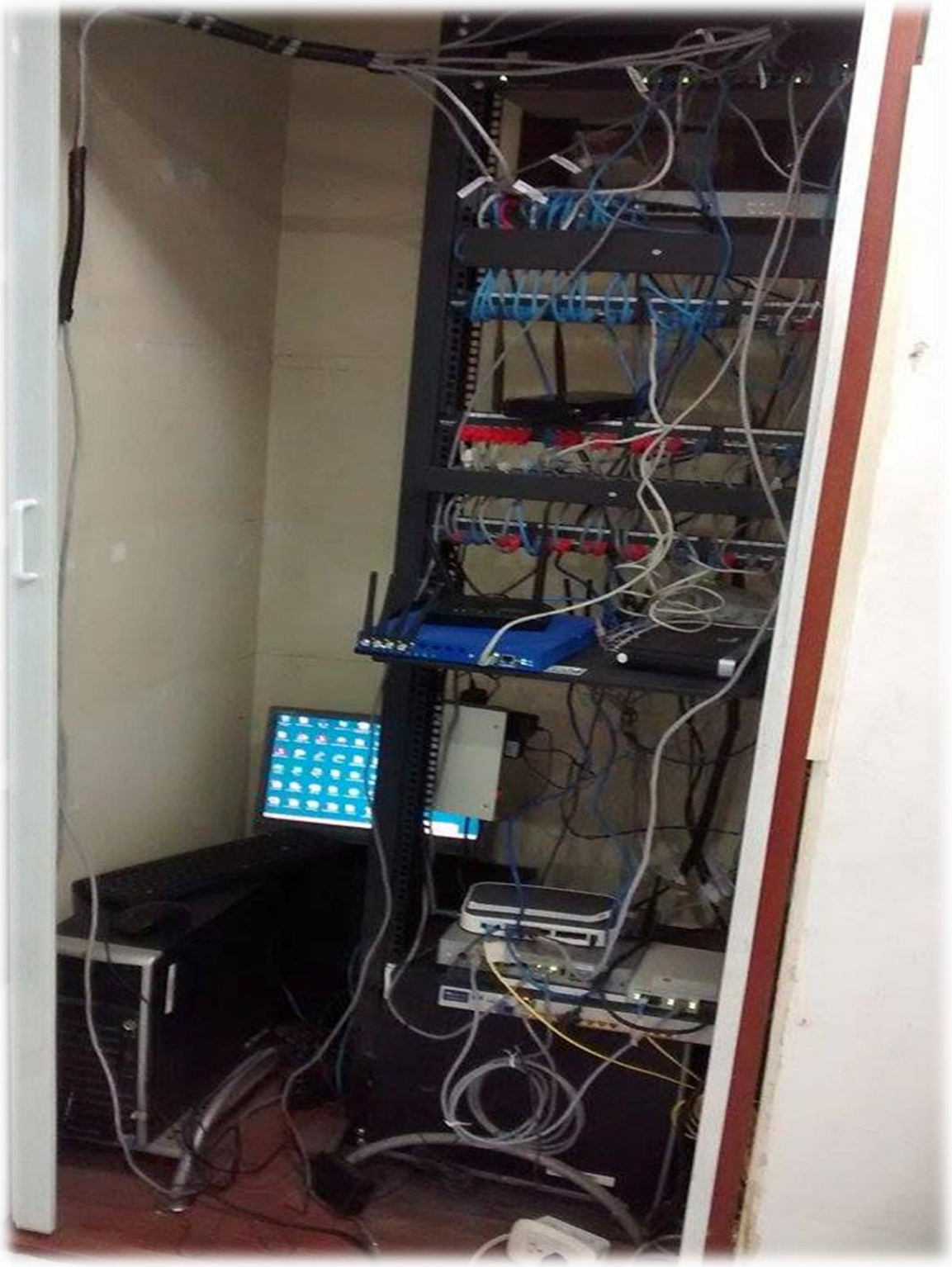
Fuente: El Autor

Area de Sistemas



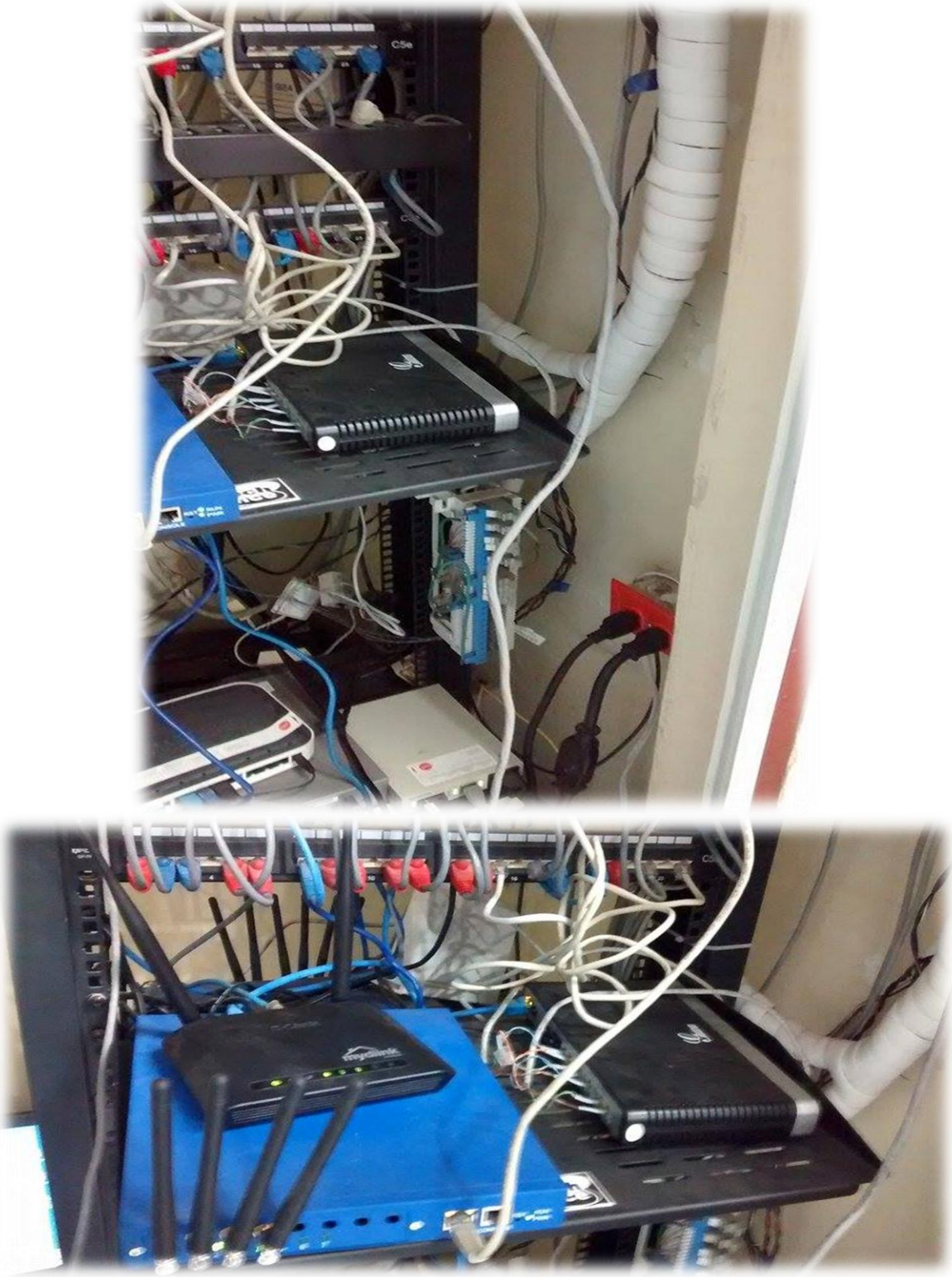
Fuente: El Autor

Rack de comunicaciones



Fuente: El Autor

Rack de comunicaciones



Fuente: El Autor

Vista cableado

Fuente: El Autor

ANEXO J. RESUMEN ANALITICO EDUCATIVO (RAE)

TÍTULO DEL DOCUMENTO	AUDITORIA AL SISTEMA DE INFORMACION DE LA CLINICA LAURA DANIELA DE LA CIUDAD DE VALLEDUPÁR
AUTOR	SARABIA DIAZ, Nehemías
AÑO DE LA PUBLICACIÓN	2017
DESCRIPCIÓN: Trabajo de grado desarrollado con el objetivo de auditar el sistema de información de la clínica Laura Daniela de la ciudad de Valledupar.	
PALABRAS CLAVES	Auditoria, Seguridad de la Información, Norma NTC ISO 27001:2013, Krystalos, Metodología Magerit.
FORMULACIÓN DEL PROBLEMA: ¿De qué manera la realización de una auditoría de sistemas de información, contribuirá al mejoramiento de los procesos para garantizar la integridad, confiabilidad, seguridad y confidencialidad de los datos en la clínica Laura Daniela?	
OBJETIVO GENERAL Realizar una auditoría al sistema de información de la clínica Laura Daniela de la ciudad de Valledupar en el marco de la norma NTC-ISO/IEC 27001 y el referente metodológico *Magerit* para el mejoramiento de los procesos garantizando la integridad, confiabilidad, seguridad y confidencialidad de los datos. **OBJETIVOS ESPECÍFICOS** • Identificar los componentes del sistema de información actual mediante revisión documental y entrevistas para establecer el plan de auditoria a desarrollar en la clínica Laura Daniela de la ciudad de Valledupar. • Realizar las pruebas de auditorías mediante la metodología de análisis y gestión de riesgos *Magerit* y herramientas de *petesting* para determinar los riesgos presentes en la clínica Laura Daniela de la ciudad de Valledupar. • Formular el informe de auditoría, recomendando los controles adecuados para el tratamiento de los riesgos según los parámetros de la norma ISO 27001, describiendo las recomendaciones y conclusiones.	
CONTENIDO: El punto de partida en este proyecto fue el conocimiento general acerca de la Clínica Laura Daniela de la ciudad de Valledupar, con el fin de obtener y presentar aspectos relacionados con las áreas legal, comercial e institucional. De igual manera, se realizará un análisis detallado de la aplicación	

Krystalos en sus procedimientos de manejo y control de los datos; y asociado a éste, se realizará un estudio alrededor de los elementos involucrados en el almacenamiento, procesamiento y distribución de la información.

El paso siguiente fue establecer los objetivos, los cuales permitirán obtener pautas claras en la realización de la investigación y enmarcarán la dinámica de trabajo en la Auditoría.

Posteriormente, se procedió a registrar los análisis, comprobaciones, verificaciones e interpretaciones; obtenidos a partir de las evidencias que proporcionarán los datos requeridos para la elaboración de los papeles de trabajo. Estos documentos serán el soporte argumentativo para dar las opiniones, juicios y conclusiones acerca del Sistema de Información examinado. La realización efectiva de visitas, entrevistas y encuestas al personal de labores de esta entidad de salud, con el objeto de obtener información veraz acerca del Sistema de Información Krystalos, garantizará la consecución de los papeles de trabajo y, por consiguiente, la argumentación necesaria para realizar finalmente un informe de Auditoria completo que describa la situación real acerca del manejo y procesamiento de la información.

La investigación estuvo enmarcada dentro del Tipo de Auditoria Externa. Esta permitirá obtener una opinión independiente y con mayor objetividad acerca de la información procesada mediante la aplicación Krystalos, y facilitará la toma decisiones a la parte administrativa en cuanto a los controles y mejoras que se requieran para optimizar el rendimiento de los procesos relacionados con el envío, procesamiento y recepción de los datos.

El alcance de la auditoria estuvo determinado por los objetivos de la misma, así como también por la verificación de los procesos, procedimientos y actividades que comprometen los activos del sistema de información, relacionados con el área administrativa y financiera. Esta auditoría se realizará en los componentes o activos de la empresa clínica integral Laura Daniela (Hardware, Software, Red, Sitio, Organización) de los cuales se identificarán sus vulnerabilidades y amenazas y se evaluarán para determinar sus controles, teniendo en cuenta la metodología ISO 27001. De lo anterior se desarrollaron sus respectivas conclusiones y recomendaciones para cada uno de los procesos evaluados en cada componente.

En el desarrollo de la auditoria de seguridad llevada a cabo en la clínica integral Laura Daniela se realizaron las pruebas sustantivas y las pruebas de penetración de acuerdo a los permisos obtenidos para tal fin. Como pruebas sustantivas se aplicarán cuestionarios, entrevistas y visitas de observación a la sede con el objetivo de determinar las falencias encontradas por el personal que maneja

directamente los sistemas de información, así como obtener las evidencias de las instalaciones físicas (Cableado, e infraestructura física).
Dentro de las pruebas de penetración se hizo uso de varias herramientas a nivel de software como lo son: Vega Vulnerability Scanner y NMAP Security Scanner.
La Metodología Magerit se presenta como una alternativa formal para investigar los riegos que presenta el Sistema de Información en la Clínica Laura Daniela y formular las medidas necesarias que se deben adoptar para controlar estos riesgos.
De esta manera, la estructura operacional que presenta el método Magerit contribuirá a un mejoramiento pleno del Sistema de Información a partir de los datos obtenidos en la investigación. El Modelo de trabajo de Magerit en torno al proceso de análisis de riesgos se encuentra seccionado en 4 bloques, que son:

1. Identificación y valoración de los activos.
2. Identificación de las amenazas asociadas a los activos
3. Identificación de salvaguardas o controles existentes.
4. Estimación del impacto y riesgo al que están sometidos los activos del sistema.

METODOLOGÍA: Esta investigación se realizó bajo los lineamientos de la metodología ISO 27001: 2013 y siguiendo los pasos básicos para la puesta en marcha de cualquier proyecto los cuales son: Análisis y observación de la empresa a auditar, planificación de la auditoria, ejecución de la auditoria e informe final. Para la consecución de las etapas anteriores se trabajó bajo los parámetros que disponen los servicios de auditoría y pruebas de seguridad informática los cuales se detallan en los siguientes pasos:

1. Definir los activos informáticos a probar.
2. Identificar las vulnerabilidades con la ayuda de auditorías internas y el pentest externo (evaluación externa).
3. Establecer las probabilidades de la ocurrencia de las vulnerabilidades informáticas que puedan comprometer la seguridad de los activos.
4. Calcular el impacto y la prioridad de cada vulnerabilidad detectada durante la auditoria interna y el pentest externo.
5. A la terminación de la auditoria interna y la evaluación externa, documentar los detalles, impactos, prioridades de las vulnerabilidades informáticas.

Para el desarrollo de los anteriores pasos se implementó la metodología de análisis y gestión de riesgos MAGERIT, la cual nos brinda una forma eficiente de gestionar los riesgos y amenazas de cada activo de información, así como el impacto generado por cada uno de ellos ante un eventual ataque.

CONCLUSIONES: Como resultado de la auditoría al sistema de información CLINICA LAURA DANIELA. Se pudo determinar que es una empresa mediana con miras a extenderse, y que a corto plazo debe velar por el mejoramiento de sus condiciones y por la revisión de debilidades puntuales tales como: a nivel de

uso no autorizado de equipos, control en la manipulación de las redes de comunicaciones, prevención ante siniestros de origen natural, y poca capacitación de personal. Todas y cada una de las anteriores son amenazas evaluadas, y a las cuales es necesario hacerles un control para disminuir los riesgos. Sin duda alguna la mayor debilidad del sistema de información es la ausencia de políticas y prácticas de seguridad planteadas por la administración de la empresa que regulen el comportamiento de los usuarios del sistema.

Por otra parte, hay riesgos medios que deben ser minimizados ante la presencia de amenazas, esto a través del tratamiento de la intrusión en el sistema, la manipulación del sistema, el uso de software falso o copiado, entre otros.

RECOMENDACIONES: Las recomendaciones finales que resaltamos de esta investigación después de haber evaluado todo el sistema y de haber encontrado todas estas fallas tanto en el sistema como en la empresa en general son las siguientes:

Se deben establecer, las políticas de seguridad informáticas para generar conciencia entre los usuarios de la importancia que tienen los activos de la empresa para la protección ante eventuales amenazas y ataques externos e internos.

Velar por el mantenimiento y mejor organización del cuarto de telecomunicaciones y el resto de la red de acuerdo a los estándares para cableado estructurado.

Se recomienda que se lleve a cabo una revisión periódica de las amenazas y riesgos, puesto que la tecnología está en constante cambios y avance, los cuales deben ser controlados para evitar futuros problemas.

Mejorar las condiciones preventivas ante riesgos laborales e incidentes de tipo natural, esto a través de asesorías con empresas de salud ocupacional, capacitación del personal y adecuación de salidas de emergencia y planes de contingencia.

Formalizar la realización, socialización y control de las políticas de seguridad entre los usuarios del sistema de información, así como la revisión periódica de las mismas por parte de la gerencia.

Bibliografía: INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACION. Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. NTC-ISO/IEC 27001:2013. Bogotá D.C. El instituto 26p.

PIATTINI, Mario G.y PESO, Emilio Del. Auditoria Informática un enfoque Práctico, 2 edición. México D.F. editorial Alfa omega 2001. 649p. ISBN 978-15-0731-2.

Elaboró	Nehemías Sarabia Díaz, 16/05/17