ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN DEL HOSPITAL E.S.E. SAN BARTOLOMÉ DE CAPITANEJO, SANTANDER

JOSÉ LEONARDO CORDERO MORENO
YADIMYR OSWALDO GARCÍA REYES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MALAGA
2016

ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN DEL HOSPITAL E.S.E. SAN BARTOLOMÉ DE CAPITANEJO, SANTANDER

JOSÉ LEONARDO CORDERO MORENO
YADIMYR OSWALDO GARCÍA REYES

Proyecto de grado presentado como requisito parcial para optar al título de:
Especialista en Seguridad Informática

DIRECTOR (A):
INGENIERA. YINA ALEXANDRA GONZALEZ.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MALAGA
2016

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Málaga, 24 de Noviembre de 2015

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

1. INTRODUCCION

Actualmente no es un secreto que las tecnologías de la información están en todos los procesos que desarrollamos a diario; lo que permite mejorar todas las actividades tanto de una empresa como personales; pero a un alto costo, ya que estos sistemas de información poseen vulnerabilidades o están expuestos a riesgos que implican que la plataforma no esté totalmente segura; es por esta razón que se debe mejorar la seguridad tanto de la parte hardware con la parte software e infraestructura de los sistemas de información.

Para ello debemos tener en cuenta que los avances tecnológicos ocurren a gran velocidad, por tal motivo la planeación estratégica debe ser muy eficaz y debe estar en constante mejoramiento para permitir aseguramiento del sistema en todos sus aspectos.

Para iniciar con el mejoramiento de la seguridad del sistema de información es necesario realizar la identificación de las vulnerabilidades o situaciones de riesgo a las cuales está expuesto internamente o externamente el sistema; con el objetivo de proteger la integridad, disponibilidad y confiabilidad de la información, para ello se hace necesario la implementación de políticas, herramientas y controles que ayuden a monitorear y reducir todos los riesgos detectados.

En este documento se especifican algunas medidas que al ser implementadas mejoraran la continuidad del negocio y se generara una administración eficiente de las tecnologías de la información que a su vez traerá consigo el aseguramiento del sistema de información del E.S.E Hospital San Bartolomé de Capitanejo.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar el análisis de riesgos y recomendaciones en los niveles de seguridad informática mediante el uso de aplicaciones que permitan evidenciar vulnerabilidades en los sistemas de información y telecomunicaciones del Hospital E.S.E. San Bartolomé de Capitanejo, Santander.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos de información y de negocio en la Institución.
- Analizar las vulnerabilidades, amenazas y riesgos existentes en los sistemas de información, determinando cuales pueden afectar a la institución.
- Proponer un plan de sensibilización, difusión y capacitación en políticas de seguridad informática para eliminar las vulnerabilidades existentes y así llevar a cabo un buen manejo y protección de la información.

3. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, gran parte de las instituciones en el departamento de Santander y en el país se apoyan en las tecnologías de la información y las comunicaciones para realizar los procesos más importantes de sus labores diarias, a medida que la gestión de la información sobre la red se hace más crítica, las instituciones tienen el deber de implementar sistemas de seguridad para proteger recursos y sus activos informáticos implementando correctamente mecanismos de seguridad en las redes de computadores, en busca de evitar el mal funcionamiento de los procesos y disminución de la eficiencia de los mismos, además de pérdidas sustanciales de dinero, credibilidad del buen nombre de la institución y obtener mayor rendimiento en la ejecución de sus procesos.

Según esto, con el paso del tiempo la información se ha convertido en el activo más importante de la mayoría de las instituciones, y por tanto se deben implementar controles de seguridad física y lógica que permitan asegurar toda esta información aplicando protección en sus actividades y que la puedan ayudar a ofrecer mejores servicios administrativos.

Desde este punto de vista el E.S.E. Hospital San Bartolomé de Capitanejo, Santander; en sus procesos informáticos se encuentra en alta vulnerabilidad ya que existen riesgos que no se han tenido en cuenta al momento de proteger la información; estos riegos o vulnerabilidades deben ser analizados y revisados para tomar medidas de control que permitan minimizar los riesgos inminentes que puedan afectar el sistema de información de la institución.

3.1 JUSTIFICACION

El Hospital E.S.E. San Bartolomé de Capitanejo, Santander; en el último año ha presentado un cambio significativo en la estructura se sus sistemas de información que han contribuido a la obtención de metas y objetivos planteados. En el año anterior se ha logrado el fortalecimiento de dicho sistema mediante la implementación de aplicativos que funcionan de manera integral, permitiendo la disminución de los tiempos de procesamiento, mejorar el control y flujo de la información y por consiguiente aumentar el porcentaje de satisfacción de los usuarios internos y externos.

Adicionalmente a lo anterior se han realizado un arduo trabajo dedicado al fortalecimiento de la plataforma tecnológica, con la implementación gradual de 3 servidores de red, estaciones de trabajo más potentes, dispositivos activos de red y de soporte eléctrico; que ayudaran a mejorar el rendimiento del sistema de información.

La implementación de estas nuevas tecnologías ha generado importantes logros en los costos de operación; además de presentar nuevas exigencias para los trabajadores en cuanto a los tiempos de capacitación y formas de trabajar. De esta manera el Hospital con esta renovación tecnológica está ejerciendo actividades económicas más efectivas que permiten posicionarlo en su entorno

competitivo tanto en términos de calidad como de estabilidad financiera como uno de los mejores.

El producto resultante de este estudio serán las recomendaciones y alternativas para darle tratamiento a los riesgos encontrados sobre los procesos, procedimientos y recursos que tienen información sensible para el hospital, permitiendo la creación de mecanismos, estrategias y cultura en las personas mediante un proceso de capacitación y/o concientización del personal del hospital en el uso correcto de los recursos tecnológicos.

3,2 RESUMEN

En el presente trabajo de grado se documenta una serie de análisis de riesgos que se han detectado en la empresa E.S.E. hospital San Bartolomé del municipio de Capitanejo, esto debido al cambio de la infraestructura y la falta de implementar unas políticas de seguridad adecuadas en la administración de tres (3) servidores en los cuales se encuentra almacenada la información de todos los procesos administrativos operativos y financieros de la empresa, se hace necesario plantear diversas recomendaciones de seguridad informática para optimizar el fortalecimiento de dichos procesos garantizando su confidencialidad, integridad y disponibilidad. El producto resultante de este estudio serán las recomendaciones y alternativas para darle tratamiento a los riesgos encontrados sobre los procesos, procedimientos y recursos que tienen información sensible para el hospital, permitiendo la creación de mecanismos, estrategias y cultura en las personas mediante un proceso de capacitación y/o concienciación del personal del hospital en el uso correcto de los recursos tecnológicos.

Palabras clave: Magerit, Análisis de riesgos, Seguridad informática, iso/iec 15408, Esteneografia, Iso/iec 27001, Pilar, Cobit, Etical Hacking, Nesuss, kali linux, backup, Antivirus, Nmap.

3.3 ABSTRACT

In this paper grade a series of risk analysis have been detected in the company ESE documents San Bartolome hospital Capitanejo Township, this due to the change of the infrastructure and the failure to implement adequate security policies in the administration of three (3) servers in which is stored the information of all operational and financial management processes company, is raising certain security recommendations to optimize these processes strengthening ensuring confidentiality, integrity and availability. The product resulting from this study will be the recommendations and options to give treatment to the risks encountered on the processes, procedures and resources that have sensitive information to the hospital, allowing the creation of mechanisms, strategies and culture in people

through a training process and / or awareness of hospital personnel in the proper use of technological resources.

Keywords: Magerit, Risk Analysis, IT security, ISO / IEC 15408, Esteneography, ISO / IEC 27001, Pilar, Cobit, Etical Hacking, Nesuss, kali linux, backup, antivirus, Nmap.

4. MARCO DE REFERENCIA

4.1 ESTADO DEL ARTE

A continuación se referencian antecedentes y trabajos relacionados a nivel Nacional.

John Jairo Perafán Ruiz, Mildred Caicedo Cuchimba desarrollaron el proyecto "Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca" para realizar el análisis de riesgos que permita generar controles para minimizar la probabilidad de ocurrencia e impacto de los riesgos asociados con las vulnerabilidades y amenazas de seguridad de la información existentes en la Institución Universitaria Colegio Mayor del Cauca en la ciudad de Popayán.

Jorge Luis Galeano villa, Cristian camilo Alzate Castañeda desarrollaron el proyecto "Protocolo de políticas de seguridad informática para las universidades de Risaralda" cuyo propósito fue construir y proponer un protocolo para la elaboración de una política seguridad informática para instituciones de educación superior en Risaralda.

Juan David Aguirre Cardona, Catalina Aristizabal Betancourt presentaron el proyecto "Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda" su objetivo general fue diseñar el sistema de gestión de seguridad de la información para el Grupo Empresarial La Ofrenda en la ciudad de Pereira.

Se referencian también antecedentes y trabajos relacionados a nivel Internacional.

Hernández Pinto María Gabriela presentó su proyecto "Diseño de un plan estratégico de seguridad de información en una empresa del sector comercial su Objetivo general es diseñar un plan estratégico de seguridad de información para una empresa comercial.
En la ciudad de Guayaquil Ecuador.

Magdalena Reyes Granados presenta su proyecto "Propuestas para impulsar la seguridad informática en materia de educación" su objetivo es **r**ealizar una investigación que permita estudiar, analizar y determinar la situación actual de la seguridad informática en México y su contraste a nivel internacional. En Ciudad de México en Octubre del año 2011
López Sevilla, Galo Mauricio, Torres Núñez, Elizabeth Magdalena presentan su proyecto " Políticas de seguridad de la información basado en la norma iso/ice 27002:2013 para la dirección de tecnologías de información y comunicación de la universidad técnica de Ambato" su objetivo es elaborar políticas de seguridad de la información en base a parámetros de la norma ISO/IEC 27002:2013 en la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato. en Ecuador Julio – 2015

4.2 MARCO CONTEXTUAL

4.2.1 Plataforma Estratégica

4.2.1.1 Misión

Nuestro hospital es una Empresa Social del Estado - E.S.E.- que presta servicios de salud de bajo nivel de complejidad, de forma segura, oportuna, humanizada y continua, para contribuir al mejoramiento de la calidad de vida de nuestros usuarios.

4.2.1.2 Visión

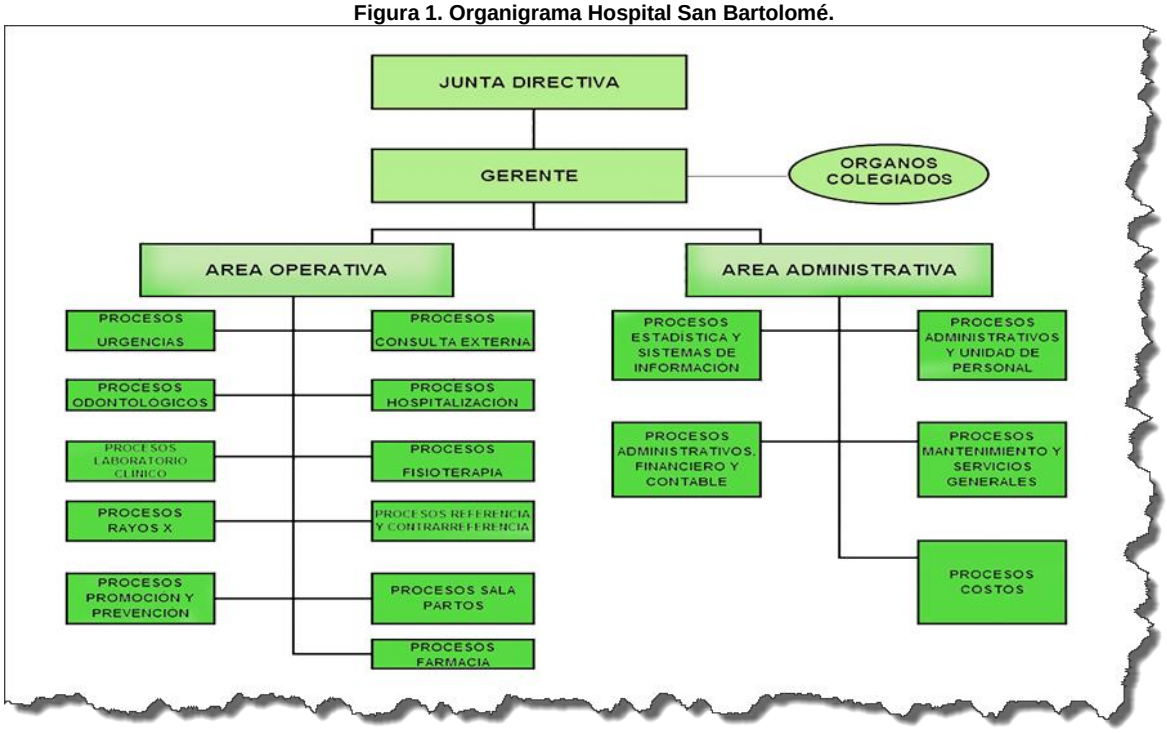
En el año 2015, el Hospital San Bartolomé será modelo de gestión en la prestación de los servicios de salud en la provincia de García Rovira, basados en principios y valores institucionales para lograr el bienestar financiero y el mayor impacto social a nuestros usuarios.

4.2.1.3 Actividad Socioeconómica

Prestar servicios de salud de primer nivel de complejidad seguro, eficiente y oportuno a la población Capitanejana y su área de influencia; todo ello enmarcado en un trato humanizado, con talento humano y tecnología adecuada para garantizar el mejoramiento continuo de la calidad de vida de sus habitantes.

4.2.2 Organigrama

Figura 1. Organigrama Hospital San Bartolomé.



Fuente: El autor

4.3 MARCO TEÓRICO

4.3.1 Seguridad de la Información.

En la Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos. Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección. [1]

4.3.2 Análisis y Gestión de Riesgos

En lo relacionado con la tecnología, generalmente el riesgo es planteado solamente como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida. Según la Organización Internacional (ISO) define riesgo tecnológico como "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños". En esta definición se identifican varios elementos que deben ser comprendidos adecuadamente para percibir integralmente el concepto de riesgo y los procesos aplicados sobre él. Dentro de estos elementos están la probabilidad, amenazas, vulnerabilidades, activos e impactos.

4.3.3 Análisis de Riesgos

El primer paso en la Gestión de riesgo es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

Existen varios métodos de como valorar un riesgo y al final, todos tienen los mismos retos -las variables son difíciles de precisar y en su mayoría son estimaciones y llegan casi a los mismos resultados y conclusiones.
En el ámbito de la Seguridad Informática, el método más usado es el Análisis de Riesgo.

Probabilidad de Amenaza: Se habla de un Ataque, cuando una amenaza se convirtió en realidad, es decir cuando un evento se realizó. Pero el ataque no dice nada sobre el éxito del evento y sí o no, los datos e informaciones fueron perjudicados respecto a su confidencialidad, integridad, disponibilidad y autenticidad.
Para estimar la Probabilidad de Amenaza nos podemos hacer algunas preguntas como:
- **¿Cuál es el interés o la atracción por parte de individuos externos, de atacarnos?**
- **¿Cuáles son nuestras vulnerabilidades?**

---

[1] Markus Erb. Gestión de Riesgo en la Seguridad Informática [en línea]. https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

• **¿Cuántas veces ya han tratado de atacarnos?**

4.3.4 Magnitud de Daño

Se habla de un Impacto, cuando un ataque exitoso perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.
Estimar la Magnitud de Daño generalmente es una tarea muy compleja. La manera más fácil es expresar el daño de manera cualitativa, lo que significa que aparte del daño económico, también se considera otros valores como daños materiales, imagen, emocionales, entre otros. Expresarlo de manera cuantitativa, es decir calcular todos los componentes en un solo daño económico, resulta en un ejercicio aún más complejo y extenso.

Algunas preguntas que podemos hacernos para identificar posibles consecuencias negativas causadas por un impacto son:

• **¿Existen condiciones de incumplimiento de confidencialidad (interna y externa)?**
• **¿Existen condiciones de incumplimiento de obligación jurídicas, contratos y convenios?**
• **¿Cuál es el costo de recuperación?**

Considerando todos los aspectos mencionados, nos permite clasificar la Magnitud del Daño. Sin embargo, otra vez tenemos que definir primero el significado de cada nivel de daño (Baja, Mediana, Alta).[2]

4.3.5 EAR /PILAR

Para conocer el estado de seguridad de un sistema, es necesario modelarlo, identificando, valorando sus activos y amenazas sobre los mismos. De esta manera se puede estimar el riesgo a que el sistema está sujeto. El riesgo se puede mitigar por medio de las salvaguardas o contramedidas desplegadas para proteger el sistema. Es inusual que las salvaguardas reduzcan el riesgo a cero; es más frecuente que siga existiendo un riesgo residual que la organización o bien pueda aceptar, o bien intente reducir más, estableciendo un plan de seguridad orientado a llevar el riesgo a niveles aceptables.

El análisis de riesgos proporciona información para las actividades de tratamiento de los riesgos. Estas actividades se ejercen una vez y otra vez, incorporando nuevos activos, nuevas amenazas, nuevas vulnerabilidades, y nuevas salvaguardas.

EAR es un conjunto de herramientas: este comprende un conjunto o compendio de herramientas que se utilizan para efectuar un análisis general, que contempla todas las dimensiones de la seguridad informática como la integridad, disponibilidad y

---

[2] Markus Erb. Gestión de Riesgo en la Seguridad Informática [en línea]. https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

confidencialidad, con el objetivo de minimizar el tiempo de caída del servicio cuando se solventa algún desastre.
Este conjunto de herramientas permite la opción de realizar tanto un análisis cualitativo como cuantitativo basado en la metodología Magerit.
PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

- ISO/IEC 27002:2005 - Código de buenas prácticas para la Gestión de la Seguridad de la Información
- ENS - Esquema Nacional de Seguridad [3]

Análisis cualitativo en PILAR: PILAR puede realizar un análisis cualitativo, usando una serie de niveles discretos para la valoración de los activos. Un análisis cualitativo se recomienda siempre en primer lugar, antes de que se intente un análisis cuantitativo detallado. Un análisis cualitativo permite:

- Identificar los activos más significativos
- Identificar el valor relativo de los activos
- Identificar las amenazas más relevantes
- Identificar las salvaguardas presentes en el sistema
- Establecer claramente los activos críticos (los que están sujetos a un riesgo máximo)

Análisis cuantitativo en PILAR: PILAR puede realizar un análisis cuantitativo detallado:

- Detalla las consecuencias económicas de la materialización de una amenaza en un activo
- Estima la tasa anual de ocurrencia (ARO) de amenazas (annual rate of occurrence)
- Detalla el coste de despliegue y mantenimiento de las salvaguardas
- Permite ser más preciso en la planificación de gastos de cara a un plan de mejora de seguridad [4]

---

[3] EAR / PILAR Entorno de análisis de riesgos [en línea]. http://www.ar-tools.com/es/index.html

[4] MARTINEZ GARCIS Robinson. PILAR Análisis y Gestión de Riesgos [en línea]. https://docs.google.com/document/d/15TYUClkxF_WYA1kTqCJa6bwQaCLlaEkwAQ-8EvFO7js/edit?pli=1

Amenazas en PILAR

- Modelo de Amenazas:

Se denomina modelo de amenazas a la terminología utilizada para concretar la valoración de las amenazas: probabilidad y degradación.

- Niveles de valoración. Los activos y los impactos se valoran cualitativamente según una escala de 0 hasta 10.

Los criterios asociados a cada nivel (es decir, argumentos que se pueden utilizar para establecer cierto nivel) se pueden consultar sobre las pantallas. Sin embargo, el resumen siguiente puede ayudar a encontrar el nivel correcto:

Figura 2 Niveles de Valoración

nivel	semántica
10	el valor más alto, el daño más alto
7	el valor más grande / el daño más grave que suele darse en servicios civiles o de la administración pública
5	cuando las consecuencias no afectan a otras organizaciones externas
3	consecuencias limitadas, de carácter interno
0	insignificante - puede ser obviado a todos los efectos prácticos

Fuente: https://seguridadinformaticaufps.wikispaces.com/file/view/4.JPG/329062204/4.JPG.

Impacto y riesgo en PILAR. Estos son factores que no se pueden desestimar, ya que al momento de realizar un análisis debemos tenerlos en cuenta, en este caso en particular el impacto nos determina que daño puede ocurrir cuando se materializan las amenazas.
Y el riesgo es un indicador de los que puede ocurrir por causa de las amenazas.
Estos dos factores pueden ser controlados a través de los salvaguardas, logramos minimizarlos a valores aceptables.
El impacto y el riesgo, el potencial y los valores residuales, constituyen información importante para tomar decisiones en materia de seguridad por ejemplo:

- Activos a supervisar
- Salvaguardas a desplegar o a mejorar

- Aceptación de riesgos operacionales[5]

4.3.6 METODOLOGIA MAGERIT

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España. Actualizada en 2012 en su versión 3. Esta metodología contempla diferentes actividades enmarcadas a los activos que una organización posee para el tratamiento de la información. A continuación se relacionan cada uno de los pasos que se deben contemplan en un proceso de análisis de riesgos, teniendo en cuenta un orden sistémico que permita concluir el riesgo actual en que se encuentra la empresa.

Como se mencionó anteriormente, los activos son todos los elementos que una organización posee para el tratamiento de la información (hardware, software, recurso humano, etc.). Magerit diferencia los activos agrupándolos en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información. A la hora de realizar el análisis de riesgo el primer paso es identificar los activos que existen en la organización y determinar el tipo. En la tabla No. 2 se relacionan cada tipo de activos.

Tabla No. 1 Relación de activos de seguridad de la información

Tipos de activos	Descripción
Activo de información	Bases de datos, documentación (manuales de usuario, contratos, normativas, etc.)
Software o aplicación	Sistemas de información, herramientas de desarrollo, aplicativos desarrollados y en desarrollo, sistemas operativos, aplicaciones de servidores etc.
Hardware	Equipos de oficina (PC, portátiles, servidores, dispositivos móviles, etc.)
Red	Dispositivos de conectividad de redes (router, swicth, concentradores, etc.)
Equipamiento auxiliar	UPS,
Instalación	Cableado estructurado, instalaciones eléctricas.
Servicios	Conectividad a internet, servicios de mantenimiento, etc.
Personal	Personal informático (administradores, webmaster, desarrolladores, etc.), usuarios finales y personal técnico.

Fuente: El autor

[5] Seguridad Informática [en línea]. https://seguridadinformaticaufps.wikispaces.com/PILAR+-+Herramienta+para+An%C3%A1lisis+y+Gesti%C3%B3n+de+Riesgos

Valoración de los activos: Cada activo de información tiene una valoración distinta en la empresa, puesto que cada uno cumple una función diferente en la generación, almacenaje o procesamiento de la información. Pero a la hora de valorarlos no sólo debemos tener en cuenta cuanto le costó a la empresa adquirirlo o desarrollarlo, sino que además debemos contemplar el costo por la función que ella desempeña y el costo que genera ponerlo nuevamente en marcha en caso de que éste llegase a dañarse o deteriorarse.

Dimensiones de Seguridad: Es necesario definir unos criterios de valoración que nos permitan ubicar la posición en que se encuentra cada activo frente a cada dimensión. A continuación se relacionan los criterios que se podrían tener en cuenta para valorar los activos con respecto a cada dimensión de seguridad, ver tabla No. 2.

Tabla No. 2 Criterios de valoración de los activos

VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Fuente: El Autor

Con base a los criterios anteriores, se puede hacer una valoración cualitativa de cada activo en relación a las 4 dimensiones de seguridad contempladas en la metodología.

Amenazas (identificación y valoración): Existen actualmente múltiples amenazas que pueden afectar los activos de una empresa, por ello es importante identificarlas y determinar el nivel de exposición en la que se encuentra cada activo de información en la organización. Se considera una amenaza, a cualquier situación que pueda dañar o deteriorar un activo, impactando directamente cualquiera de las 4 dimensiones de seguridad. La ISO/IEC 13335-1:2004 define que una “amenaza es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización”.

4.3.7 ETICAL HACKING

Actualmente debemos tener en cuenta que las computadoras en todo el mundo son susceptibles de ser atacadas por crackers o hackers capaces de comprometer los sistemas informáticos y robar información valiosa, o bien borrar una gran parte de ella. Esta situación hace imprescindible conocer si estos sistemas y redes de datos están protegidos de cualquier tipo de intrusiones.

Por tanto el objetivo fundamental del Ethical Hacking (hackeo ético) es explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc.
Con la intención de ganar acceso y "demostrar" que un sistema es vulnerable, esta información es de gran ayuda a las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados. Dicho lo anterior, el servicio de Ethical Hacking consiste en la simulación de posibles escenarios donde se reproducen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que: "Para atrapar a un intruso, primero debes pensar como intruso"

4.3.8 KALI LINUX

Es una distribución de Linux basada en Ubuntu que incluye numerosas aplicaciones para realizar tests de seguridad y análisis informático forense.

Gracias a esas aplicaciones Kali linux se ha convertido en una distribución imprescindible para los administradores de sistemas y profesionales de la auditoria informática.

La distribución incluye utilidades para la auditoría de redes wireless, scanners de puertos y vulnerabilidades, sniffers, archivos de exploits, etc. La mayoría de ellas actualizadas a sus últimas versiones, Algunas de esas herramientas son: dnsmap, Netmask, PsTools, TCtrace, Nmap, Protos, utilidades para la detección de vulnerabilidad en redes Cisco, SQL Inject, SMB-NAT, SNMP Scanner, Pirana, Dsniff, Hydra, Sing, WebCrack, Wireshark, NSCX, Airsnort, aircrack, BTcrack, SNORT, Hexedit, etc. Hasta completar más de 300.[6]

4.3.9 NMAP

Nmap es un programa de código abierto utilizado para efectuar rastreo de puertos fue desarrollado inicialmente para Linux aunque en la actualidad es

---

[6] Saiz Esteban. Backtrack una distribución Linux para expertos en seguridad. [en línea]. http://www.genbeta.com/mobile.php/sistemas-operativos/backtrack-4-una-distribucion-linux-para-expertos-en-seguridad

multiplataforma. 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.

4.4 MARCO CONCEPTUAL

A continuación se definen algunos términos que serán mencionados y utilizados en el desarrollo del proyecto de acuerdo con:

Vulnerabilidades: Son ciertas condiciones inherentes a los activos, o presentes en su entorno, que facilitan que las amenazas se materialicen y los llevan a la condición de vulnerabilidad. Las vulnerabilidades son de diversos tipos como por ejemplo: la falta de conocimiento de un usuario, la transmisión a través de redes públicas, entre otros.

Activos: Los activos a nivel tecnológico, son todos los relacionados con los sistemas de información, las redes y comunicaciones y la información en sí misma, Por ejemplo los datos, el hardware, el software, los servicios que se presta, las instalaciones, entre otros.

Impactos: Son las consecuencias de la ocurrencia de las distintas amenazas y los daños por pérdidas que éstas puedan causar. Las pérdidas generadas pueden ser financiaras, económicas, tecnológicas, físicas, entre otras.

Análisis de Riesgos: Este tipo de análisis se utiliza como herramienta para obtener un diagnostico que nos ayude a establecer la exposición real a los riesgos que está expuesto el hospital. Su objetivo primordial es la plena identificación de los riesgos, teniendo en cuenta el riesgo total y residual que pueden generar y a través de eso aplicar contramedidas en términos cuantitativos o cualitativos.

Probabilidad: para establecer la probabilidad de ocurrencia se puede hacerlo cualitativa o cuantitativamente, considerando lógicamente, que la medida no debe contemplar la existencia de ninguna acción de control, o sea, que debe considerarse en cada caso que las posibilidades existen, que la amenaza se presenta independientemente del hecho que sea o no contrarrestada.

Amenazas: las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en las operaciones de la organización, comúnmente se referencia como amenazas a las fallas, a los ingresos no autorizados, a los virus, a los desastres ocasionados por fenómenos físicos o ambientales, entre otros. Las amenazas pueden ser de carácter físico como una inundación, o lógico como un acceso no autorizado a la base de datos.

Riesgo: se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo, de manera cuantitativa e, riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado.

Así definido un riesgo conlleva a dos tipos de consecuencias: Ganancias o pérdidas.

En lo relacionado con tecnología, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición o el grado de una perdida (Por ejemplo el riesgo de que se pierdan los datos por el daño del disco duro, virus informáticos entre otros).
La organización Internacional para la normalización (ISO), define riesgo tecnológico como:
"La probabilidad de que una amenaza se materialice, utilizando una vulnerabilidad existente de un activo o un grupo de activos, generándole pérdidas o daños". [7]

MAGERIT: La Metodología MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

5. MARCO LEGAL

El desarrollo del proyecto está basado en el desarrollo y aplicación de estándares, metodologías y buenas prácticas para tener un uso eficaz y seguro del sistema de información del Hospital E.S.E. San Bartolomé de Capitanejo, Santander; logrando minimizar todos los riesgos y vulnerabilidades a los cuales está expuesto ese bien tan preciado e intangible; para ello el hospital nos dio el aval para desarrollar este proyecto en sus instalaciones y sistemas informáticos **(anexo cartas de autorización).** Adicionalmente a lo mencionado anteriormente existe en nuestro medio un fundamento jurídico que logra parametrizar la utilización de los sistemas de información, y toma medidas contra aquellas personas que intentan realizar ataques contra ellos.
Algunas de las leyes y normas de la legislación colombiana relacionada con seguridad de la información tomadas son:

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

---

[7] SOLARTE SOLARTE Francisco Nicolás Javier. Riesgos y Control Informático [en línea]. http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_21_generalidades_del_estndar_cobit.html

los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

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

Decreto No. 2693 de 2012: (21), Por el cual se establecen los lineamientos generales de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, Y se dictan otras disposiciones.

6. DISEÑO METODOLOGICO

6.1 METODOLOGIA

El área de tecnologías de la información y las comunicaciones en el E.S.E. hospital San Bartolomé de Capitanejo, Santander; comprende una infraestructura de equipos computacionales y software para la interconexión de todas las dependencias de la institución, brindando la posibilidad de acceso a redes externas, incluyendo internet. Entre el edificio y las áreas del hospital existe una red de datos que permite su interconexión con todas las dependencias que utilizan los recursos tecnológicos ofrecidos por el área de TIC’S.

Dentro de la infraestructura del hospital debemos tener en cuenta que existe un soporte tecnológico, mediante un backbone que comunica todas las dependencias y dentro de ella existe un cableado estructurado que interconecta las estaciones de trabajo; dentro de esta red tenemos aproximadamente 50 puntos activos con acceso a internet, a través de dos enlaces contratados con empresas dedicadas a este servicio.

El análisis de riesgos específicamente se aplicará al Área de Informática, ubicada en la parte administrativa E.S.E. Hospital San Bartolomé de Capitanejo, Santander y en particular a los servidores y la aplicación llamada Medisoft; por ser el servicio más crítico puesto que maneja y controla los procesos de historias clínicas, facturación, generación de Rips, estadísticas, y las bases de datos de los pacientes.

Este proyecto consiste en el diseño y realización de un análisis de riesgos, la documentación y diseño de las recomendaciones necesarias a través de políticas, procedimientos y controles de seguridad dentro del contexto de acceso y administración de la red, tanto interna como pública; abarcando dentro de esta solución el diseño de las herramientas, métodos y técnicas a utilizar para el levantamiento de la información, definición del marco teórico de la metodología,

caracterización y evaluación de activos, identificación de vulnerabilidades, análisis y evaluación de riesgos para finalmente realizar una propuesta del plan de acción y recomendaciones para mitigar los riesgos hallados al aplicar el modelo seleccionado en la implementación de las políticas de Seguridad de la Información al área de Tecnologías de Información y las comunicaciones del E.S.E. Hospital San Bartolomé de Capitanejo, Santander.

La propuesta será presentada ante la administración del área de Tecnologías de la Información y las comunicaciones del E.S.E. Hospital San Bartolomé de Capitanejo, Santander, para su aprobación y futura implementación.

Para el levantamiento de la información y caracterización de activos se utilizarán diferentes instrumentos que faciliten el desarrollo del proceso, entre las que se encuentran:

- **La Observación Directa**: La observación directa consiste en observar atentamente el fenómeno tomar información y registrarla para su posterior análisis. Este instrumento es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos.

  Para el desarrollo del presente proyecto, se realizaron visitas guiadas por el personal de sistemas del Hospital E.S.E. San Bartolomé de Capitanejo, las distintas áreas e instancias del Hospital; lo que permitió tomar evidencia fotográfica y visual del estado actual de los recursos técnicos y tecnológicos, su utilización, organización y de los demás elementos que intervienen en el desarrollo normal del core del negocio de la institución.

- **La Entrevista**: este es un instrumento directo e indirecto de recolección de datos con una intencionalidad y un objetivo dado por la investigación; para el presente proyecto este instrumento se puede utilizar en las reuniones programadas. Durante el desarrollo de las mismas se debe contar con la asistencia del personal de sistemas, administradores, usuarios de sistemas de información y de recursos tecnológicos en general; con el fin de identificar y conocer sus opiniones frente a la importancia de proteger y de utilizar de manera adecuada los recursos informáticos.

  Igualmente se debe hacer uso de la entrevista dirigida mediante una serie de encuestas y listas de chequeo; a fin de poder obtener la mayor cantidad de información precisa y valida que nos facilitará la identificación de posibles fallas, falencias, vulnerabilidades y aspectos por mejorar que rodean el uso de los recursos tecnológicos dentro del E.S.E. Hospital San Bartolomé de Capitanejo, Santander.

- **Pruebas de Penetración y Ethical Hacking**: para desarrollar esta actividad debemos tener en cuenta que debemos utilizar herramientas de software no pago, como las que están creadas dentro del lenguaje de Linux; estas herramientas deben ser ejecutadas en los activos de sistemas del hospital (servidores y aplicaciones propias del Sistema de información); todo esto se debe aplicar bajo la supervisión del departamento de las tic; adicionalmente a esto, estas pruebas se deben ejecutar en horarios donde no se vaya a producir algún traumatismo en el normal funcionamiento del sistema de información del hospital.

6.2 Alternativa de grado: Monografia

6.3 Línea de investigación: cadena de formación de sistemas, linea de gestión de sistemas

7. DESARROLLO DEL PROYECTO

7.1 Definición y descripción del entorno de aplicación.

La E.S.E. Hospital San Bartolomé, se encuentra ubicado en la cabecera municipal de Capitanejo en el departamento de Santander, a 35 kilómetros de distancia del municipio de Málaga y a 197 kilómetros de distancia de la ciudad de Bucaramanga. En el municipio, la E.S.E. se encuentra ubicada en el casco urbano en el barrio Libertadores, a 45 minutos de distancia en carro a la vereda de Ovejeras que es la más alejada.

FASE 1: IDENTIFICACION

7.2 Inventario Tecnológico

Tabla 3. Activos E.S.E. Hospital san Bartolomé

TIPO ACTIVO	ACTIVO	SERVICIO	SISTEMA OPERATIVO	CANTIDAD
Tangible	Switch Dlink DGS-1024D	Intercomunicación de la red LAN		1
Tangible	Red telefónica ADSL	Intercomunicación entre extensiones		1
Tangible	Computadores de escritorio Lenovo Procesador Intel core i3, 4 Gb de memoria Ram, Disco duro 300 Gb		Windows 7 de 64 Bits Office 2010 Antivirus Kaspersky	20
Tangible	Impresoras Kyocera			15
Tangible	Servidor HP ProLiant DL380p Gen8,		Windows server 2012	1

	procesador Intel® Xeon® E5-2600 v2; memoria Ram máxima de 768 Gb		R2	
Tangible	Servidor HP ProLiant DL380 Generation 5, procesador Quad-Core and Dual-Core Intel® Xeon, memoria RAM de 64 Gb		Windows server 2012 R2	1
Tangible	Servidor HP MicroServer G8: 1x CPU Dual-Core Intel Pentium G2020T (2.5 GHz), 2 GB RAM, 4x Bahías LFF NHP SATA HDD cage, 1 x Adaptador Ethernet 332i, 1Gb de 2 puertos		Windows server 2012 R2	1
Tangible	Portátiles Lenovo Procesador: Intel Core i5 2410M (2300 MHz - 2900 MHz) RAM: 4 GB DDR3 (1066 MHz) Pantalla: 14.0" (1366x768) Batería: 6 celdas Almacenamiento: HDD 500 GB (5400 rpm)		Windows 7 de 64 Bits Office 2010 Antivirus Kaspersky	20
Intangible	Bases de datos	Suministrar información de los usuarios que están activos para la prestación de servicios		1
Tangible	Ups	Supresor de picos y soporte de electricidad en caídas de la luz		30
Tangible	Cámaras de vigilancia			32
Tangible	Teléfonos			40
Tangible	Ups de respaldo			43
tangible	Planta eléctrica			1
Intangible	Servicio de internet			2
Intangible	Software de historias clínicas Medisoft		Instalado sobre plataforma Windows	1
Intangible	Antivirus	Karspersky		43
Tangible	Red de cableado estructurado			1

Fuente: propia.

7.3 Políticas de Seguridad.

El departamento de las TIC (División de Tecnologías de la Información y las Comunicaciones) del E.S.E Hospital San Bartolome del Municipio de Capitanejo; radica su funcionamiento en el personal calificado que lo compone y a su vez de sus equipos para realizar sus labores de aseguramiento tanto del sistema de información como de sus usuarios externos e internos; quienes son los que hacen uso del servicios prestados por la institución.

Es por esta razón que el departamento de las TIC debe realizar una labor de administración de una manera responsable para tomar decisiones acertadas para garantizar la protección del sistema ante cualquier ataque o falla del mismo.
Para ejecutar lo anteriormente mencionado, el departamento de las tic debe establecer medidas o políticas de seguridad que logren minimizar los riesgos a los que está expuesto el sistema de información; con el propósito de proteger y preservar la integridad del sistema y asi asegurar la prestación continua de los servicios.

7.4 identificación de activos

El primer paso para iniciar el análisis de riesgos del Hospital es la identificación de los activos esenciales para el buen funcionamiento del sistema de información. Para lograr este fin se realizaron visitas a los sitios donde tenían influencia los sistemas computacionales y a su vez se realizaron diferentes técnicas de recolección de datos como la aplicación de encuestas, entrevistas e inspección visual de las áreas que manejan el sistema de información.

Figura 3. Zona de ingreso al área de sistemas

Fuente: el autor.

7.4.1 Inspección visual de los activos.

Durante los recorridos hechos por las instalaciones del hospital se logró hacer una clasificación de los mismos basados en la ubicación y sus características.

- Al ingresar a la sala de sistemas hay una cámara que apunta a la puerta como medida de seguridad, logrando la identificación de las personas que quieren ingresa a la misma.

Como segunda medida de control de acceso a la sala de sistemas en la puerta esta implementado un control biométrico, el cual garantiza el acceso únicamente de quienes tienen los privilegios de entrar al sitio.

Figura 4. Áreas de servidores.

Fuente: El autor.

En la Figura anterior se observa uno de los racks de comunicaciones donde están ubicados los servidores en donde esta almacenada la información que se gestiona en el hospital. Además de esto también encontramos una consola por la cual se realiza el monitoreo de todos los servidores que se encuentran en esta sala.

Se puede identificar que el espacio entre cada servidor es el óptimo para que fluya el aire. Ya que se cuenta con un espacio suficiente para fluya la ventilación entre cada uno de ellos, evitando que haya sobre calentamiento y que se produzca un apagado de los equipos por esta razón.

El switch que vemos en esta imagen tiene una distribución y etiquetado de cables adecuado, lo que permite la identificación rápida de los equipos, ante cualquier falla que se pueda presentar.

Figura 5, Switch distribuidor rack

Fuente: El autor.

La consola de monitoreo de los servidores es una pantalla plana con teclado y mouse para trabajar sobre los mismos en algunos procesos de configuración, el cual debería de tener una llave para poder ser abierto este rack; además de esto todo esta soportado por una mesa de madera, la cual no debería estar allí ya que la madera es un elemento vulnerable al fuego.

Con lo observado en la visita se puede determinar que la sala debe mejorar algunos aspectos que ayuden a mejorar la seguridad de los equipos y por ende la información; para ello se debe mejorar las siguientes condiciones:

- El sistema de marquillas en los servidores y de los cables de datos.

Adicionalmente se deben implementar los siguientes dispositivos:

- un extractor de calor.
- Medidores de temperatura y humedad.
- sistema de detección contra incendios o de humo.
- Aire acondicionado para regular la temperatura

Por último se debe tener en cuenta que no existe un registro de entrada y salida de la sala.

Figura 6 Área de Switches y planta telefónica

Fuente: el autor.

En la Figura vemos tanto la planta telefónica que intercomunica todas las dependencias del hospital tanto internamente como externamente, lo que mejora el servicio de manera eficaz; allí también se encuentran los switches, los cuales son los utilizados junto con los patch panel para realizar la interconexión de nodos

y trasmisión de los datos de la red del hospital. Tanto el rack de los servidores como el rack de la planta telefónica están protegidos eléctricamente por medio de una ups y así evitar tanto picos de luz como apagones que interrumpan el normal funcionamiento de los mismos.

Algunos de los hallazgos encontrados aquí son los siguientes aspectos:

- el cableado tanto de la planta telefónica y del swich se encuentran un poco desordenados y enredados
- Las salidas de los cables de datos no son las adecuadas.
- Se encuentra una silla plástica la puede ser causante de un incendio dentro de la sala de servidores.

Evidencia sistema eléctrico área de servidores: Dentro de la sala de servidores, se encuentra el tablero de control eléctrico regulado y este es un elementó de mucho cuidado.

Figura 7. Tablero de control eléctrico área de servidores

Fuente: El autor

Como vimos en las imágenes logramos determinar que el cableados eléctrico cuenta con todas las medidas de seguridad establecidas.

Figura 8. UPS

Fuente: El autor

En las figuras anteriores se encuentra la ups en su forma, tamaño y su distribución en el cuarto de comunicaciones; esta puede ser monitorizada a través de la red para verificar su estado y su comportamiento.

Figura 9. Distribución de cables en la infraestructura

En la Figura se observa como los cables de red están soportados internamente en el edificio de la UMI, por medio de escalerillas para que sea más fácil la distribución en el edificio.

Figura 10. Cables sin normas

Fuente: El autor

También indica el ingreso de todos los cables de hacen la interconexión de cada una de las áreas del hospital

Cabe anotar que la red inicialmente tenía un tamaño óptimo y que la infraestructura que la contenía era la más adecuada, pero actualmente si vemos la fotografía vemos que los cables ya no caben dentro de la escalerilla cuando llegan al rack; por esta razón se debe realizar un ajuste para que no se presente esta situación.

En la siguiente imagen se observa uno de los dispositivos de comunicación el cual recibe los conectores de fibra óptica el cual tiene el backbone entre los switches de los dos rack de comunicaciones

Figura 11. Distribución Backbones Fibra Óptica

Fuente: El autor

Figura 12. Controles subestación eléctrica


Fuente: El autor

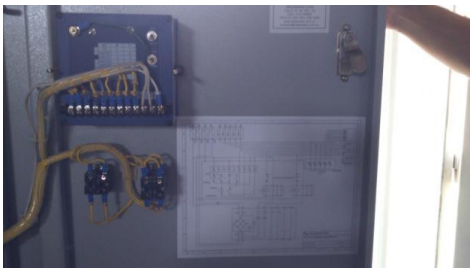
En las figuras anteriores se observa cómo está constituida la subestación eléctrica y cuáles son los tableros de monitorización y sus respectivas alarmas, lo que permite mantener el control de la subestación en completo funcionamiento.

Figura 13. Distribución subestación eléctrica.


Fuente: El autor

En estas figuras se observa la transferencia de la subestación al hospital la cual se encuentra configurada en estado automático y esta se realiza a los pocos segundos de producirse un corte del fluido eléctrico.

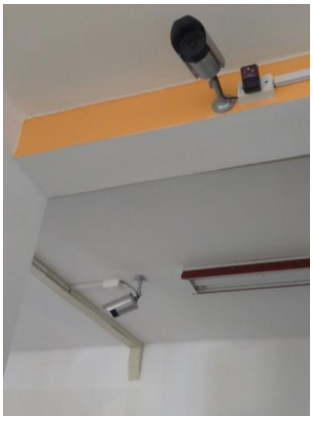
Figura 14. Planos eléctricos en las transferencias.

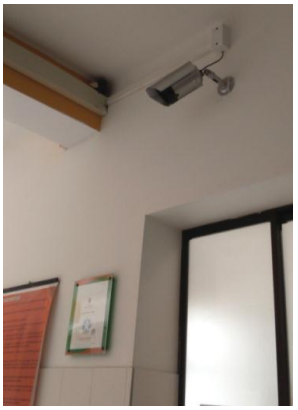


Fuente: El autor

Identificación de los circuitos de la subestación eléctrica

Figura 15. Cámaras de vigilancia área asistencial.

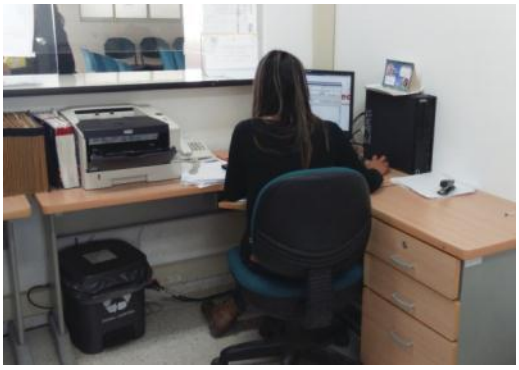




Fuente: El autor

En las imágenes anteriores podemos observar algunos de los sistemas de video cámaras que se utilizan para salvaguardar todos los activos del hospital. Dentro de los dispositivos encontramos unos sistemas de seguridad de última generación con detección de movimiento y un detector de metales con los cuales es posible identificar cuando una persona en particular puede estar cargando armas de fuego, cuchillos entre otros.

Figura 16. Distribucion de equipos en las estaciones de trabajo



Fuente: El autor

Acá podemos observar cómo estas dispuestas las estaciones de trabajo en cuanto a los monitores, teclados y mouse. La evidencia fue tomada durante las horas laborales y se les realizo la recomendación de no tener ni bebidas ni comida cerca de los equipos de cómputo.

Figura 17. Elementos de seguridad contra incendios

Fuente: El autor

En la figura anterior se identifican algunos de los elementos contra incendios que existen en cada cuarto de equipos de cómputo y de red en el hospital como norma de seguridad.

7.4.2 Clasificación de activos.

[BK] BACKUP: como su nombre lo indica representa las copias de seguridad que se realizaran como soporte al sistema de información en caso de que se presente algún evento que perjudique la información como tal. Estas copias se realizan cada día y son almacenadas tanto en discos duros como en DVD, se debe tener en cuenta que este es uno de los activos más importantes y por tal motivo el acceso a estas debe ser restringido; ya que contienen información importante como las historias clínicas de los pacientes.
[SO] SISTEMAS OPERATIVOS: esta categoría agrupa la parte intangible del sistema de información como los sistemas operativos que están instalados en los equipos de cómputo como son Windows server 2008, Windows Seven, Windows 8 los cuales están instalados con sus respectivas licencias comerciales.
[OF] SOFTWARE OFIMÁTICO: esta categoría agrupa todos los paquetes ofimáticos instalados en los equipos del hospital como son Office 2010, Office 2013 2010 y open office los cuales poseen sus respectivas licencias.

[NA] NAVEGADORES: Esta categoría agrupa los navegadores instalados en los equipos como son: Internet Explorer, Mozilla Firefox, Google Chrome.
[UV] SERVIDOR CLIENTE: en esta categoría se incluye software dedicado al control remoto de ordenadores y servidores.
[AN] ANTIVIRUS: Esta categoría contiene todos esos programas dedicados a eliminar todas las amenazas como virus informáticos. En este caso en particular el hospital tiene instalado el Karspersky.
[PH] PLATAFORMA DEL HOSPITAL: esta categoría contiene el software desarrollado a la medida para gestionar todos los procesos del hospital.

FASE 2: ANALISIS

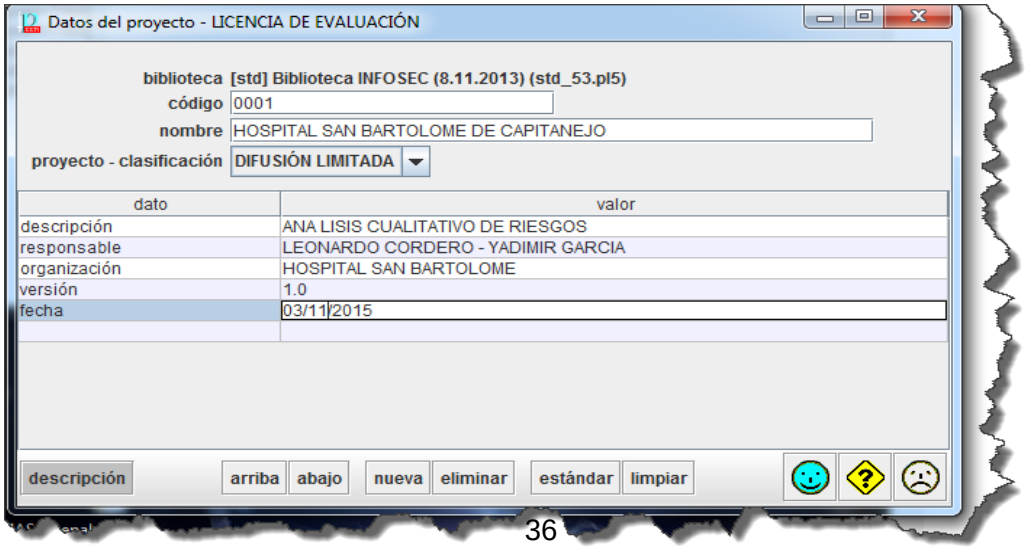
7.5 Metodología de evaluación de riesgos.

Dentro de la metodología que se va a utilizar para lograr los objetivos del proyecto será la metodología de análisis y evaluación de riesgos Magerit; a través de la herramienta tecnológica EAR PILAR.

Gracias a esta metodología tenemos las herramientas necesarias para realizar el análisis investigativo sobre el nivel de seguridad en el que se encuentra el sistema de información del hospital y tomar las medidas necesarias y de reacción para minimizar todos aquellos riesgos a los cuales está expuesto el sistema de información.
Inicialmente debemos realizar la gestión de riesgos; la cual nos permite determinar una defensa que evitara que le pase algo malo al sistema de información y así prevenir incidentes que impidan el buen funcionamiento del mismo.

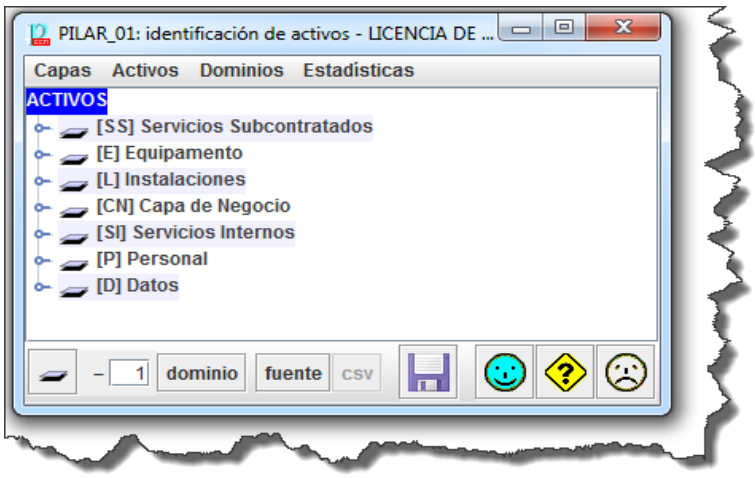
Ahora daremos inicio al desarrollo de los objetivos propuestos; para ello empezaremos a trabajar con el software PILAR el cual está basado en la metodología magerit para hacer el análisis y gestión de los riesgos.

Figura 18 Inicio del análisis cualitativo de los activos



Fuente: El autor

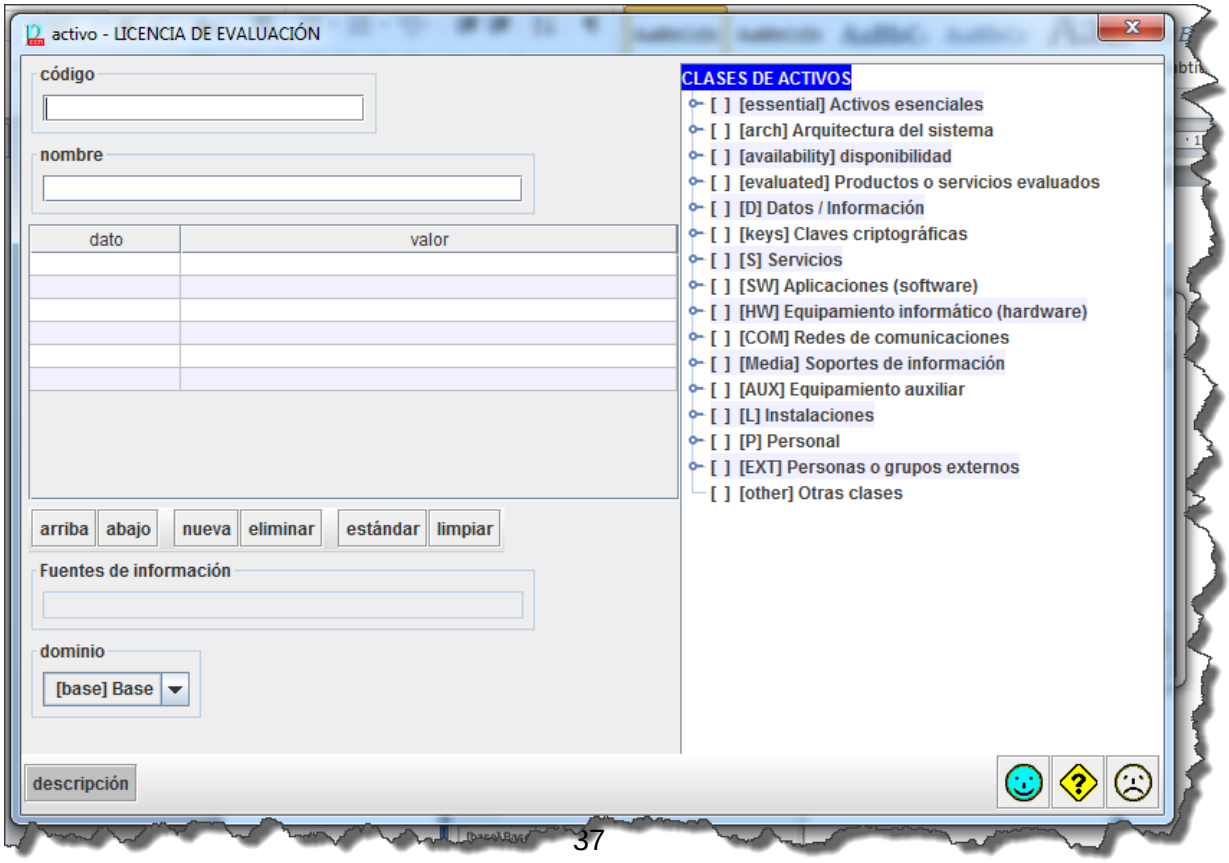
Figura 19. Identificación de Activos



Fuente: El autor

Inicialmente lo que realizamos fue la creación de las capas donde van a esta almacenados todos los activos que tiene la empresa; donde cada activo esta identificado con un código, un nombre y una clasificación o caracterización del activo, como lo veremos en la siguiente imagen.

Figura 20. Identificación de activos



Fuente: El autor

Por cada activo encontrado en el hospital se realizó el mismo procedimiento anterior; teniendo en cuenta que únicamente se ingresaron los más importantes; ya que el software almacena una cantidad limitada de los mismos.

Entre los equipos que se identificaron se encuentran, Equipos de cómputo, Equipos de Comunicaciones, Infraestructura, Aplicación que para el manejo de los servicios y el personal

Figura 21. Activos Identificados

Fuente: El autor

7.5.1 Valoración de los Activos.

En cuanto a la valoración de activos se debe tener en cuenta que todos son importantes para el hospital y por tal razón tienen un valor
Los activos son importantes para una organización y, por lo tanto, tienen un valor. En este caso en particular los activos que conforman los sistemas de información, se deben valorar teniendo en cuenta todas sus dimensiones. Dentro del software Pilar tenemos una opción donde se realiza la gestión de valoración de los activos,

en donde se define el valor de los mismos, según el impacto que tendría en el sistema de información del hospital.
Al realizar el ingreso y clasificación de los activos encontrados en el hospital; debemos realizar una ponderación a través de un análisis cualitativo basado en cinco aspectos fundamentales que son:

- **"[I]" (INTEGRIDAD DE LOS DATOS):** esta clasificación pondera cual sería el impacto que tendría en el hospital, el hecho de que la información utilizada para prestar los servicios no es correcta o está incompleta.
- **"[C]" (CONFIDENCIALIDAD DE LOS DATOS):** esta clasificación pondera cual sería el impacto que tendría en el hospital, el hecho de que la información utilizada para prestar los servicios fuera vulnerada por personas no autorizadas.
- **"[A]" (AUTENTICIDAD DE LOS DATOS):** esta clasificación pondera cual sería el impacto que tendría en el hospital, el hecho de que no pueda saber quién ha accedido a la información que se utiliza para prestar los servicios.
- **"[T]" (TRAZABILIDAD DE LOS DATOS):** esta clasificación pondera cual sería el impacto que tendría en el hospital, el hecho de que no pueda saber que se ha hecho con la información o no se pueda conocer quien hace que y cuando con el servicio.
- **"[D]" (DISPONIBILIDAD):** esta clasificación pondera cual sería el impacto que tendría en el hospital, el hecho de que se deje de prestar los servicios.

Resultado de esta ponderación se obtuvo que dentro de los activos encontremos como en estado crítico las siguientes categorías de aplicaciones:

- ✓ Dinamica Gerencial
- ✓ El Backup
- ✓ Sql server

A causa de que estos son la base fundamental del sistema de información que maneja el hospital. En la siguiente figura veremos cuál fue la ponderación obtenida en el software Pilar de este grupo de activos.

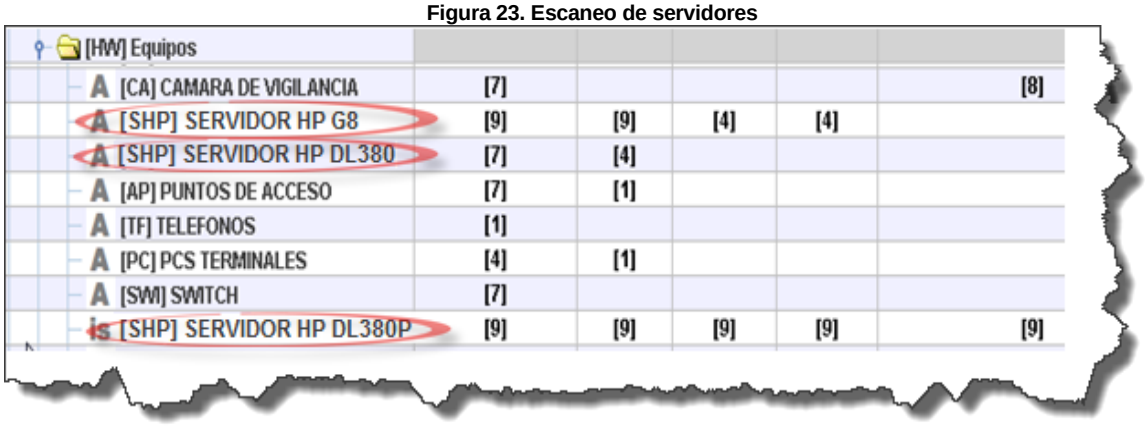
Figura 22. Ponderación de Activos del Hospital

[E] Equipamiento					
[SW] Aplicaciones					
[SO] SISTEMAS OPERATIVOS	[9]	[7]	[5]	[3]	[1]
[OF] SOFTWARE OFIMATICA	[1]	[1]	[1]		[1]
[DE] SOFTWARE DESARROLLO	[4]				
[NA] NAVEGADORES	[5]				
[SM] SENDMAIL	[7]	[4]			
[UV] VNC SLAVIDOR CLIENTE	[1]	[1]			
[FS] FIRESTARTER	[7]				
[PA] PANDION	[1]				
[AN] ANTIVIRUS	[7]	[4]	[4]		[4]
[DG] DINAMICA GERENCIAL	[9]	[9]	[9]	[9]	[9]
[PH] PLATAFORMA HOSPITAL	[7]	[4]	[4]	[4]	[4]
[SQ] SQL SERVER	[10]	[10]	[9]	[9]	[9]
[TB] THUNDERBIRD	[4]	[1]	[1]		
[IIS] INTERNET INFORMATION SERVE	[9]	[7]			

Fuente: El autor

Continuando con el análisis de activos tenemos la categoría de equipos; dentro de los cuales encontramos algunos críticos como el servidor DL380 de las bases de datos y el servidor HP G8 de antivirus; los cuales representan una parte fundamental del sistema de información; ya que uno contiene toda la información y el software que utiliza el hospital para desarrollar todas sus actividades y el otro se encarga de evitar que se infecte el mismo o se propague uno de ellos a través de la topología de la red llegando a estropear el sistema operativo de las estaciones de trabajo.

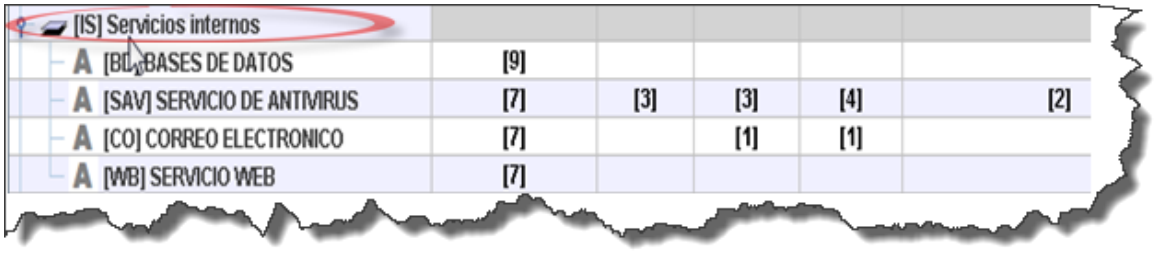
Figura 23. Escaneo de servidores



Fuente: El autor

Otra de las categorías que maneja el software Pilar son los servicios, que dentro de los cuales tenemos a los antivirus y los servicios que prestan las bases de datos; los cuales son uno de los pilares fundamentales del sistema de información ya que el antivirus se encarga de la seguridad y las bases de datos.

Figura 24. Ponderación de los Servicios del Hospital



Fuente: El autor

Adicionalmente a lo que se analizó en los ítems anteriores hay que tener en cuenta que las áreas como los racks o centrales de cableado, poseen soporte en la parte eléctrica, gracias a las ups y a la planta eléctrica con las que cuenta el hospital. Adicionalmente a lo anterior las bases de datos están configuradas de manera de cluster con el objetivo de respaldar el servicio en el momento de que algún servidor

falle; todo esto porque las bases de datos son uno de los activos mas críticos ya que si estas llegaran a fallar el sistema de información colapsaría; en conclusión estas deben estar en alta disponibilidad en todo momento.

7.5.2 Identificación de Amenazas.

Al realizar la evaluación de las amenazas se fundamentó en la frecuencia de materialización de la amenaza; lo que quiere decir que se valora la posibilidad de que se pueda ocurra realmente dicha amenaza; basado en la cantidad de veces que se pueda presentar en un año.
Para ello se debe tener en cuenta la siguiente escala de clasificación:

- 0,1 - una vez cada 10 años
- 1 - todos los años
- 10 Todos los meses
- 100 - todos los días

En la siguiente figura veremos los resultados sobre el análisis de las probabilidades de materialización de amenazas, teniendo como resultado que el activo Backup; ya que este presenta mayores probabilidades de que se materialicen las amenazas de acceso no autorizado ya que esto puede suceder todos los días y así mismo tenemos otras amenazas con frecuencia con valor de 10 que pueden materializarse durante el mes

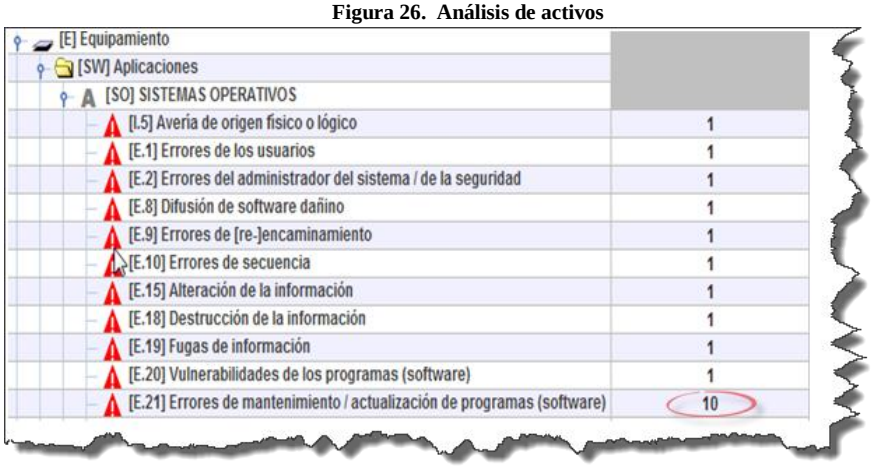
Figura 25. Amenazas Activo Backup

activo	frecuencia
ACTIVOS	
[D] DATOS	
[BK] BACKUP	
[E.1] Errores de los usuarios	10
[E.2] Errores del administrador del sistema / de la seguridad	1
[E.15] Alteración de la información	1
[E.18] Destrucción de la información	1
[E.19] Fugas de información	1
[A.5] Suplantación de la identidad del usuario	10
[A.6] Abuso de privilegios de acceso	10
[A.11] Acceso no autorizado	100
[A.15] Modificación de la información	10
[A.18] Destrucción de la información	10
[A.19] Revelación de información	10

Fuente: El autor

Analizando los resultados obtenidos en el análisis de los activos de aplicaciones; encontramos que la amenaza más frecuente son los errores de mantenimiento o actualización de software como se evidencia en la siguiente figura.

Figura 26. Análisis de activos



Fuente: El autor

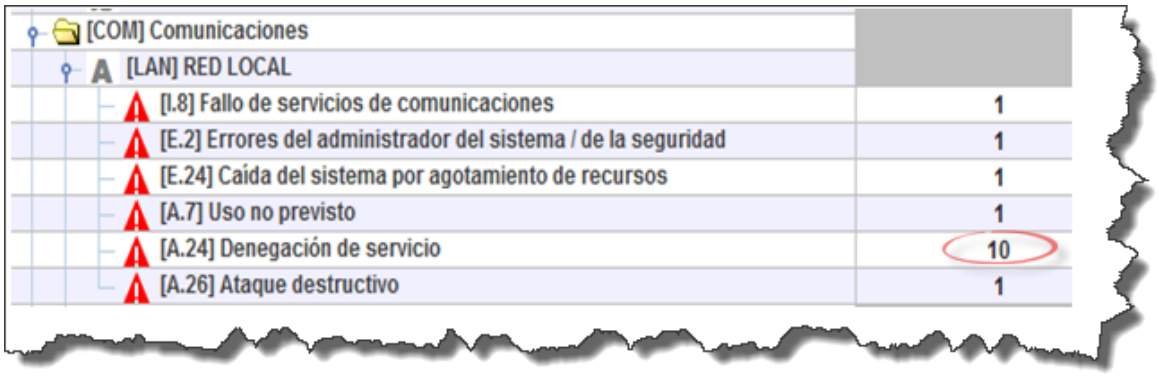
En el análisis realizado en la categoría de activos de equipos podemos evidenciar que la amenaza más recurrentes encontramos la caída del sistema por agotamiento de recursos; dentro de los dispositivos más importantes tenemos los servidores y los switches y debemos tener en cuenta que estos los tenemos ubicados en sitios donde el acceso es restringido; por lo tanto la amenaza depende única y exclusivamente de los recursos de los mismos.

Figura 27. Análisis de riesgos

Fuente: El autor

En el análisis realizado en la categoría de activos de comunicación encontramos que la amenaza más frecuente es la denegación del servicio; si se llegase a materializar podría ocasionar la caída del servicio e interrumpir el buen funcionamiento de las labores del hospital.

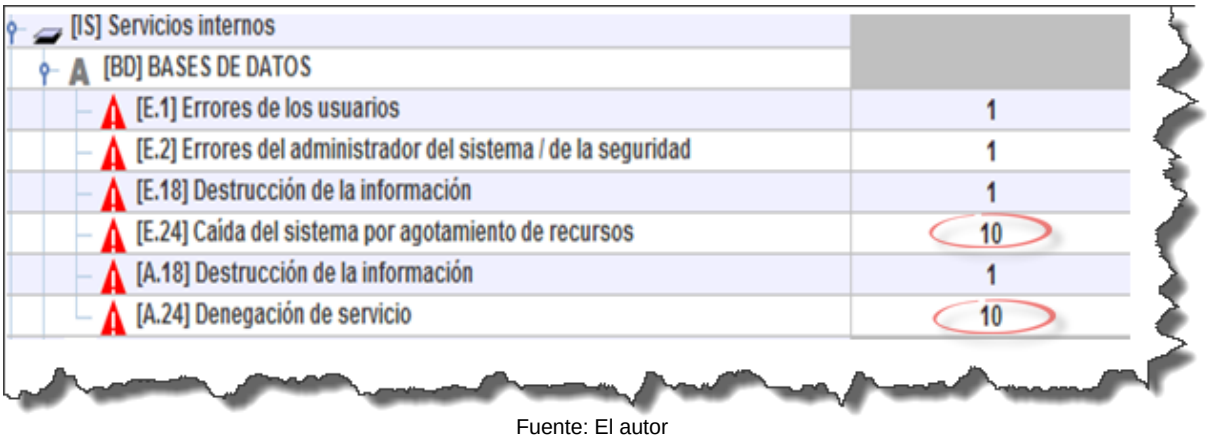
Figura 28. Amenazas activos comunicaciones



Fuente: El autor

Haciendo referencia al análisis de los servicios internos encontramos que las amenazas con mayor frecuencia son la caída del sistema por agotamiento de recursos; este depende de los recursos hardware donde se encuentra instalado el servicio y denegación del servicio se puede producir a causa de que está expuesto a este tipo de ataques.

Figura 29. Amenazas activos Servicios internos



Fuente: El autor

FASE 3: VALORACION

7.5.3 Identificación de Vulnerabilidades.

Esta identificación se realizó mediante las visitas que se llevaron a cabo en las instalaciones del hospital, a través de la inspección visual de todos y cada uno de los activos, adicionalmente a esto se aplicaron entrevistas al personal que interactúa

con el sistema de información y además se aplicaron herramientas de ethical hacking para evaluar vulnerabilidades en el sistema informático.

7.5.4 Entrevista al personal responsable de los recursos informáticos.

Para aplicar esta herramienta de recolección de información se elaboraron una serie de listas de verificación que están fundamentadas en unos estándares que permiten la plena evaluación de los activos que conforman el sistema de información.
Las listas se basaron en el Estándar EIA/TIA 568A y el reglamento RETIE5 (Reglamento Técnico de Instalaciones Eléctricas (RETIE) expedido por el Ministerio de Minas y Energía)

7.5.5 Lista de verificación sala de servidores.

A continuación, se muestran los resultados de la entrevista realizada al personal responsable del manejo del área de servidores.

Tabla 4. Resultados entrevista personal área de servidores

ELEMENTO CON LOS QUE DEBE CONTAR	**Si**	**No**
CUARTO DE ALOJAMIENTO DE SERVIDORES		
Altura de 2,50 metros en el cuarto de servidores se cumple.	x	
Número de estaciones que albergará la sala: hasta 100: 14 m2, entre 101 y 400: 37 m2, entre 401 y 800: 74 m2 y entre 801 y 1200: 111 m2. Numero de servidores:(4)	x	
Ubicado lejos de fuentes electromagnéticas.	x	
Esta cerca de Fuentes de inundación.		x
Tamaño de las puertas (sencilla 0,91 m, doble 2 m).	x	
Las puertas tienen retardante para el fuego.		x
Temperatura en el cuarto (19°).	x	
Humedad relativa (30%-55%).	x	
Iluminación (50-foot candles @ 1 m sobre el piso).	x	
Polvo en el medio ambiente.	x	
Cuenta con un equipo contra incendios al entrar al área.	x	
El cuarto es resistente al fuego.		x
Normas comunes de conservación y limpieza.	x	
No se utilizan paneles de obturación para los cables.	x	

La configuración de las losas perforadas no es apropiada.	x	
Existe cableado bajo el piso elevado que no se utiliza y puede eliminarse.		x
Cuenta con aisladores los racks**.**	x	
Cuenta con un sistema de marquillas en los equipo dentro del cuarto.		x
Equipos de respaldo para todos los elementos que interviene en el funcionamiento.	x	
Accesibilidad para el suministro de equipos.	x	
SEGURIDAD EN EL AREA		
Al Ingresar a la sala de servidores tiene un sistema de seguridad que le permita saber quién ingresó.		x
Cuenta con un sistema de seguridad de cámara de vigilancia.	x	
Tiene sistema de alarma contra incendios.		x
Tienen el sistema de alarmas de control de temperatura y humedad.		x
CABLEADO DE RED		
Categoría de cableado marque con una X: 5A___,6A_X__, 7A____	x	
Tipo de red marque con una X: clase A____, clase B___, clase C_X__	x	
Los puntos de red dentro de las áreas son los adecuados.		x
Cumple con el radio mínimo de curvaturas: 4x0 en funcionamiento.	x	
Diseño lógico de redes en el entorno marque con x: Anillo__, Bus_____, Mixta___, Malla___, Doble anillo___, Árbol_____, Estrella_X__	x	
Topologías y desempeño para cableado de fibra y cobre.	x	
Utilizan canaletas metálicas o plásticas para la protección del cableado en el edificio.	X	
Dentro de las oficinas los puntos de red están dispuestos a la distribución de las áreas.	x	
CABLEADO ELÉCTRICO		

El cable esta con la conformidad con los estándares de seguridad contra incendios: UL VW-1, IEC 332-1.		x
Estabilizadores de tensión.	x	
Transformadores de aislación.	x	
Tableros de distribución.	x	
Los puntos eléctricos dentro de las áreas son los adecuados y		x
La función del “back-bone” es proveer interconexión entre los	x	
Cuenta con señales de seguridad donde al vierta peligro de		x
TIERRA CONFIABLES		
Los gabinetes y los protectores de voltaje están conectados a una barra de cobre de polo a tierra.	x	
ENERGIA ININTERRUNPIDA UPS		
Protección de energía para servidores de nivel de entrada, Dispositivos pequeños de conexión en red y de más dispositivos.	x	
Protección de energía redundante de alto rendimiento con potencia y autonomía escalables para servidores.	x	
Protección de energía trifásica diseñada para cumplir con requisitos de infraestructuras pequeñas y grandes y aplicaciones para salas de equipos.	x	
Administración remota	x	
Fuentes de alimentación. Confiabilidad 24 x 7.	x	
AIRE ACONDICIONADO		
Ventiladores en la parte superior de los racks de los servidores.		x
Existen fugas en el piso elevado o en el sistema de suministro de aire.		x
Los puntos de referencia de los aires acondicionados son apropiados.		x
Climatización para la sala de servidores.		X
Controles de temperatura.		X
Cuenta con des humidificación y ventilación.		x
La configuración del sistema de retorno de aire es apropiada.		x

Tienen implementado un régimen de mantenimiento del sistema de enfriamiento.		x
Sensores dañados o sin calibrar.		x
Tuberías de suministro y retorno invertidas.		x
Válvulas defectuosas.		x
Hay sistemas de enfriamiento que no fueron puestos en		x

Fuente: El autor

A través de la aplicación de estos instrumentos obtuvimos las siguientes conclusiones de las condiciones en que se encuentra la sala de servidores del E.S.E Hospital San Bartolomé

La sala de servidores del Hospital cumple con las condiciones de distribución de equipos, sistemas de seguridad, iluminación, sistemas de respaldo eléctrico y por ende los sistemas eléctricos; pero se evidencia con preocupación que no existen sistemas de alarmas, dispositivos de control de acceso que permita determinar quién ingreso al sitio y para que ingreso, ni aire acondicionado o dispositivos que regulen la temperatura dentro de la sala, todo esto especificado en la norma estándar EIA/TIA 568A, TIA 942 para Data Center o sala de servidores.

7.5.6 Lista de Verificación Centro de Cableado (Área de Switches).

A continuación, se muestran los resultados de la entrevista realizada al personal responsable del manejo del área del centro de cableado principal.

Tabla 5. Resultados entrevista personal del centro de cableado principal.

ELEMENTO CON LOS QUE DEBE CONTAR	Si	No
Altura de 2,50 metros en el cuarto de servidores se cumple.	X	
Ubicado lejos de fuentes electromagnéticas.	X	
Esta cerca de Fuentes de inundación.		X
Tamaño de las puertas (sencilla 0,91 m, doble 2 m).	X	
Las puertas tienen retardante para el fuego.		X
Temperatura en el cuarto (19°).	X	
Humedad relativa (30%-55%).	X	
Iluminación (50-foot candles @ 1 m sobre el piso).		X
Polvo en el medio ambiente (100 microgramos/m3 en un período de 24 horas).		X
Cuenta con un equipo contra incendios cercano.	X	
El cuarto es resistente al fuego.		X
Normas comunes de conservación y limpieza.		X
No se utilizan paneles de obturación para los cables.	X	
Existe cableado bajo el piso elevado que no se utiliza y puede eliminarse.		X
Cuenta con aisladores los racks**.**	X	
Cuenta con un sistema de marquillas en los equipo dentro del cuarto.	X	
Equipos de respaldo para todos los elementos que interviene	X	

Accesibilidad para el suministro de equipos.	X	
SEGURIDAD EN EL ÁREA		
Al Ingresar a la sala de Switches tiene un sistema de seguridad que le permita saber quién ingreso.		X
Cuenta con un sistema de seguridad de cámara de vigilancia.		X
Tiene sistema de alarma contra incendios.		X
Tienen el sistema de alarmas de control de temperatura y humedad.		X
CABLEADO DE RED		
Categoría de cableado marque con una X: 5ª____,6A_X_,7A_____	X	
Tipo de red marque con una X: clase A_____, clase B____, clase C_X_	X	
Los puntos de red dentro de las áreas son los adecuados.	X	
Cumple con el radio mínimo de curvaturas: 4x0 en funcionamiento.	X	
Diseño lógico de redes en el entorno marque con x: Anillo__, Bus___, Mixta_____, Malla_____, Doble anillo_____, Árbol_____, Estrella _X_____	X	
Topologías y desempeño para cableado de fibra y cobre.	X	
Utilizan canaletas metálicas o plásticas para la protección del cableado en el edificio.		
Dentro de las oficinas los puntos de red y eléctrico están dispuestos con la norma.	X	
CABLEADO ELÉCTRICO		
El cable esta con la conformidad con los estándares de seguridad contra incendios: UL VW-1,IEC 332-1.		X
Estabilizadores de tensión.	X	
Transformadores de aislación.	X	
Los puntos eléctricos dentro de las áreas son los adecuados y	X	
La función del “back-bone” es proveer interconexión entre los	X	
Cuenta con señales de seguridad donde al vierta peligro de corto circuito o peligro.		X
ÁREA DE TIERRA CONFIABLES		
Los gabinetes y los protectores de voltaje son conectados a una barra de cobre (busbar) con “agujeros” (de 2” x 1/4”)	X	
Estas barras se conectan al sistema de tierras (grounding backbone) mediante un cable de cobre cubierto con material aislante (mínimo número 6 AWG, de color verde o etiquetado de manera adecuada	X	
ENERGIA ININTERRUMPIDA UPS		
Protección de energía funcional para equipos de computación voz y datos.	X	
Protección de energía para servidores de nivel de entrada, Dispositivos pequeños de conexión en red y dispositivos de punto	X	
Protección de energía redundante de alto rendimiento con potencia y autonomía escalables para la redes de voz y datos	X	
Administración remota	X	
Fuentes de alimentación. Confiabilidad 24 x 7.	X	

AIRE ACONDICIONADO		
Ventiladores en la parte superior del cuarto.		X
Existen fugas en el piso elevado o en el sistema de suministro de aire.		X
Los puntos de referencia de los aires acondicionados son apropiados.		X
Climatización para centros de ups.		X
Controles de temperatura.		X
Des humidificación y ventilación.		X
La configuración del sistema de retorno de aire es apropiada.		X
Tienen implementado un régimen de mantenimiento del sistema de enfriamiento.		X

Fuente: El autor

A través de la aplicación de estos instrumentos obtuvimos las siguientes conclusiones de las condiciones en que se encuentra el centro de cableado principal del E.S.E Hospital San Bartolomé

El centro de cableado principal del Hospital tiene una infraestructura en la parte eléctrica donde hay soporte del mismo en todo momento, además se encuentra ubicado en una zona donde puede ser evitada una eventualidad catastrófica como inundaciones o tormentas eléctricas que puedan afectar los equipos, además de esto cuando se presenta la necesidad de realizar mantenimiento los técnicos pueden intervenir directamente los equipos; caso contrario a lo anteriormente dicho esta sala no posee sistemas mínimos de seguridad para el acceso de personal, adicionalmente a esto la sala no cuenta con un sistema de refrigeración que permita controlar las condiciones climáticas adversas de sobrecalentamiento.

7.5.7 Lista de Verificación Sistemas Eléctricos y UPS.

Los resultados obtenidos con la aplicación de las entrevistas realizadas al personal que maneja los equipos eléctricos y de respaldo son:

Tabla 6. Resultados entrevista personal sistemas eléctricos.

ELEMENTO CON LOS QUE DEBE CONTAR	Si	No
Existencia de planos, esquemas, avisos que hay una fuente de energía y señales de estas mismas.	X	
Accesibilidad a todos los equipos de protección.	X	
Identificación de los conductores como Fase, Neutro y Tierra.	X	
Los materiales están acorde con las condiciones ambientales.	X	
Los niveles de iluminación están acorde con la norma para los hospitales según el RETIE.	X	
El sistema eléctrico del edificio cuenta con protección contra electrocución por contacto directo en las áreas de trabajo.	X	
El sistema eléctrico del edificio cuenta con protección contra electrocución por contacto indirecto en las áreas de trabajo.	X	

El sistema eléctrico del edificio cuenta con un proceso de certificación de los productos que se utilizan y también de la red eléctrica.	X	
Cuentan con un sistema de protección contra rayos.	X	
Están por separado los circuitos de la red regulada y normal	X	
Los tomas de la red regulada y normal están marcados con	X	
Ubicado lejos de fuentes electromagnéticas.	X	
Esta cerca de Fuentes de inundación.		X
Tamaño de las puertas (sencilla 0,91 m, doble 2 m).	X	
Las puertas tienen retar dante para el fuego.	X	
Temperatura en el cuarto (19°).	X	
Humedad relativa (30%-55%).	X	
Cuenta con un equipo contra incendios.	X	
El cuarto es resistente al fuego.	X	
Normas comunes de conservación y limpieza.	X	
Se utilizan paneles de obturación para los cables.	X	
Cuenta con un sistema de marquillas en el equipo dentro del cuarto y los circuitos de todo que están dentro del edificio.	X	
Accesibilidad para el suministro de equipos.	X	
SEGURIDAD EN EL ÁREA		
Al Ingresar al área de las plantas eléctricas cuenta con un sistema de seguridad que le permita saber quién ingreso.	X	
Cuenta con un sistema de seguridad de cámara de vigilancia.	X	
Tiene sistema de alarma contra incendios.	X	
Tienen el sistema de alarmas de control de temperatura y humedad.	X	
ENERGIA ININTERRUMPIDA/UPS		
Funcionamiento del corte automático de la alimentación.	X	
Administración remota	X	
Fuentes de alimentación. Confiabilidad 24 x 7.	X	
Las Ups son de batería: seca_____x___, liquida_____.	X	
La capacidad de soporte de cada ups está por circuitos.		
El mantenimiento de estas es cada: mes_3_, 6 meses_____, año_____, dos años_____	X	
CABLEADO ELÉCTRICO		
El cable esta con la conformidad con los estándares de seguridad contra incendios: UL VW-1,IEC 332-1.	X	
Estabilizadores de tensión.	X	
Transformadores de aislación.	X	
Tableros de distribución.	X	
Los puntos eléctricos dentro de las áreas son los adecuados y están acordes a la norma.	X	
Cuenta con señales de seguridad donde al vierta peligro de corto circuito	X	
TIERRA CONFIABLES		

Debe ser una barra de cobre, de 6 mm de espesor y 100 mm de ancho mínimos. El largo puede variar, de acuerdo a la cantidad de cables que deban conectarse a ella.	X	
Continuidad de los conectores de tierra y conectores equipotenciales.	X	
Estas barras se conectan al sistema de tierras mediante un cable de cobre cubierto con material aislante (mínimo número 6 AWG, de color verde o etiquetado de manera adecuada.	X	
AIRE ACONDICIONADO		
Los puntos de referencia de los aires acondicionados son apropiados.	X	
Controles de temperatura.	X	
Des humidificación y ventilación.	X	
La configuración del sistema de retorno de aire es apropiada.	X	
Sensores dañados o sin calibrar.		X

Fuente: El autor

A través de la aplicación de estos instrumentos se obtuvieron las siguientes conclusiones de las condiciones en que se encuentra el sistema eléctrico del E.S.E Hospital San Bartolomé

El sistema eléctrico del Hospital cuenta con los dispositivos de control automático que permitiría generarse un corte en el fluido eléctrico en caso de corto circuito; así como el de mantener el fluido normalmente para el buen funcionamiento del sistema, además la infraestructura del sistema eléctrico posee transformadores que permiten la regulación de la misma.

FASE 4: EJECUCION

7.5.8 Pruebas de Análisis de Vulnerabilidades Ethical Hacking.

Para la realización de este ítem se utilizaron las herramientas que trae el sistema operativo Kali Linux, como nmap, netcat, xprobe, netcat, user2sid, userdump; para realizar las pruebas de vulnerabilidad. Iniciaremos a utilizar el nmap para realizar el escaneo de las direcciones IP en uso en las diferentes estaciones de trabajo.

Se utilizó el sistema operativo Kali Linux con el programa nmap para realizar los siguientes escaneos en búsqueda de vulnerabilidades en los equipos y servidores del hospital.

Figura 30. Escaneo al primer servidor.

Fuente: El autor

En la figura anterior se realiza una exploración del primer servidor a través de la herramienta Nmap para efectuar un rastreo de puertos donde podemos determinar que vulnerabilidades posee el mismo. A través del análisis de paquetes ip crudos. Observamos abierto el puerto 22/tcp ssh el cual permite administrar remotamente otros ordenadores

Figura 31. Escaneo al segundo servidor.

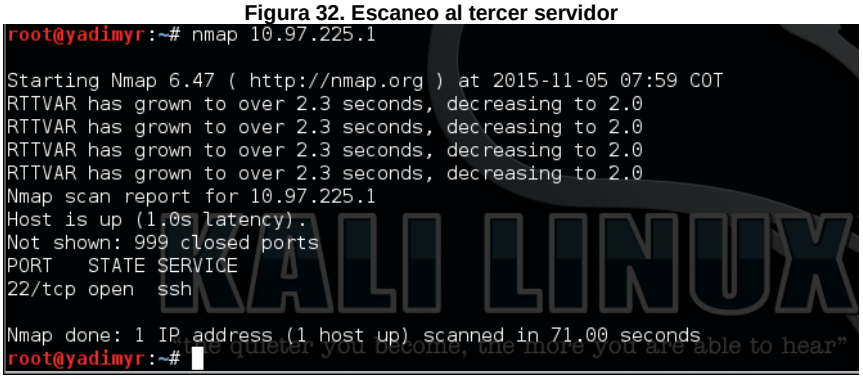
Fuente: El autor

En la figura anterior se realiza una exploración del segundo servidor a través de la herramienta Nmap para efectuar un rastreo de puertos donde podemos determinar que vulnerabilidades posee el mismo. A través del análisis de paquetes ip crudos.

En primer lugar encontramos abierto el protocolo para transferencia simple de correo 25/tcp (smtp), el protocolo de oficina de correos (pop3), el Protocolo de

acceso a mensajes de Internet (imaps) y otros puertos de mensageria interna y de correos.

Figura 32. Escaneo al tercer servidor



Fuente: El autor

En la figura anterior se realiza una exploración del tercer servidor a través de la herramienta Nmap para efectuar un rastreo de puertos donde podemos determinar que vulnerabilidades posee el mismo. A través del análisis de paquetes ip crudos. Se encuentra abierto el puerto 22 de ssh control de acceso remoto.

A continuación realizaremos un escaneo de puntos al azar (estaciones de trabajo) en los diversos puestos de trabajo del hospital, la identificación de cada una se dará por el nombre del trabajador que se desempeña en él.

Figura 33. Escaneo al equipo denominado WILLIAM.

Fuente: El autor

En la figura anterior se realiza una exploración de una estación de trabajo a través de la herramienta Nmap; donde se logra determinar que se hace necesario cambiar los banners para evitar dar información sobre el sistema operativo instalado en ellas. Observamos abierto el puerto netbios, utilizado para enlazar un sistema operativo de red con diverso hardware en la red.

Figura 34. Escaneo al equipo denominado CESAR

Fuente: El autor

En la figura anterior se realiza una exploración de una estación de trabajo a través de la herramienta Nmap; donde se logra determinar que se hace necesario cambiar los banners para evitar dar información sobre el sistema operativo instalado en ellas.

Adicionalmente a los puertos abiertos en los escaneos anteriores, aca observamos también abierto el puerto (ms-sql –s) que hace referencia a la falta de activación o utilización de un firewall.

Figura 35. Escaneo al equipo denominado ERICA.

Fuente: El autor

En la figura anterior se realiza una exploración de una estación de trabajo a través de la herramienta Nmap; donde se logra determinar que se hace necesario cambiar los banners para evitar dar información sobre el sistema operativo instalado en ellas.

Figura 36. Escaneo al equipo denominado CARLOS

Fuente: El autor

En la figura anterior se realiza una exploración de una estación de trabajo a través de la herramienta Nmap; donde se logra determinar que se hace necesario cambiar los banners para evitar dar información sobre el sistema operativo instalado en ellas.

Encontramos abierto un puerto virtualizado vmrdp el cual permite acceso remoto al escritorio, en un sistema no virtualizado utiliza por defecto el puerto 3389

Figura 37. Escaneo al equipo denominado NERY

Fuente: El autor

En la figura anterior se realiza una exploración de una estación de trabajo a través de la herramienta Nmap; donde se logra determinar que se hace necesario cambiar los banners para evitar dar información sobre el sistema operativo instalado en ellas.

Observamos abiertos puertos similares a los anteriores casos aparece también el puerto ms – olap4 utilizado para administrar los clientes de servicios OLAP a través de una intranet, extranet o internet, son generalmente usados por el servidor y el cliente.

Figura 38. Escaneo al equipo denominado ANGYE

Fuente: El autor

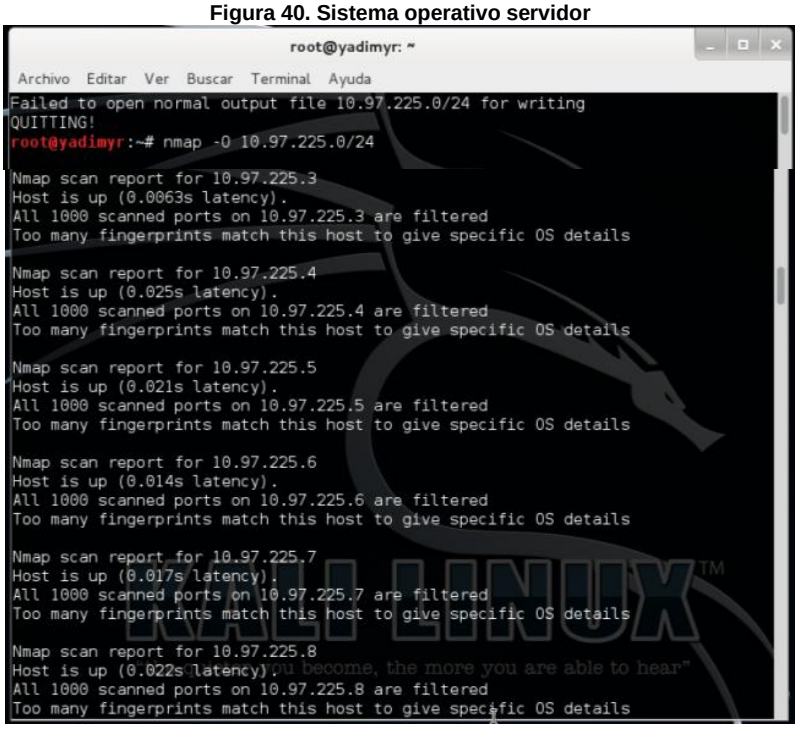
En la figura anterior se realiza una exploración de una estación de trabajo a través de la herramienta Nmap; donde se logra determinar que se hace necesario cambiar los banners para evitar dar información sobre el sistema operativo instalado en ellas.

Figura 39. Prueba de escaneos de puertos en los servidores

Fuente: El autor

De igual forma se realizó una prueba para detectar el sistema operativo de uno de los servidores y como se muestra en la siguiente figura, se observa que esta no representa una vulnerabilidad, pues no muestra exactamente el nombre del sistema operativo que utilizan.

Figura 40. Sistema operativo servidor

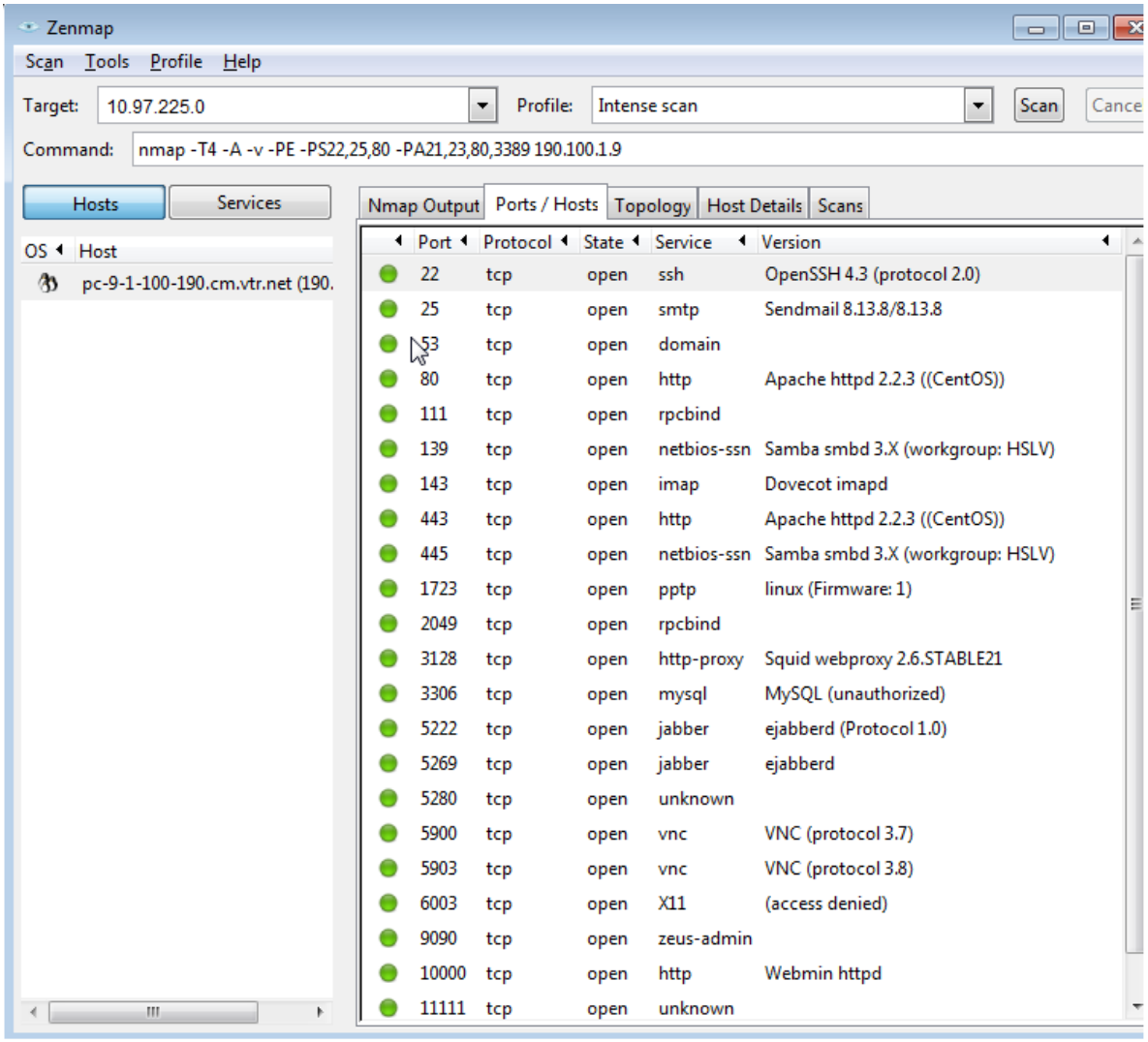


Fuente: El autor

En la figura anterior a través de la herramienta Nmap analizamos un servidor; y se logra determinar que no este no da información sobre el sistema operativo instalado en él.

Por último se aplicaron escaneos con Zenmap para hallar las vulnerabilidades las cuales se muestran en las siguientes figuras esto con el fin de corroborar los resultados obtenidos anteriormente en las cuales se observaron puertos abiertos tanto en servidores como en los demás equipos de estaciones de trabajo.

Figura 41. Escaneo de vulnerabilidades con Zenmap



Fuente: El autor

En este grafico se observan vulnerabilidades similares descritas a los procesos anteriores realizadas con n-map, adicionalmente se muestra abierto el puerto del servidor apache para un servidor con sistema operativo CentOS, también observamos abierto el puerto 3306 utilizado por defecto por bases de datos Mysql, lo cual representa una gran amenaza para sistemas de información del hospital San Bartolomé. El puerto 9090 también es vulnerable hace referencia al puerto Zeus admin pues básicamente es un virus, gusano que infecta todo el sistema

7.5.9 Análisis de Vulnerabilidades.

Al tener identificados los activos y a su vez se hallan terminado los escaneos y pruebas de vulnerabilidad, podemos realizar un análisis de amenazas y formular una posible recomendación que logre mitigar o minimizar el impacto de la misma; para ello veremos la siguiente tabla:

Tabla 7 Análisis de vulnerabilidades

TIPO	DESCRIPCION	RECOMENDACIONES
Amenaza	Se puede evidenciar que en el acceso a la sala de servidores no hay una puerta de madera y no cuenta con algún sistema que retrase la acción del fuego en caso de incendio, tampoco cuenta con un sistema de acceso biométrico.	Se recomienda cambiar la puerta por una que tenga sistema biométrico de acceso y con componentes electro mecánicos para auto cerrado de las mismas
Riesgo	El cuarto donde se encuentran los servidores cuenta con un grupo de ventanas las cuales no tienen vidrios de seguridad que posiblemente ocasionen cortadas o daños al personal de la empresa.	Es recomendado utilizar una ventana con vidrios de seguridad que soporten gran presión o en otro caso cerrar los espacios de esa ventana.
Riesgo	En la sala de servidores se encuentran materiales como madera, cartón, cortinas de tela y sintéticas, y estos materiales al ocasionarse un corto circuito o un incendio ayudaran a que el incendio se propague mucho más rápido.	Se recomienda trasladar de esta instalación este tipo de material ya que sería un riesgo para la sala de servidores
Riesgo	En la sala de servidores además se observa que alguno de los módems con su respectivo cableado no se encuentran bien ubicados como lo recomiendan los estándares, poniendo ocasionar un incidente al ingreso de las personas, las cuales se pueden enredar con dichos cables.	Se recomienda que estos dispositivos se ubiquen de forma correcta.
Riesgo	En la primera visita se encontró un servidor ubicado en una mesa de madera lo cual no es recomendado puesto que en caso de corto circuito o sobrecalentamiento del mismo, podría ocasionar un incendio.	Se recomienda adquirir una base o soporte de metal con resistencia suficiente.
Riesgo	Se halló una silla plástica lo cual no es recomendado por ser considerado como frágil al calor y en caso de incendio ayuda a propagar más rápido las llamas.	Se recomienda cambiarla por una de metal
Riesgo	En el área de servidores, no se cuenta con dispositivos detectores de calor, de humo, o fuego ni humedad.	Se recomienda la utilización e instalación de estos dispositivos que son de suma importancia para este área de servidores
Vulnerabilidad	Se encontró que los servidores no	Se recomienda identificar

	cuentan con etiquetas para su identificación, la cual debe ir de acuerdo a sus aplicaciones y servicio que prestan dentro de la empresa.	por medio de etiquetas estos servidores dependiendo el servicio que prestan.
Riesgo	Se encontró que en la sala donde se encuentran los rack no se cuenta con un sistema de cámaras de video que vigilen el ingreso de personal a la sala de servidores.	Se recomienda ampliar el sistema de dvr para permitir instalar cámaras para vigilar el acceso a los servidores.
vulnerabilidad	Se hallaron servidores y racks en estado de mal aseo, tanto a su alrededor como polvo sobre los mismos.	Se recomienda realizar campañas periódicas de aseo para mantener en buen estado todos los equipos de red de esta sala.
vulnerabilidad	Algunas áreas de la sala de servidores tienen desorden en su cableado y algunos tomas de corriente están en mal estado.	Se recomienda utilizar espirales para organizar los cables que están en desorden e introducir dentro de las canaletas los que se puedan organizar en ellas.
Riesgo	En la parte de oficinas se observa que los empleados de los equipos toman bebidas y comen al estar interactuando con los dispositivos de trabajo.	Se recomienda hacer campañas de sensibilización sobre el no consumo de productos ni bebidas sobre los equipos de trabajo.
Riesgo	Se encontró que no hay configurado en el sistema operativo un sistema de protector de pantallas en un lapso de tiempo de inactividad del servicio del negocio.	Se hace la recomendación para configurar estos servicios en los sistemas operativos.
vulnerabilidad	Se encontró que los equipos que se encuentran ubicados en la sección de enfermería y en hospitalización se encuentran mal ubicados y el cableado de estos se puede enredar y causar des conectividad y posible incidente con el personal.	Se recomienda ubicar estos equipos y utilizar espirales para recoger los cables.
Riesgo	Se ha encontrado que en la planta eléctrica antigua hay una pequeña fuga de combustible en el tanque de la planta eléctrica.	Se recomienda de forma inmediata reparar o remplazar dicho tanque de combustible para la planta.
Riesgo	Se encontró en la parte superior de la subestación electica que esta es atravesada por los tubos de agua los cuales al generar una eventualidad de desastre al edificio estos pueden romperse y causar un grave incidente para la planta física.	Se recomienda cambiar la forma como están ubicados estos tubos.
Riesgo	No se cuenta con una política de control que permita registrar o referenciar el acceso a los archivos ejecutables de las aplicaciones en producción.	Se recomienda la creación de una política para cumplir con el objetivo de este control.

Riesgo	No se cuanta con un sistema para llevar el control de copias de seguridad en los sistemas de información.	Se recomienda la creación de una política para cumplir con el objetivo de este control.
Riesgo	Se evidencia que el hospital San Bartolomé no ha adquirido un contrato con una entidad externa para guardar una copia adicional fuera de la institución.	Se recomienda la creación de una política para cumplir con el objetivo de este control.
Vulnerabilidad	Se evidencia que el hospital no se tiene ningún control en la utilización de los recursos de equipos de cómputo.	Se recomienda la creación de una política para cumplir con el objetivo de este control.
Riesgo	En el requerimiento de soporte no se cuenta con un contrato que obligue el proveedor a brindar soporte a dinámica gerencial.	Es recomendado realizar la contratación de un proveedor que cumpla con este requerimiento.
Riesgo	Se encontró que el sistema de firewall presenta un contrato de soporte con vigencia de un año.	Se recomienda ampliar estos plazos o realizar contrato de licencias definitivas.
Vulnerabilidad	Se evidencia la existencia de un aplicativo donde se registra los cambios en los equipos, hay una planilla de soporte para los equipos. Pero este no es un documento o procedimiento formal.	Es recomendado realizar un procedimiento formal para cumplir con este requerimiento.
Riesgo	Se encuentra que para la solicitud de los cambios se expone en un comité, luego se envía la solicitud de cambios al proveedor para página web.	Se recomienda la elaboración un contrato o documento formal que responsabilice al proveedor de este procedimiento.
Vulnerabilidad	Se evidencia la falta de un empleado cuyo objeto del contrato sea brindar soporte de peticiones como entrar a la página para realizar las solicitudes.	Realizar la contratación de un empleado para este fin.
Riesgo	Se encuentra que no existe un reporte para verificar la eficiencia y evaluación de resultados del soporte.	Se recomienda verificar por medio de reportes los resultados de este trámite con los proveedores.
Amenaza	En la actualidad no se cuenta con los procedimientos en los cuales se soporte la necesidad de adquirir nuevos dispositivos de red y de implementar nuevas redes de datos	Se le recomienda que se generen un formato donde se marque con niveles de importancia de tener que adquirir nuevos elementos de red, software y otros equipos. Es un procedimiento de control por servicios
Vulnerabilidad	No se cuenta con un formato de los pasos en de los cuales estén enmarcados las actividades a seguir y que queden evidenciados estos procesos al realizar un cambio de los dispositivos.	Se recomienda crear un formato en donde se evanecían los cambios que se realizan en estas tareas.

Vulnerabilidad	Se evidencia que los equipos que se compran nuevos en muchas ocasiones no se les realizan las pruebas pertinentes por el personal encargado sino que se instalan en el ambiente directamente.	Se recomienda crear un formato en donde se evanecían los cambios realizados a los equipos.
Vulnerabilidad	No se cuenta con un diseño actualizado de la topología de red en el edificio, pero si se cuenta con marquillas de identificación de los puntos de red y los dispositivos de red No hay ningún formato	Se recomienda generar un procedimiento en el cual se enmarque las actividades a seguir en estos casos y que quedes evidenciados los pasos que se realizaron.
Vulnerabilidad	Se evidencia la falta de un plano completo de la red de datos para facilitar y agilizar procesos de distribución y reparación de posibles daños.	Se le recomienda al área de informática generar y diseñar planos
Vulnerabilidad	Se observa que los equipos que tienen el SO Windows no están activados con licencias auténticas.	Se recomienda adquirir licencias para los equipos que no cuentan con estas.

Fuente: El autor

7.5.10 Resultados de las pruebas de ethical hacking, entrevistas y desarrollo de encuestas

Tabla 8. Resultados etical hacking

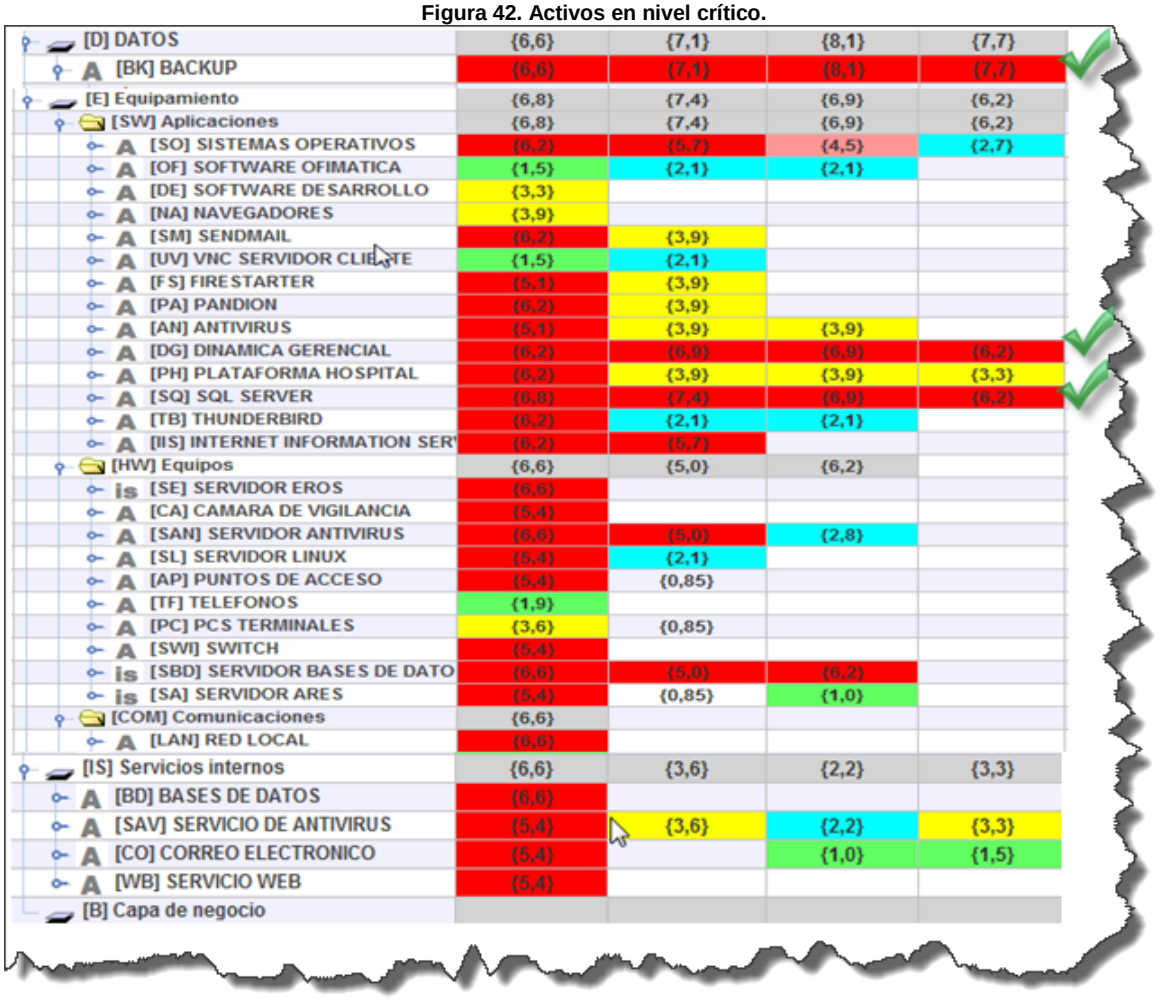
Item	# ACTIVOS VULNERABLES	Nombre Plugin	GRAVEDAD (A – M – B)	VULNERABILIDAD	DESCRIPCION	SOLUCION
41028	3	Por defecto del agente SNMP de nombre de comunidad (público)	Gravedad Alta	El nombre de comunidad SNMP del servidor remoto se puede descifrar. Dispositivo: 10.97.225.1	Es posible obtener el nombre de comunidad por defecto del mando a distancia Servidor SNMP. Un atacante puede utilizar esta información para adquirir más conocimientos acerca de la host remoto, o para cambiar la configuración del sistema remoto (En caso de la comunidad por defecto que permiten modificaciones).	Deshabilitar el servicio SNMP en el host remoto, si no lo utiliza, filtro de entrada paquetes dirigidos a este puerto, o cambiar la configuración predeterminada cadena de comunidad.
53514	3	MS11-030: Una vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código (2509553) (ver a distancia)	Gravedad Alta	Escribe texto o la dirección de un sitio web, o bien, traduce un documento. Arbitraria de código se puede ejecutar en la máquina remota a través de la instalación del cliente DNS de Windows. Dispositivos: 10.97.225.11 10.97.225.10 10.97.225.1	Una falla en la forma en que el cliente DNS de Windows instalados procesos de enlace local de resolución de nombres de multidifusión (LLMNR) consultas puede ser utilizada para ejecutar código arbitrario en el contexto de la cuenta Network. Tenga en cuenta que Windows XP y 2003 no son compatibles con la explotación LLMNR y éxito en esas plataformas requiere acceso local y la capacidad de ejecutar una aplicación especial. El R2 de Windows Vista, 2008, 7, y 2008, sin embargo, el problema puede ser explotado de forma remota.	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y Server 2008 R2: http://www.microsoft.com/technet/security/Bulletin/MS11-030.mspx
34460	1	Web de detección de servidores obsoletos	Gravedad Alta	El servidor web remoto es obsoleto. Dispositivos: 10.97.225.7	Según su versión, el servidor web remoto es obsoleto y ya no se mantiene por su vendedor o proveedor. La falta de apoyo no implica que nuevos parches de seguridad están siendo liberadas por él.	Quitar el servicio si ya no es necesario. De lo contrario, la actualización a una versión más reciente, si es posible o cambiar a otro servidor.

Fuente: El autor

7.5.11 Impacto.

Este indica las consecuencias que puede producir la materialización de una amenaza; en este caso en particular vemos que tenemos algunos activos que están en un nivel crítico (dinámica gerencial, backup y Sql server); evidencia de esto veremos la siguiente imagen.

Figura 42. Activos en nivel crítico.



[D] DATOS	{6,6}	{7,1}	{8,1}	{7,7}
[BK] BACKUP	{6,6}	{7,1}	{8,1}	{7,7}
[E] Equipamiento	{6,8}	{7,4}	{6,9}	{6,2}
[SW] Aplicaciones	{6,8}	{7,4}	{6,9}	{6,2}
[SO] SISTEMAS OPERATIVOS	{6,2}	{5,7}	{4,5}	{2,7}
[OF] SOFTWARE OFIMATICA	{1,5}	{2,1}	{2,1}	
[DE] SOFTWARE DESARROLLO	{3,3}			
[NA] NAVEGADORES	{3,9}			
[SM] SENDMAIL	{6,2}	{3,9}		
[UV] VNC SERVIDOR CLIENTE	{1,5}	{2,1}		
[FS] FIRESTARTER	{5,1}	{3,9}		
[PA] PANDION	{6,2}	{3,9}		
[AN] ANTIVIRUS	{5,1}	{3,9}	{3,9}	
[DG] DINAMICA GERENCIAL	{6,2}	{6,9}	{6,9}	{6,2}
[PH] PLATAFORMA HOSPITAL	{6,2}	{3,9}	{3,9}	{3,3}
[SQ] SQL SERVER	{6,8}	{7,4}	{6,9}	{6,2}
[TB] THUNDERBIRD	{6,2}	{2,1}	{2,1}	
[IIS] INTERNET INFORMATION SER	{6,2}	{5,7}		
[HW] Equipos	{6,6}	{5,0}	{6,2}	
[SE] SERVIDOR EROS	{6,6}			
[CA] CAMARA DE VIGILANCIA	{5,4}			
[SAN] SERVIDOR ANTIVIRUS	{6,6}	{5,0}	{2,8}	
[SL] SERVIDOR LINUX	{5,4}	{2,1}		
[AP] PUNTOS DE ACCESO	{5,4}	{0,85}		
[TF] TELEFONOS	{1,9}			
[PC] PCS TERMINALES	{3,6}	{0,85}		
[SWI] SWITCH	{5,4}			
[SBD] SERVIDOR BASES DE DATO	{6,6}	{5,0}	{6,2}	
[SA] SERVIDOR ARES	{5,4}	{0,85}	{1,0}	
[COM] Comunicaciones	{6,6}			
[LAN] RED LOCAL	{6,6}			
[IS] Servicios internos	{6,6}	{3,6}	{2,2}	{3,3}
[BD] BASES DE DATOS	{6,6}			
[SAV] SERVICIO DE ANTIVIRUS	{5,4}	{3,6}	{2,2}	{3,3}
[CO] CORREO ELECTRONICO	{5,4}		{1,0}	{1,5}
[WB] SERVICIO WEB	{5,4}			
[B] Capa de negocio				

Fuente: El autor

Para poder entender la imagen anterior debemos tener claridad de cuáles son sus parámetros:

- ✓ **Activos:** representa el activo que va a ser valorado.
- ✓ **Amenaza:** esta variable fue agrupada según su origen, donde cada una de ellas tiene un código; los códigos se evidencian porque están dentro de corchetes.

- ✓ **Dimensión:** este representa la dimensión que ha sido definida previamente. En este análisis en particular se utilizaron dimensiones como [D] disponibilidad, [I] integridad, [C] Confidencialidad, [A] Autenticidad y [T] Trazabilidad.
- ✓ **V (Valor):** representa el valor del activo.
- ✓ **VA (Valor acumulado):** representa el valor acumulado del activo (la suma del valor del propio activo más el valor de los activos que dependen de él.)
- ✓ **D (Degradación):** representa la degradación que le provoca la amenaza al activo.
- ✓ **I (Impacto):** representa el impacto que le provoca la materialización de la amenaza al activo.
- ✓ **Frecuencia:** representa la frecuencia o estimación con la que se puede materializar una amenaza.

A continuación veremos cuál es el riesgo acumulado que tiene ciertos activos; donde podemos evidenciar que algunos de ellos se encuentran en un nivel crítico; entre ellos se encontraron los que tienen relación directa con los aplicativos y las bases de datos.

Tabla 9. La tabla de riesgo acumulado

Activo	Amenaza	Dimensión	V	VA	D	I	F	Riesgo
[BK] BACKUP	[A.11] Acceso no autorizado	[C]	[10]	[10]	50%	[9]	100	{8,1}
[BK] BACKUP	[A.19] Revelación de información	[C]	[10]	[10]	100%	[10]	10	{7,7}
[BK] BACKUP	[A.5] Suplantación de la identidad del usuario	[A]	[10]	[10]	100%	[10]	10	{7,7}
[SW.SQ] SQL SERVER	[A.22] Manipulación de programas	[I]	[10]	[10]	100%	[10]	5	{7,4}
[BK] BACKUP	[A.6] Abuso de privilegios de acceso	[C]	[10]	[10]	50%	[9]	10	{7,2}
[BK] BACKUP	[A.5] Suplantación de la identidad del usuario	[C]	[10]	[10]	50%	[9]	10	{7,2}
[BK] BACKUP	[A.15] Modificación de la información	[I]		[9]	100%	[9]	10	{7,1}
[SW.DG] DINAMICA GERENCIAL	[A.22] Manipulación de programas	[C]	[9]	[9]	100%	[9]	5	{6,9}

[SW.DG] DINAMICA GERENCIAL	[A.22] Manipulación de programas	[I]	[9]	[9]	100%	[9]	5	{6,9}
[SW.SQ] SQL SERVER	[A.22] Manipulación de programas	[C]	[9]	[9]	100%	[9]	5	{6,9}
[SW.SQ] SQL SERVER	[A.8] Difusión de software dañino	[I]	[10]	[10]	100%	[10]	1	{6,8}
[SW.SQ] SQL SERVER	[A.7] Uso no previsto	[D]	[10]	[10]	100%	[10]	1	{6,8}
[SW.SQ] SQL SERVER	[A.8] Difusión de software dañino	[D]	[10]	[10]	100%	[10]	1	{6,8}
[BD] BASES DE DATOS	[E.24] Caída del sistema por agotamiento de recursos	[D]	[9]	[9]	50%	[8]	10	{6,6}
[BK] BACKUP	[A.18] Destrucción de la información	[D]	[4]	[9]	50%	[8]	10	{6,6}
[HW.SAN] SERVIDOR HP G8	[E.24] Caída del sistema por agotamiento de recursos	[D]	[9]	[9]	50%	[8]	10	{6,6}
[HW.SE] SERVIDOR EROS	[E.24] Caída del sistema por agotamiento de recursos	[D]	[9]	[9]	50%	[8]	10	{6,6}
[COM.LAN] RED LOCAL	[A.24] Denegación de servicio	[D]	[9]	[9]	50%	[8]	10	{6,6}
[BD] BASES DE DATOS	[A.24] Denegación de servicio	[D]	[9]	[9]	50%	[8]	10	{6,6}

Fuente: El autor

Los resultados de la tabla anterior fueron obtenidos a través de la herramienta pilar; y podemos observar una descripción detallada de en qué estado se encuentra cada activo del Hospital.

7.5.11 Salvaguardas y Controles.

Para minimizar los riegos a los que está expuesto el sistema de información del Hospital, es necesario mejorar las salvaguardas existentes o si es necesario realizar la incorporación de otras nuevas.
Debemos tener claro que lo que se pretende a través de los salvaguardas es la reducción de los riesgos a través de dispositivos físicos o lógicos, que permitan realizar la neutralización antes de que se materialice la amenaza o la reducción del resultado de la agresión.

En el programa aparecen gráficamente unos paraguas que significan de acuerdo a su color lo siguiente:

-  Interesante.
-  Importante.
-  Muy importante.
-  Crítica.

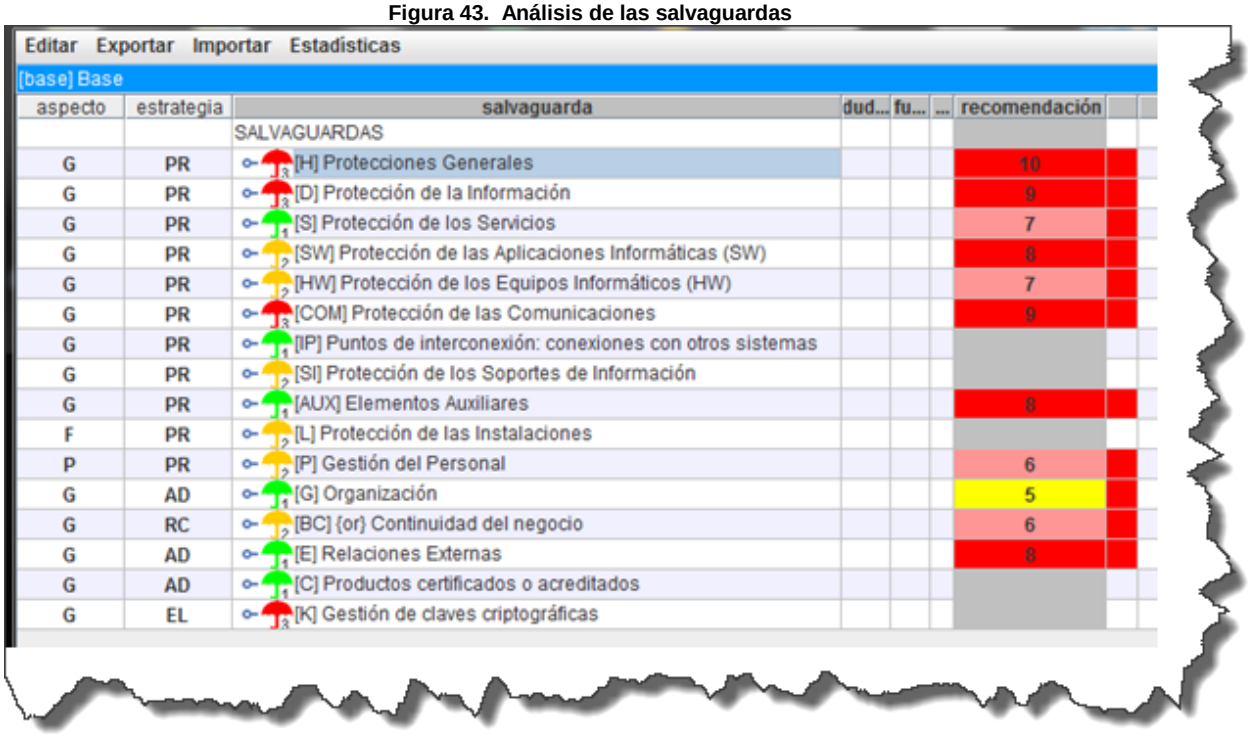
Dentro de los resultados obtenidos por el programa Pilar, presenta una serie de aspectos y estrategias, los cuales debemos tener claros para la interpretación del resultado y estas son:

- ✓ **Aspectos :**
  - G: Gestión.
  - T: Técnico.
  - P: Personal.
  - F: Seguridad física.
- ✓ **Estrategia**: representa la estrategia que toma la salvaguarda frente a los incidentes para mitigarlos o eliminarlos; dentro de ellas tenemos los siguientes valores:

CR (Corrección): Se parte de que ya se produjo un daño y debe ser corregido o reparado
EL (Eliminación): actúa antes de que el incidente ocurra e impide que este tenga lugar en sistema de información.
PR (Prevención): es preventiva cuando se reducen las oportunidades de que un incidente ocurra.
IM (Minimización / limitación del impacto): Se dice que se minimiza el impacto cuando limita las consecuencias de un incidente.
DR (Disuasión): este valor nos indica que genera un efecto tal sobre los atacantes que logra que ellos no se atrevan a atacar al sistema.
DT (Detección): funciona detectando un ataque e informando de que este está ocurriendo; permitiendo que entren en operación otras medidas que mitiguen la progresión del ataque, minimizando daños.

RC (Recuperación): Se ofrece recuperación cuando permite regresar al estado anterior al incidente.
MN (Monitorización): como su nombre lo indica trabajan monitorizando lo que está ocurriendo reaccionando ante un incidente limitando su impacto.
AW (Concienciación): son las capacitaciones de las personas que interactúan con el sistema teniendo como objetivo la reducción de los errores de los mismos, lo cual tiene un efecto preventivo.
AD (Administración): se refiere a la administración de los componentes de seguridad del sistema. Tiene como objetivo evitar dejar puertas abiertas que permitan el éxito de un ataque.
STD (Normativa, Standard): Se refiere a las salvaguardas basadas en normas.
PROC (Procedimiento de seguridad): Se refiere a las salvaguardas basadas en procedimientos.
CERT (Producto certificado): Se refiere a las salvaguardas basadas en productos certificados.

Figura 43. Análisis de las salvaguardas



aspecto	estrategia	salvaguarda	dud...	fu...	...	recomendación		
		SALVAGUARDAS						
G	PR	[H] Protecciones Generales				10		
G	PR	[D] Protección de la Información				9		
G	PR	[S] Protección de los Servicios				7		
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				8		
G	PR	[HW] Protección de los Equipos Informáticos (HW)				7		
G	PR	[COM] Protección de las Comunicaciones				9		
G	PR	[IP] Puntos de interconexión: conexiones con otros sistemas						
G	PR	[SI] Protección de los Soportes de Información						
G	PR	[AUX] Elementos Auxiliares				8		
F	PR	[L] Protección de las Instalaciones						
P	PR	[P] Gestión del Personal				6		
G	AD	[G] Organización				5		
G	RC	[BC] {or} Continuidad del negocio				6		
G	AD	[E] Relaciones Externas				8		
G	AD	[C] Productos certificados o acreditados						
G	EL	[K] Gestión de claves criptográficas						

Fuente: El autor

De acuerdo a los resultados obtenidos podemos observar que debemos tomar acciones correctivas a las protecciones generales y protección de la información; ya que son un activo muy importante para el hospital porque allí se maneja información confidencial; protección de las comunicaciones y la gestión de claves criptográficas; ya que esto representa tanto la conectividad de las comunicaciones

como el control de acceso tanto a la red como a la información que viaja por ella, es por eso que debemos tener en cuenta la importancia de las encriptación de las comunicaciones.

FASE 5: PRODUCTO FINAL

8. DEFINICIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS.

8.1 Política de Seguridad de la Información.

Esta política tiene como objetivo proteger tanto la información del hospital como la tecnología que la contiene; frente a las amenazas que están expuestos, ya sean de origen externo e interno. Todo esto basado en los pilares de la seguridad de la información como confidencialidad, integridad, disponibilidad y confiabilidad de la información.

8.1.1 Principio de Confidencialidad:

- ✓ **Principio de Acceso al equipo de Cómputo:** todos los empleados del Hospital San Bartolomé de Capitanejo deben ser registrados en el sistema con un usuario y una contraseña única para el acceso y manejo de la estación trabajo.
- ✓ **Principio de Contraseña de Usuario Registrado en el Dominio:** La contraseña debe cumplir con ciertas condiciones como mínimo 8 caracteres con símbolos, letras en mayúscula y minúsculas.
- ✓ **Principio de manejo de la Contraseña:** se debe establecer una política de cambio de contraseña, en donde cada mes se debe realizar.
- ✓ **Principio de manejo de la información en un equipo de Cómputo:** La información se guardara en la carpeta que viene por defecto por el sistema operativo Windows y será guardada en orden cronológico; todos esto para evitar que si otro usuario ingresa al computador con un usuario de invitado no pueda ver la información personal de la persona que tiene a cargo la estación de trabajo.

8.1.2 Principio de Integridad:

- ✓ **Principio de Salvaguardar la información**: para salvaguardar la información se programara un Backup del sistema de información, quemándola en un dvd diariamente a las 2:00 de la mañana; esta copia será almacenada por el jefe del área de las Tic del hospital.
- ✓ **Principio de Integridad de la información**: para realizar la modificación de la información, el usuario deberá solicitar por escrito ante el departamento de sistemas y este a su vez realizara la modificación y se levantara un acta dejado manifiesto de la modificación hecha.
- ✓ **Principio de Salvaguardar la Información de los Equipos de Cómputo:** cada usuario que tenga asignado una estación de trabajo deberá realizar un backup de la información en medio físico cada vez que el área de sistemas lo requiera.

- ✓ **Principio de manejo de la Información de los Equipos de Cómputo:** en el momento en que un empleado finalice su contrato, estará obligado a informar por escrito sobre la información que esta almacenada en el equipo al jefe de sistemas y entregara una copia de la misma en medio físico.

8.1.2 Principio de disponibilidad y confiabilidad de la información.

- ✓ **Principio de Escaneo de la Información en los Equipos de Cómputo**: Se deberá implementar un sistema de detección de virus en las estaciones de trabajo de todo el hospital, con el fin de salvaguardar la integridad y garantizar su disponibilidad y confiabilidad en todo momento.
- ✓ **Principio de Creación de Perfiles**: se deberán crear perfiles y cada uno tendrá derechos especiales para el manejo del sistema de información, dependiendo del cargo y las funciones que desempeña cada empleado en el hospital.

8.2 Organización de la Seguridad de la Información.

Para realizar una adecuada organización de la información es necesario tener claridad y una buena planificación sobre el marco de gestión, con lo cual se realizaran las diferentes tareas, dentro de las cuales tenemos la aprobación de la política, su implementación, asignación de funciones y responsabilidades con el personal. Todo esto con el fin de lograr una eficiente administración de la seguridad de la información.

Adicionalmente a lo anterior el Hospital debe tener en cuenta que algunas actividades requieren la interacción de terceras personas con la información que allí se maneja; es por esta razón que la información puede ponerse en riesgo si este acceso se produce dentro de un inadecuado acceso de la misma; es por esta razón que se deben establecer las siguientes medidas de protección:

Inicialmente debemos establecer un comité de seguridad que tendrá unas funciones específicas en la administración de la seguridad de la información, como:

- ✓ Inspeccionar y realizar la socialización con los directivos del E.S.E Hospital San Bartolomé de Capitanejo de la política de seguridad de la información, en busca de su aprobación
- ✓ Realizar monitoreos constantes a los cambios que puedan presentar los riesgos de la información frente a las amenazas que los acechan.
- ✓ Coordinar la investigación y monitoreo de los posibles incidentes relacionados a la seguridad de la información.
- ✓ Recibir, analizar y aprobar las propuestas que mejoren o incrementen la seguridad de la información, teniendo en cuenta las competencias y responsabilidades de cada área.
- ✓ Verificar y coordinar la implementación de los controles establecidos en la política de seguridad en los nuevos procesos, sistemas o servicios.
- ✓ Coordinar y controlar la continuidad de operación del sistema de información del Hospital frente a imprevistos de seguridad

Al constituir el comité, se deben asignar las funciones a cada uno de los miembros, para que cada uno de ellos se desempeñe en sus actividades y mejorar la seguridad del sistema de información del Hospital.

Adicionalmente a esto el comité debe encargarse que en los contratos a terceros sean establecidos y ejecutados por cada persona que sea contratada; dentro de los puntos que se deben tener en cuenta son:

a) Cumplimiento a cabalidad de la política de seguridad de la información del Hospital
b) Mantener constantemente un la protección de los activos del hospital, así:
    - ✓ Ejecutar los procedimientos que permitan proteger los activos hardware y software de la institución.
    - ✓ Establecer procedimientos que permitan establecer si se ha presentado algún incidente que comprometa la integridad de la información.
    - ✓ Establecer medidas de protección que permita realizar la recuperación de la información y evitar la destrucción de la misma, en el momento en que se dé por finalizada la vigencia del contrato
    - ✓ Establecer parámetros de restricción en la copia y divulgación de la información
c) Monitoreo sobre el nivel de servicio esperado como servicio esperado.
d) Mantener claridad sobre las obligaciones del acuerdo y responsabilidades legales.
e) Tener claras las definiciones que respectan a la protección de datos
f) Mantener acuerdos de control de acceso que contemplen:
    - ✓ Establecer métodos de acceso, control e identificadores de usuarios en el sistema de información.
    - ✓ Establecer privilegios de los usuarios de acuerdo a la función desempeñada
    - ✓ Mantener actualizada la lista de empleados autorizados para acceder al sistema de información.
g) Establecimiento de controles comprobables sobre los niveles de desempeño
h) Establecimientos de protocolos para la resolución de problemas y planes de contingencia
i) Asignar responsabilidades al momento de la instalación y mantenimiento tanto de hardware como de software.
j) Mantener procesos claros y detallados que permitan la administración de cambios en el sistema de información
k) Establecer controles de protección física y mecanismos que aseguren la implementación de los mismos.
l) Establecer metodologías que permitan el entrenamiento de usuarios y administradores en el área de seguridad de la información.
m) Establecer controles que protejan al sistema contra software malicioso.
n) Realizar informes periódicos donde se notifiquen los avances de las investigaciones de los incidentes relativos a la seguridad del sistema de información

8.3 Gestión de los Activos de la Red.

Es función del departamento de la Tic, garantizar la seguridad del sistema de información y de los activos que lo constituyen, para ello deben tener en cuenta los activos de red y para ello se deben establecer los siguientes principios de seguridad:

a) **Principio de Seguridad de la Información en la red**: el departamento de las tic del hospital deberá implementar un servidor firewall para lograr realizar una plena

administración del servicio de internet y de datos que fluyen a través de la red; este servidor debe prestar servicios de protección de acceso no autorizado, servicio de proxy, eliminación de spam y encriptación de correos electrónicos; todo esto con el fin de garantizar el buen funcionamiento de la red y del servicio de internet.

b) **Creación de los Perfiles en el Servidor Firewall:** para realizar una optima administración de los servicios prestados por la red, se hace necesario la creación de perfiles, los cuales tendrán derechos dentro del sistema de información; teniendo en cuenta esto se crearían los siguientes perfiles:
    - ✓ **Perfil Administrativo:** como su nombre lo indica este perfil se creara para el personal administrativo del hospital y estará encabezado por los líderes de cada departamento.
    - ✓ **Perfil Medico:** este perfil será creado para todos los usuarios que forman parte del departamento asistencial médico del hospital.
    - ✓ **Perfil de Usuarios Generales:** este perfil se creara especialmente para usuarios que únicamente tendrán acceso a la parte básica del sistema, como por ejemplo acciones de consulta.
    - ✓ **Perfil de sistemas:** en este perfil estará todo el personal del área de sistemas, los cuales según el rol que desempeñen dentro del área de las tic cumplirán la función de administradores.

Adicionalmente debemos tener en cuenta que cualquier equipo informático que se conecte a la red del Hospital, debe estar sujeto a las normas y políticas establecidos por la institución, con el fin de preservar y mantener la integridad del sistema.

8.4 Seguridad Física y del Entorno.

Dentro de las medidas que hay que tener en cuanto a la seguridad física y del entorno debemos minimizar los riesgos que puedan afectar el sistema de información del Hospital San Bartolomé de Capitanejo; dentro de los parámetros a controlar tenemos los accesos físicos no autorizados mediante el establecimiento de perímetros de seguridad. Además se deben implementar dispositivos que permitan controlar algunos factores ambientales que permitan garantizar el correcto funcionamiento de los equipos de cómputo, minimizando las interrupciones del servicio.

Para proteger los equipos de condiciones adversas deben ser ubicados en áreas protegidas y resguardadas por un perímetro de seguridad definido, con controles de acceso apropiados; asi mismo se deben tener en cuenta medidas de protección fuera del perímetro que se encuentra resguardado.

Frente a los factores ambientales estos deben controlarse a través de dispositivos electrónicos, ya que estos podrían perjudicar el correcto funcionamiento de los equipos que contienen la información del hospital.

8.5 Control de Acceso.

En el hospital se hace necesario el establecimiento de controles de acceso que impidan el acceso no autorizado a personas ajenas o que no tienen los permisos necesarios para acceder al sistema; por tal motivo se hace necesario la implementación de dispositivos y

procedimientos que permitan controlar este tipo de accesos no autorizados al sistema del Hospital San Bartolome de Capitanejo.

Dentro de la implementación de la política de seguridad debemos tener en cuenta que debe aplicarse a todos los usuarios, tanto internos como externos al hospital; ya que estos poseen diferentes permisos dentro del sistema pero debe existir un control.

Dentro de los parámetros que se recomiendan establecer tenemos:

- Configurar el sistema para que el automáticamente pueda denegar el acceso al mismo, a cuentas anónimas o usuarios no identificados
- Realizar un monitoreo a aquellas cuentas que poseen privilegios especiales.
- Después de que el usuario haya intentado cierto número de veces de acceder al sistema de manera fallida, configurarlo para que este se bloquee o suspenda para evitar intromisiones en el mismo.
- Mantener actualizada la lista de cuentas de usuarios para evitar que personas que ya no pertenecen a la compañía puedan ingresar al sistema.
- Realizar una suspensión de servicios después de 30 minutos de inactividad.
- Realizar una deshabilitación de las configuraciones por defecto de servicios o puertos no utilizados.
- Cada periodo de tiempo forzar a los usuarios del sistema que realicen el cambio de contraseña y estas deben tener ciertas características de seguridad como cierto número de caracteres, mezclar numero con caracteres y letras mayúsculas con minúsculas.
- Realizar periódicamente auditorías a los usuarios y sus labores con el sistema de información

8.5.1 Identificación y Autenticación de los usuarios

En el caso de identificación y autenticación de usuarios, se debe tener en cuenta que todos sin excepción tienen que tener una identificación única, de uso personal y exclusivo. De manera que cualquier movimiento o actividad no autorizada en el sistema pueda ser monitoreado y rastreada para identificar al responsable.

8.5.2 Restricción del acceso a la información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación acorde al procedimiento de asignación de privilegios. Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación, para lo cual el administrador de la red debe manejar los privilegios de acuerdo al perfil del usuario y con los requerimientos realizados formalmente por el responsable de cada área.

b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
c) Controlar los derechos de acceso de los usuarios.
d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.
e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.
f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento.

8.5.3 Protección de los puertos de diagnóstico remoto

El departamento de las Tic tiene el privilegio de que los computadores o sistemas de comunicación pueden se accedidos remotamente para realizar tanto diagnósticos, como instalaciones de software. Es por esta razón que debe existir una medida de protección que permita el control de accesos no autorizados.

Inicialmente se debe realizar un escaneo de los puertos para verificar cuáles de ellos se encuentran abiertos y si los hay tomar las medidas respectivas, para controlar el acceso.

8.6. Revisión técnica de los cambios en el sistema operativo

Cada vez que se requiera realizar un cambio o mantenimiento de un sistema operativo, estos deben ser monitoreados para que no se llegue a producir ningún impacto en su funcionamiento o seguridad.

Para ello, el administrador del sistema debe tener un manual de procedimiento en el cual se incluye:

a) Realizar un monitoreo a los sistemas para verificar la integridad y funcionamiento de las mismas para garantizar que funcionen correctamente.

b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación. Para lo cual el administrador debe planificar el día en el cual se llevará a cabo el cambio e informarlo a los usuarios y coordinar con los responsables de cada área en caso de que ellos deban realizar algún trabajo por el cual no pueden suspender sus actividades. Estos cambios deben programarse para fines de semana donde no haya impacto en los usuarios.

8.7 Gestión de Incidentes de Seguridad de la Información.

8.7.1 Divulgación de eventos y de debilidades de la seguridad de la información.

Es de suma importancia que el hospital y en especial el departamento de sistemas tenga un manual de procedimientos donde se indique cuáles son los pasos a seguir cuando se presente algún incidente de seguridad en el sistema de información e ir documentando

todos lo que se presente ante una eventualidad como esta para que se pueda retroalimentar y mejorar los sistemas o medidas de seguridad que están actualmente implementadas

El Hospital debe tener en cuenta que se debe realizar un uso apropiado de los recursos que ofrece la red, dejando claro que deben usarse de manera ética y responsable. Este uso se puede categorizar como aceptable, tolerable, o prohibió:• El uso aceptable de recursos de tecnología de información es el uso legal consistente con los requerimientos de la organización, en base a las políticas de la misma que permitan solventar los problemas de la Institución.

- El uso tolerable es el uso legal para otros propósitos que no chocan con en la política del uso aceptable de la organización.
- El uso prohibido es el uso ilegal y todo el otro uso que son aceptables " ni tolerables.

8.7.2 Administración de incidentes y mejoras de la seguridad de la información

A continuación de que el incidente se haya resuelto, se debe documentar y dejar plasmadas las experiencias aprendidas del evento. Adicionalmente se debe realizar un análisis de ese reporte y generar alarmas o advertencias sobre qué acciones se deben tomar para minimizar las vulnerabilidades que se explotaron durante el incidente.

Entre estas alertas es importante que se especifique de forma clara:
- Asegurar que sólo personal autorizado tiene el acceso a los archivos electrónicos.
- Reducir el riesgo de que cualquier usuario no autorizado pueda modificar archivos o copiar información sensible en dispositivos extraíbles.
- capacitar al personal del hospital para que aprendan a proteger la información contra la perdida de la misma
- Proveer del respaldo y recuperación de archivos para proteger contra la pérdida de información.
- Mantener un respaldo de los archivos de información que permitan proteger el sistema contra la pérdida de información.

8.8 Gestión de Continuidad del Negocio.

Para sobrevivir, la organización debe asegurar el funcionamiento de aplicaciones críticas en un tiempo razonable, frente a un desastre. Las organizaciones necesitan entrenar a sus empleados para ejecutar los planes de contingencia, para lo cual se requiere:
- Que los empleados sean conscientes de la necesidad del plan de contingencia
- Informar a todos los empleados de la existencia del plan y proporcionar los procedimientos para seguir en caso de una emergencia
- Entrenar al personal con las responsabilidades identificadas para cada uno de ellos, para realizar la recuperación del desastre y procedimientos de continuidad de negocio

- Dar la oportunidad para que se pueda llevar a cabo el plan de contingencia, para poder realizar un simulacro de la forma en la que se ejecuta el mismo.

8.8.1 Desarrollo e implantación de planes de contingencia

Para el plan de contingencia se debe tener claro cuáles son las responsabilidades y funciones que debe desarrollar cada persona dentro de un proceso determinado; para se deben crear los siguientes comités o departamentos que serán los responsables de:

- Personal encargado de la administración de la recuperación.- El cual debe actuar en el momento en el cual se presente el desastre, y cuyo trabajo consiste en ejecutar el plan de recuperación de desastre y restaurar los procesos críticos en el menor tiempo, para este caso es el Comité de Seguridad.
- Personal operacional. Son aquellos que están encargados de la operación del negocio hasta que las cosas vuelvan a la normalidad, estas personas tienen responsabilidades cotidianas y desarrollan las mismas funciones bajo circunstancias normales.
- Personal de las comunicaciones. Personal que diseña los medios de comunicar la información a los empleados, a los clientes, y al público en general. Son los encargados de considerar qué información puede darse y por quién. Esto es crítico en los primeros días de una interrupción pues habrá una mayor demanda para la información, y ocurre en un momento en que los canales normales son interrumpidos por daños en los mismos.

Una vez que se encuentra definido el personal necesario para los diferentes procesos del plan, es necesario que se realicen pruebas del mismo. Pues un plan que no ha sido probado puede presentar fallas en el momento de su ejecución. Las pruebas no deben ser costosas ni interrumpir la operación diaria del negocio. Entre las pruebas que se pueden considerar son:

- **Prueba de papel**. Esto puede ser tan simple como discutir el plan en una reunión del personal considerando sucesos actuales. Es importante documentar la discusión y utilizar cualquier lección aprendida como parte del proceso para mejorar el plan.
- **Camino Estructurado.** Aquí es donde el personal define diversos panoramas para supervisar el plan en equipo.
- **Prueba de componentes.** En esta prueba, cada parte del plan total se puede probar independientemente. Los resultados entonces se miran para considerar cómo el plan total pudo haber trabajado si todos los componentes fueron probados simultáneamente.
- **Simulación.** No incluye realmente la mudanza a una localización alterna sino puede incluir la simulación de interrupciones para uso general como manera de ver que tan completo es un plan.
- **Ejercicio de la recuperación del desastre.** En esta prueba, se activa el plan y los sistemas informáticos se cambian a sus sistemas de reserva, que pueden incluir el funcionamiento en los sitios alternativos. Esto a veces se llama una prueba "paralela" pues los sistemas de producción seguirán siendo funcionales mientras que los sistemas de la recuperación se ponen en producción para probar su funcionalidad.

9. CONCLUSIONES

Con el desarrollo de la primera fase de la monografía se ha logrado establecer los activos de información que existen en el E.S.E. Hospital San Bartolomé el cual cuenta con una amplia y diversa cantidad de tecnologías pasadas y modernas que se encuentran expuestas a riesgos y vulnerabilidades que pueden afectar la integralidad de los sistemas de información y el negocio de la empresa.

Con la aplicación de la metodología Magerit a través del software Pilar, se logra determinar cuáles son los procesos críticos que maneja el E.S.E Hospital San Bartolomé de Capitanejo y así iniciar a determinar cuáles son las medidas que se deben tener en cuenta para mejorar y garantizar la seguridad, confidencialidad, integridad y disponibilidad de los procesos e información que se manejan en la institución.

Al realizar la implementación de las medidas o políticas propuestas en este documento se lograra que el E.S.E Hospital San Bartolomé pueda tener un mayor control sobre todos y cada uno de los activos del sistema de información que existe dentro de la institución.

Para nadie es un secreto que la información es el principal activo de toda empresa, por esta razón hay que tener medidas efectivas para el almacenamiento y manipulación de la misma. Que permitan dar un soporte efectivo al sistema de información al momento de presentarse algún hecho desafortunado.

Con el desarrollo y culminación del proyecto se logró determinar que se cumplieron a cabalidad todos los objetivos propuestos, dando como resultado una propuesta enfocada a minimizar las vulnerabilidades encontradas durante el desarrollo del mismo, planteando las bases para el mejoramiento de la seguridad del sistema de información del E.S.E Hospital San Bartolomé de Capitanejo.

10. RECOMENDACIONES

Se recomienda que la parte directiva tenga en cuenta todas y cada una de las sugerencias dadas en este documento por los integrantes del proyecto, para el mejoramiento de la seguridad de los procesos.

Se debe dar continuidad al proyecto con el objetivo de minimizar cualquier nuevo riesgo que se presente en la confidencialidad, integridad y disponibilidad del sistema de información.

Se recomienda que se realice una constante evaluación de las políticas de seguridad, para que se mantengan actualizadas y ajustadas a las necesidades de la seguridad del sistema de información, mediante la realización de auditorías internas cada semestre o en caso extraordinario cuando este lo amerite.

Se debe realizar una monitorización constante sobre el personal en cuanto a la aplicación ejecución y control de las políticas, sujetándose al cumplimiento de las mismas, para garantizar que se apliquen las recomendaciones diseñadas en el documento.

11. BIBLIOGRAFIA

[1] Markus Erb. Gestión de Riesgo en la Seguridad Informática [en línea]. https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

[2] Markus Erb. Gestión de Riesgo en la Seguridad Informática [en línea]. https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

[3] MARTINEZ GARCIS Robinson. PILAR Análisis y Gestión de Riesgos [en línea]. https://docs.google.com/document/d/15TYUClkxF_WYA1kTqCJa6bwQaCLlaEkwAQ-8EvFO7js/edit?pli=1

[4] EAR / PILAR Entorno de análisis de riesgos [en línea]. http://www.ar-tools.com/es/index.html

[5] MARTINEZ GARCIS Robinson. PILAR Análisis y Gestión de Riesgos [en línea]. https://docs.google.com/document/d/15TYUClkxF_WYA1kTqCJa6bwQaCLlaEkwAQ-8EvFO7js/edit?pli=1

[6] Seguridad Informática [en línea]. https://seguridadinformaticaufps.wikispaces.com/PILAR+-+Herramienta+para+An%C3%A1lisis+y+Gesti%C3%B3n+de+Riesgos

[7] Saiz Esteban. Backtrack una distribución Linux para expertos en seguridad. [en línea]. http://www.genbeta.com/mobile.php/sistemas-operativos/backtrack-4-una-distribucion-linux-para-expertos-en-seguridad

[8] SOLARTE SOLARTE Francisco Nicolás Javier. Riesgos y Control Informático [en línea]. http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_21_generalidades_del_estndar_cobit.html

12. ANEXOS

Anexo 1. Carta aval de la Gerente del Hospital

E. S. E. Hospital San Bartolomé
Nit: 800.194.328-4

Protegemos el don más valioso de la vida, su salud.

Capitanejo, Mayo 6 de 2015

Señores:
JOSÉ LEONARDO CORDERO MORENO
YADIMIR GARCÍA REYES
Malaga - Santander

Respetados Señores:

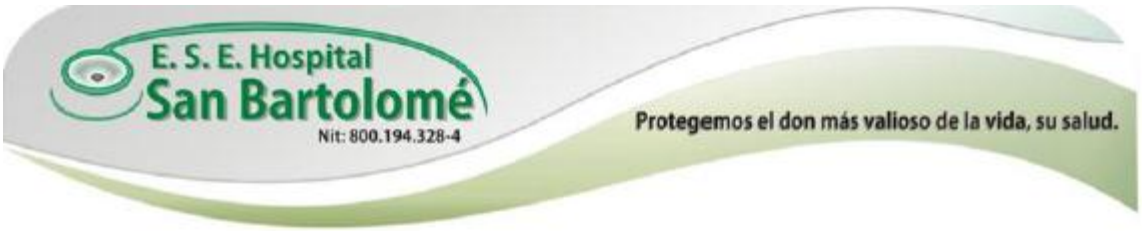
SONIA CASTELLANOS CASTRO, en mi condición de Representante legal de la E.S.E. SAN BARTOLOMÉ DE CAPITANEJO SANTANDER, por medio del presente escrito me permito notificarles que de acuerdo a la solicitud por ustedes realizada para desarrollar su trabajo de grado titulado: ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN DEL HOSPITAL E.S.E. SAN BARTOLOMÉ DE CAPITANEJO, SANTANDER, para optar al título de Especialistas en Seguridad informática ha sido APROBADA por esta gerencia para que a partir de la fecha la desarrollen en nuestra institución hospitalaria.

Cordialmente,

Sonia Castellanos Castro
SONIA CASTELLANOS CASTRO
Gerente Hospital E.S.E San Bartolomé

Carrera 4 No 1-05 Capitanejo Santander
Email: hospitalbartolome@hotmail.com. Tel: 6600446 Celular 3118081792
www.hospitalsanbartolome-santander.gov.co

Anexo 2. Carta aval del Jefe de Sistemas del Hospital



Málaga, mayo 6 de 2015

Señores:
José Leonardo Cordero Moreno
Yadimir García Reyes
L.C

Por medio de la presente yo, Benjamín Suarez Rodríguez, actuando como encargado del departamento de Sistemas y TIC´S de la E.S.E. Hospital San Bartolomé de Capitanejo, Santander. Les notifico que de acuerdo a la solicitud hecha por ustedes para desarrollar su trabajo de grado titulado: ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN DE LA E.S.E. HOSPITAL SAN BARTOLOMÉ DE CAPITANEJO, SANTANDER. Para optar al título de Especialistas en Seguridad informática. Ha sido aprobada para que la desarrollen en nuestras instalaciones.

Cordialmente,

Ing. **BENJAMÍN SUAREZ RODRÍGUEZ**
Dpto de Sistemas y TIC´S
E.S.E Hospital San Bartolomé
Cel: 3142984596
Capitanejo - Santander