ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN AL AREA DE INFORMACIÓN Y TECNOLOGÍA DEL HOSPITAL SUSANA LÓPEZ DE VALENCIA DE LA CIUDAD DE POPAYÁN

HENRY EDUARDO BASTIDAS PARUMA
IVAN ARTURO LÓPEZ ORTIZ
HERNANDO JOSÉ PEÑA HIDALGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
POPAYÁN
2014

ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN AL AREA DE INFORMACIÓN Y TECNOLOGÍA DEL HOSPITAL SUSANA LÓPEZ DE VALENCIA DE LA CIUDAD DE POPAYÁN

HENRY EDUARDO BASTIDAS PARUMA
IVÁN ARTURO LOPEZ ORTIZ
HERNANDO JOSÉ PEÑA HIDALGO

Línea de Investigación: Infraestructura tecnológica y Seguridad en Redes, de acuerdo a la propuestas por la escuela (1)

Director
FRANCISCO SOLARTE SOLARTE
Ingeniero de Sistemas, Mg. Docencia Universitaria

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERIA
POPAYÁN
2014

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Popayán, octubre de 2014

DEDICATORIA

Dedicamos en primer lugar nuestro trabajo a Dios fue el creador de todas las cosas, el que ha dado la fortaleza para continuar.

De igual forma, a nuestros padres, a quienes les debemos toda nuestra vida, agradecemos su cariño y su comprensión a ustedes quienes han sabido formarnos con buenos sentimientos, hábitos y valores, lo cual han ayudado a salir adelante buscando siempre el mejor camino.

AGRADECIMIENTOS

Agradecemos primero y antes que nada a Dios, por estar con nosotros en cada paso que damos, por fortalecer nuestros corazones e iluminar nuestra mente y por haber puesto en nuestro camino a aquellas personas que de una u otra manera apoyaron y contribuyeron al desarrollo de este trabajo.

Agradecer hoy y siempre a nuestras familias por el esfuerzo realizado por ellos, por la comprensión y paciencia, por su apoyo incondicional.

A nuestros padres, esposas, familiares e hijos ya que brindan el apoyo, la alegría y la fortaleza necesaria para seguir adelante.

Un agradecimiento especial a los Ingenieros Robert Camacho y Cristian Diego González del área de Informática del Hospital Susana López de Valencia E.S.E Popayán por toda su disposición y apoyo incondicional ya que sin su decidida colaboración no hubiera sido posible el desarrollo del presente trabajo, a nuestros tutores y director del proyecto por su colaboración y resolver nuestras dudas y sus valiosos aportes.

Ing. Henry Eduardo Bastidas Paruma
Ing. Iván Arturo López Ortiz
Ing. Hernando José Peña Hidalgo

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

INTRODUCCION

En la actualidad se puede considerar a La Información como un activo más de una organización, tan importante como los activos comerciales o físicos, llegando a convertirse en algunos casos como el pilar fundamental para el buen funcionamiento de la misma organización, por tal caso esta debe ser protegida adecuadamente, al estar expuesto a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

Por otro lado la información puede ser almacenada en equipos de cómputo u servidores en forma de documentos de texto, hojas de cálculo, bases de datos y/o de forma impresa, por lo tanto es necesario implementar un sistema de gestión de seguridad de la información que garantice dada una eventualidad, (llámese ataque informático, pérdida de información o desastre natural) le permita a la organización de forma rápida volver a un normal funcionamiento.

Para satisfacer dichas necesidades de Seguridad de la Información se debe implementar un adecuado conjunto de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Donde el tipo de seguridad que necesita la red debe relacionar los requisitos de seguridad básicos (como confidencialidad, integridad, disponibilidad, etc.) a la visión de negocios de la empresa, siempre teniendo en cuenta los factores de impacto crítico frente a un ataque o pérdida de información (tales como pérdida financiera, pérdida de productividad, daño en la reputación, responsabilidad legal, etc.). Así mismo se necesitan establecer, implementar, monitorear, revisar y mejorar dichos controles cuando sea necesario para aseguras que cumplan con los objetivos de seguridad específicos.

Con este propósito el documento presenta el análisis de los riesgos lo mismo que las recomendaciones presentadas al área de información y tecnología del hospital Susana López de Valencia en la ciudad de Popayán. Todo esto bajo la utilización de la metodología Magerit y enmarcado en la norma ISO 27001.

1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, todas las instituciones en el departamento del Cauca y en el país tienden a apoyarse 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 reforzar la seguridad de sus 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 tiempo de ejecución de proyectos.

Según lo anterior, con el paso del tiempo la información se ha convertido en el activo más importante de estas instituciones, y por lo tanto se debe aplicar controles de seguridad física y lógica que permita salvaguardar dicha información de eventos que la puedan afectarla, permitiendo así disponer de la misma a las personas o usuarios que la requieran.

La falta de implementación de algunos controles y procedimientos adecuados, puede llevar en determinado momento a una situación que afecte la información, dejando a la institución en una situación compleja de pérdida, robo o alteración de la misma.

Ahora, si bien es cierto que en la actualidad el hospital Susana López de Valencia, cuenta con una área encargada del control informático y que muchos de los procesos que ahí se llevan a cabo están debidamente documentados, también es cierto que existen muchas vulnerabilidades que precisan ser analizadas, revisadas

y documentadas con el propósito de implantar mecanismos de control que permitan detectar riesgos inminentes frente a las anomalías presentes y futuras.

De acuerdo a esto es importante buscar mediante el uso de controles, estándares, herramientas y recomendaciones vigentes, un diagnóstico de seguridad de la información en la División de Tecnologías de la Información y las Comunicaciones del Hospital Susana López de Valencia de la ciudad de Popayán con el fin de establecer políticas y procedimientos en relación a los objetivos de la institución, en busca de minimizar los riesgos en la alteración de la información.

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo el proceso de análisis y evaluación de riesgos de seguridad de la información en la oficina de gestión de sistemas de información y telecomunicaciones permitirá mejorar los niveles de seguridad de la información en el Hospital Susana López de Valencia E.S.E de la ciudad de Popayán?

2. JUSTIFICACION

El Hospital Susana López de Valencia en el último quinquenio ha presentado un cambio significativo que ha contribuido a la obtención de metas y objetivos planteados. En estos años se ha logrado el fortalecimiento del sistema de información 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.

Unido a lo anterior se ha trabajado en el fortalecimiento de la plataforma tecnológica mediante la adquisición gradual de servidores de red, equipos de cómputo, equipos activos y de soporte eléctrico

La implantación de estas nuevas tecnologías ha tenido importantes repercusiones en los costos de operación además de presentar nuevas exigencias para el personal en cuanto a los tiempos de capacitación y formas de trabajar. De esta manera el Hospital está respondiendo a la renovación tecnológica permitiendo posicionarlo en su entorno competitivo tanto en términos de calidad como de estabilidad financiera.

El hospital Susana López de Valencia y en especial el área de informática (información y tecnología), consciente de la importancia del cuidado que debe tener para salvaguardar la información que por su dependencia hace tránsito, está en el propósito de establecer los procesos y mecanismos necesarios que permitan garantizar la seguridad de los sistemas de información soportados por esta oficina. En este momento se están trabajando dos aspectos importantes, el primero relacionado con los sistemas de información y el segundo relacionado con la

renovación tecnológica y de telecomunicaciones, que se constituyen en los aspectos fundamentales que atiende la oficina de informática.

Con este proyecto se busca realizar un estudio de las vulnerabilidades que pueda afectar la seguridad de la información que maneja el hospital en los diferentes servicios, lo cual permitirá identificar las principales falencias resultantes de este estudio como producto del análisis de los recursos tecnológicos que intervienen en los procesos desarrollados dentro de la institución y recomendar 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.

A partir de un análisis de vulnerabilidades y mediante el uso de herramientas y técnicas propias de análisis de evaluación de riesgos, se busca identificar los riesgos para evitar a futuro pérdidas sensibles o de vital importancia de la misma.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar mejoras a los niveles de seguridad informática mediante la aplicación del proceso de análisis y evaluación de riesgos de seguridad de la información en la oficina de gestión de sistemas de información y telecomunicaciones del Hospital Susana López de Valencia E.S.E de la ciudad de Popayán.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar el estudio de vulnerabilidades y amenazas a la infraestructura tecnológica en la oficina de gestión de sistemas de información y telecomunicaciones del Hospital Susana López de Valencia E.S.E

- Realizar un diagnóstico de las vulnerabilidades y amenazas encontradas en la oficina de gestión de sistemas de información y telecomunicaciones del Hospital Susana López de Valencia E.S.E.

- Proponer mecanismos de control y gestión de información que minimicen las vulnerabilidades detectadas en la oficina de gestión de sistemas de información y telecomunicaciones del Hospital Susana López de Valencia E.S.E.

.

- Proponer mejoras a las prácticas de manejo de los recursos tecnológicos de manera que permita concientizar al personal de tecnología y en general a todo el personal de la organización sobre la necesidad de contar con mecanismos que apoyen el aseguramiento la información.

4. MARCO DE REFERENCIA

4.1 ANTECEDENTES DE INVESTIGACIÓN

El proyecto propuesto se desarrolla al interior de una entidad de salud pública de la ciudad de Popayán y en este sentido se hacen necesario realizar una revisión documental referente al sector que ocupa el presente informe al interior del país, sobretodo que se ha adelantado en relación a la seguridad de la información por lo cual es importante mencionar que desde el mismo ministerio de salud y de la protección social se han venido adelantando proyectos tendientes a proteger la información sensible que se genera dentro de las entidades e instituciones de salud en el país, es así como mediante la resolución número 10000509 del 25 de febrero del 2013 se crea dentro del ministerio el Comité de Seguridad de la Información del Ministerio de Salud y de la Protección Social.

Dentro de la resolución en su artículo 1 de Creación y Objeto resuelve “Crear el Comité de Seguridad de la Información (CSI) del ministerio de salud y de la protección social, como órgano operativo y de apoyo para coordinar la formulación y la implementación del Sistema de Gestión de Seguridad, en el marco de la estrategia de Gobierno en Línea y anti trámites, tanto al interior como del sector social y salud”.

Es importante mencionar que la entidad objeto del estudio es de carácter público por lo cual la rige y cubre esta resolución puesto que el Hospital Susana López de Valencia E.S.E Popayán, se encuentra reglamentado y registrado en el ministerio de Salud y de la Protección Social.

[1] Resolución número 10000509 del 25 de febrero del 2013. Ministerio de Salud y de la Protección Social

Dentro del presente proyecto de igual manera se revisa estudios adelantados como el desarrollado por la universidad Pontificia Bolivariana Seccional Bucaramanga, en cual se desarrolló una investigación denominada (3)., el desarrollo de la tecnología y la implementación de la misma en las diferentes áreas, ha permitido un mayor avance en campos como la ciencia y la medicina; sin embargo, así como el avance genera desarrollo y este a su vez innovación, también aparecen nuevas brechas en el ámbito de seguridad que antes no se habían percibido. Siempre se ha procurado buscar la confidencialidad de cierto tipo de datos, su cuidado y sobre todo la integridad de los mismos, por lo cual a este ritmo de crecimiento acelerado de la tecnología es imposible no incluir los datos médicos de los pacientes en este nuevo avance. El objeto de esta investigación fue realizar un análisis profundo sobre las regulaciones actuales en Colombia con respecto al trato de los datos médicos contenidos en la historia clínica, y las regulaciones existentes en otros países, con el fin de presentar las recomendaciones necesarias para alcanzar la confidencialidad, integridad y disponibilidad de los datos de la historia clínica.

Dentro de esta investigación se concluyó:

> En Colombia se estableció el uso de la Historia Clínica Electrónica y aunque esto representa un gran avance en cuanto a la implementación de las tecnologías de la información en todas las áreas, el estado colombiano no tuvo en cuenta la importancia ni la privacidad de los datos que se manejan en la HCE, por el contrario como se menciona en el artículo su legislación fue de una forma muy precaria, sin garantizar el cumplimiento de los derechos de todos los pacientes; razón por la cual es necesario establecer unas medidas mínimas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la HCE, un marco legal que obligue a las instituciones prestadoras de salud a alinear sus sistemas de información para garantizar la seguridad adecuada a los datos que manejan, así como también una estandarización de todos los sistemas de información con el único fin de promover el desarrollo tecnológico, la interoperabilidad de los sistemas y el intercambio de información con otros países[2].

[2] Ley 1438 de 2011, que reformó el Sistema de Seguridad Social en Salud Colombiana.

4.2 MARCO CONTEXTUAL

(4), El 22 de Noviembre de 1947, el congreso de Colombia expidió la ley 27, por la cual se planifica y nacionaliza la lucha contra la tuberculosis, reglamentando diferentes aspectos y disponiendo mecanismos de control y tratamiento, así como obras de infraestructura discriminadas para cada departamento; en lo que respecta al Departamento del Cauca incluía la creación de tres hospitales sanatorios, uno en Popayán con capacidad para 300 camas, otro en Mercaderes o El Bordo con 120 camas y un tercero en Santander de Quilichao. A esta ley solo se le dio cumplimiento parcial 10 años después, cuando el 15 de marzo de 1957, se inició en Popayán la construcción del hospital antituberculoso.

El 30 diciembre de 1952 la alcaldía de Popayán, mediante el Decreto No. 97 destino un lote de terreno de 5.000 metros cuadrados, en la zona norte del predio "La Ladera" para construcción del hospital antituberculoso, el cual fue aprobado por la Gobernación del Cauca por el Decreto No. 7 del 5 de enero de 1953. En 1957 se concretó su ejecución, para lo cual el Departamento del Cauca en cabeza de la entonces gobernadora Josefina Valencia de Hubach, destino una partida inicial de $450.000 pesos.

Según el boletín informativo de la gobernación, los trabajos se iniciaron el 15 de marzo de 1957 y se ejecutaron hasta finales de 1958 cuando debieron suspenderse por falta de presupuesto, lo que causo graves problemas sociales, puesto que además de no contar los internos con la atención requerida, los que quedaban por fuera (más o menos el 50%) deambulaban libremente constituyéndose en foco de contagio para toda la comunidad. Los diferentes estamentos pidieron la culminación del Hospital como una sentida necesidad de la cuidad payanesa, fue así como el Hospital se construyó con pequeñas partidas presupuestales; recibiendo poco a poco los fondos para la terminación y dotación hasta que finalmente fue posible el traslado de los enfermos del lamentable

pabellón San Roque, al nuevo hospital de vías respiratorias inaugurado el 10 de diciembre de 1964.

Los primeros servicios fueron los de rayos X (certificados pulmonares) y consulta para tratamiento, tanto hospitalario como ambulatorio de enfermedades pulmonares.

Inicialmente se llamó Hospital de Vías Respiratorias y luego se le bautizó con el nombre de Susana López de Valencia, en memoria a la Primera Dama de la República por su apoyo a esta obra. La señora López de Valencia falleció el mismo año en que se fundó el Hospital.

El Hospital además del manejo integral de los pacientes tuberculosos, tuvo proyección comunitaria, realizaba visitas domiciliarias y apoyaba centros y puestos de salud con el fin de prevenir la enfermedad.

El terremoto de marzo de 1983, obligó al Hospital a adecuarse para apoyar la atención de la emergencia, a pesar que el 60% de su estructura sufrió daños.
En 1989 el Hospital se convierte en cabeza de la Unidad Regional Centro del Cauca, lo que significó que los hospitales y centros de salud de Morales, Silvia. Jámbalo, Totoró, Puracé, Sotará, Popayán, Santa Rosa (Bota Caucana), Timbío, Rosas, La Sierra, La Vega, Almaguer, Piendamo y Cajibio dependieran administrativamente del Hospital Susana. Con esta responsabilidad el Hospital pasó de ser especializado en el manejo de la tuberculosis, a ser Hospital General y por lo tanto de referencia de la regional Centro del Cauca.

Con la ley 100 de 1993, que creó el Sistema General de Seguridad Social en Salud, se definió que los hospitales públicos debían transformarse en Empresa Sociales del Estado E.S.E, por lo cual en enero de 1995 mediante ordenanza No. 001, se transformó al Hospital en Empresa Social del Estado, como

establecimiento público, descentralizado, de carácter departamental, con la función de prestar servicios de salud en el segundo nivel de atención en el Departamento del Cauca.

En enero de 1997 empieza su operación como Empresa Social del Estado, una vez se independiza de la Dirección Departamental de Salud del Cauca y de los Hospitales que hacen parte de la Unidad Regional Centro.

4.2.1 Plataforma Estratégica.

4.2.1.1 **Misión.** Prestamos la mejor atención de salud, en la diversidad y con responsabilidad social.

4.2.1.2 **Visión.** SUSANA será el primer Hospital Acreditado del departamento del Cauca y líder en la prestación de servicios de salud con énfasis materno infantil.

4.2.1.3 **Política de calidad.** El hospital Susana López de Valencia E.S.E. presta servicios de atención en salud, de manera efectiva, humanizada y con calidad; mediante personal calificado e infraestructura segura y tecnología adecuada; donde usuarios, servidores, entes de control, proveedores y comunidad contribuyen con su permanencia y mejoramiento continuo.

El hospital Susana López de Valencia E.S.E será el mejor centro de referencia para la atención en salud de mediana complejidad, con énfasis materno infantil, competitivo, humano, moderno y de calidad, que desarrollará servicios complementarios de acuerdo a las necesidades de la población, mediante esfuerzos institucionales y comunitarios basados en los principios del control social.

4.2.2 Políticas de dirección, gestión y funcionamiento del HSLV E.S.E.

4.2.2.1 **Atención en Salud.** Todos los servicios de salud del hospital preste a la población, estarán acordes con los lineamientos del sistema obligatorio de Garantía de Calidad de Atención en Salud – SOGCS además normas aplicables; se caracterizaran por alcanzar y mantener niveles superiores de calidad, garantizando la debida accesibilidad, oportunidad, seguridad, penitencia, continuidad y equidad; para lograr la adhesión y satisfacción de los usuarios.

4.2.2.2 **Desarrollo del Talento Humano.** La gestión del Talento Humano se realizará bajo las mejores condiciones para el ingreso, permanencia y retiro, de todos los trabajadores del Hospital; buscando un buen clima organizacional, servidores idóneos, capacitados y comprometidos con el desarrollo del Hospital.

4.2.2.3 **Estilo de Dirección.** La Gerencia del Hospital se caracterizara fundamentalmente por su capacidad orientadora y generadora de responsabilidad, participación y confianza, con la correspondiente atención de necesidades y expectativas de clientes y/o usuarios, un efectivo compromiso de control y autocontrol, mejoramiento continuo de procesos y resultados, calidad, seguridad, comunicación, trasparencia y responsabilidad social.

4.2.2.4 **Operación.** La marcha del hospital estará guiada por una gestión integral de sistemas y procesos, soportados en actividades y procedimientos debidamente concatenados, documentados y registrados con apoyo en guías y manuales para consulta y uso de todos los trabajadores en el desarrollo de sus tareas y funciones. Dicha gestión se organizará a su vez, bajo una estructura funcional acorde con los procesos definidos y orientados al logro de resultados, metas y objetivos del Hospital.

4.2.2.5 **Principios y Valores.** El comportamiento y actuaciones de todos los trabajadores del Hospital estarán guiados por los principios y valores definidos institucionalmente, de forma participativa y conforme al compromiso de responsabilidad social y conductas éticas.

4.2.2.6 **Austeridad y Eficiencia.** Toda contratación, compra o adquisición de bienes o servicios se realizará previo estudio de convivencia y necesidades del Hospital; se registraran de acuerdo a las normas aplicables y serán controlados en procura de su uso óptimo.

4.2.2.7 **Contables.** Todos los hechos y transacciones serán reconocidos, identificados, clasificados y registrados dentro del sistema integral de información contable y financiero del Hospital, se analizarán, interpretarán, revelarán y comunicarán de forma permanente y oportuna, bajo la normatividad aplicable; buscando garantizar las características y objetivos definidos para la información contable pública, con la correspondiente utilidad para los diferentes usuarios internos y externos.

4.2.2.8 **El CORE del Negocio.** El CORE del Negocio del Hospital Susana López de Valencia E.S.E, es la prestación de servicios de Salud.

Todos los servicios de salud que el Hospital preste a la población, estarán acordes con los lineamientos del Sistema Obligatorio de Garantía de Calidad de Atención en Salud- SOGCS y demás normas aplicables; se caracterizarán por alcanzar y mantener niveles superiores de calidad, garantizando la debida accesibilidad, oportunidad, seguridad, pertinencia, continuidad y equidad; para lograr la adhesión y satisfacción de los usuarios.

Los servicios que actualmente presta el Hospital se describen en el portafolio de servicios.

4.2.2.9 **Portafolio de servicios.** El Hospital Susana López de Valencia E.S.E. presta los siguientes servicios de salud que se muestran en las figuras 1 a .5.

4.2.2.10 Quirúrgicos.

Figura 1. Servicios Médicos Quirúrgicos

Fuente: Portafolio Digital Hospital Susana López

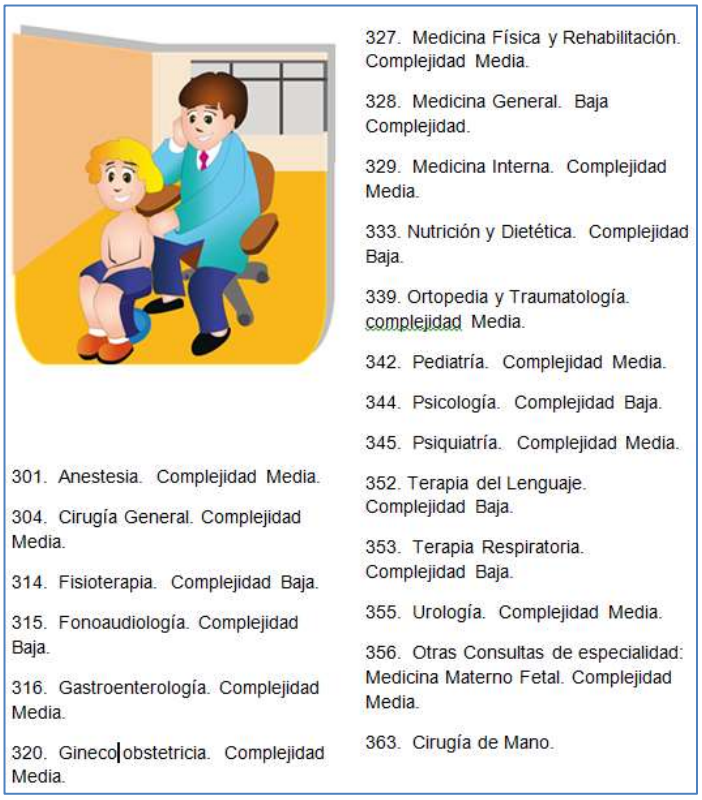
4.2.2.11 Apoyo, diagnóstico y complementación terapéutica.

Figura 2. Servicios de Apoyo, diagnóstico y complementación terapéutica

Fuente: Portafolio Digital Hospital Susana López

4.2.2.12 Ambulatorio

Figura 3. Servicios Ambulatorios



Fuente: Portafolio Digital Hospital Susana López

4.2.2.13 Urgencias

Figura 4. Servicio de Urgencias

Fuente: Portafolio Digital Hospital Susana López

4.2.2.14 Transporte especial de pacientes

Figura 5. Servicio de Transporte de Pacientes

Fuente: Portafolio Digital Hospital Susana López

4.3 MARCO TEÓRICO

4.3.1 Seguridad de la Información. (5), presenta la información, en todas sus formas (automatizada o no automatizada, formalizada o no formalizada, pública o reservada, etc.), como uno de los principales activos de cualquier organización, necesario para el normal funcionamiento y la consecución de los objetivo que se tengan marcados.

Debido a esa importancia, las organizaciones necesitan proteger su información para asegurar que esté disponible cuando se necesite, que sea fiable y que su distribución esté controlada. Esta necesidad se ve agravada por el hecho de que

la cantidad de información que maneja una organización y su complejidad crece de forma exponencial, dificultando los esfuerzos para su protección.

La seguridad de los sistemas de información es una disciplina en continua evolución. La meta final de la seguridad es permitir que una organización cumpla con todos sus objetivos de negocio o misión, implementando sistemas que tengan un especial cuidado y consideración hacia los riesgos relativos a las TIC de la organización, a sus socios comerciales, clientes, administración pública, suministradores, etc. Según (6), Los objetivos principales de la seguridad son los siguientes:

1. ***Disponibilidad y accesibilidad*** **de los sistemas y datos**, solo para su uso autorizado. Es un requisito necesario para garantizar que el sistema trabaje puntualmente, con prontitud y que no deniegue el servicio a ningún usuario autorizado. La disponibilidad protege al sistema contra determinados problemas como los intentos deliberados o accidentales de realizar un borrado no autorizado de datos, de causar cualquier tipo de denegación del servicio o de acceso a los datos y de los intentos de utilizar el sistema o los datos para propósitos no autorizados. La disponibilidad, frecuentemente, es uno de los objetos de seguridad más importante de toda organización.
2. ***Integridad****.* Se encarga de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados, evitando la perdida de consistencia. Presenta dos facetas:
    a. ***Integridad de datos****.* Es la propiedad de que los datos no hayan sido alterados de forma no autorizada, mientras se procesaban, se almacenaban o se transmitían.
    b. ***Integridad del sistema****.* Es la cualidad que posee un sistema cuando realiza la función deseada, de manera no deteriorada y libre de manipulación no autorizada. La integridad, normalmente, es el objetivo de seguridad más importante después de la disponibilidad.

3. ***Confidencialidad de datos y de la información del sistema***. Es el requisito que intenta que la información privada o secreta no se revele a individuos no autorizados. La protección de la confidencialidad se aplica a los datos almacenados durante su procesamiento, mientras se transmite y se encuentran en tránsito. Para muchas organizaciones la confidencialidad se encuentra frecuentemente, detrás de la disponibilidad y de la integridad, en términos de importancia. Para algunos sistemas y para tipos específicos de datos, como los autenticadores, la confidencialidad es de extrema importancia.
4. ***Responsabilidad* a nivel individual** (registro de auditoría). Es el requisito que permite que puedan trazarse las acciones de una entidad de forma única. A menudo, es un requisito de la política de la organización y soporta de forma directa el no repudio, la disuasión, el aislamiento de fallos, la detección y la prevención de intrusiones y, después, la acción de recuperación y las acciones legales pertinentes.
5. ***Confiabilidad (****aseguramiento).* Es la garantía en que los cuatro objetivos anteriores se han cumplido adecuadamente. Es la base de la confianza en que las medidas de seguridad, tanto técnicas, como operacionales, funcionan tal y como se idearon para proteger el sistema y la información que procesa.

En consecuencia se entiende por gestión de la seguridad de la información (7), el proceso por el cual la organización define, alcanza y mantiene unos niveles apropiados de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad para la información que necesita operar.

4.3.2 Familia de Normas ISO 27000. (8), La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.”

4.3.3 Origen. (7) Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

- 1979 Publicación BS 5750 - ahora ISO 9001
- 1992 Publicación BS 7750 - ahora ISO 14001
- 1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa - británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma BS 7799-1 es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte BS 7799-2, publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar

ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO

27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de la ISO27001: 2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

4.3.4 La serie 27000. A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- **ISO 27001:** (9) **Publicada** el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO

- **27002:2005: -**Nueva numeración de ISO 17799:2005 (10) desde el 1 de Julio de 2007- , para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. ISO 27002 Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.

- **ISO 27003:** Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y

en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- **ISO 27004:** Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

- **ISO 27005:** Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC.

- **ISO 27006:** Publicada el 13 de Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

- **ISO 27007:** Publicada en Mayo de 2010. Consiste en una guía de auditoría de un SGSI.

- **ISO 27011:** En fase de desarrollo; su fecha prevista de publicación es finales de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

- **ISO 27031:** Es una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

- **ISO 27032:** Consiste en una guía relativa a la ciberseguridad.

- **ISO 27033:** Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y remuneración de ISO 18028.

- **ISO 27034:** Consiste en una guía de seguridad en aplicaciones.

- **ISO 27799:** Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de

seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos y imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida.

4.3.5 Sistema de gestión de Seguridad de la Información SGSI. (10)La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso se puede constituir por el SGSI (Sistema de Gestión de la Seguridad de la Información), que podría considerarse, como una analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

El propósito del sistema de gestión de la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con el objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la

organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad (Véase Figura 4.6).

Figura 6. Ciclo SGSI

Fuente: http://sugestion.quned.es/archivos_publicos/conocimiento_fichas/46/2010-10-04--190804--3425_mini.png

- ***Plan (planificar):*** establecer el SGSI - es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados

- ***Do (hacer):*** implementar y utilizar el SGSI - es una fase que envuelve la implantación y operación de los controles.

- ***Check (verificar):*** monitorizar y revisar el SGSI - es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

- ***Act (actualizar):*** mantener y mejorar el SGSI - en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

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.

Análisis de Riesgos

Es una herramienta de diagnóstico que permite establecer la exposición real a los riesgos por parte de una organización. Este análisis tiene como objetivos la identificación de los riesgos (mediante la identificación de sus elementos), lograr establecer el riesgo total y posteriormente el riesgo residual luego de aplicadas las contramedidas en términos cuantitativos o cualitativos.

(11), El riesgo total es la combinación de los elementos que lo conforman, calculando el valor del impacto por la probabilidad de ocurrencia de la amenaza y

cuál es el activo que ha sido impactado. Presentado en una ecuación matemática para la combinación válida de activos y amenazas:

RT (riesgo total) = probabilidad x impacto

El proceso de análisis descrito genera habitualmente un documento que se conoce como matriz de riesgo, donde se ilustran todos los elementos identificados, sus relaciones y los cálculos realizados. La sumatoria de los riesgos residuales calculados, es la exposición total de la organización a los riesgos. Realizar el análisis de riesgos es fundamental para lograr posteriormente administrar los mismos.

El objetivo general del análisis de riesgos, es identificar sus causas potenciales de los principales riesgos que amenazan el entorno informático. Esta identificación se realiza en una determinada área para que se pueda tener información suficiente al respecto, optando así por un adecuado diseño e implantación de mecanismos de control con el fin de minimizar los efectos de eventos no deseados, en los diferentes puntos de análisis.

Otros objetivos específicos del proceso de análisis de riesgos son: analizar el tiempo, esfuerzo, recursos disponibles y necesarios para atacar los problemas; llevar a cabo un minucioso análisis de los riesgos y debilidades; identificar, definir y revisar los controles de seguridad; determinar si es necesario incrementar las medidas de seguridad; y la identificación de los riesgos, los perímetros de seguridad y los sitios de mayor peligro, se pueden hacer el mantenimiento más fácilmente.

Algunos aspectos que se debe tener en cuenta antes de realizar el análisis de riesgos son los siguientes: las políticas y las necesidades de la organización, los nuevos avances tecnológicos y la astucia de intrusos expertos, los costos vs la efectividad del programa de mecanismos de control a desarrollar, la junta directiva de la organización debe incluir presupuesto, los gastos necesarios para el

desarrollo de programas de seguridad. Otro aspecto que se debe tener en cuenta es la sobrecarga adicional que los mecanismos y contramedidas puedan tener sobre el entorno informático, sin olvidar los costos adicionales que se generan por su implementación.

El análisis de riesgos utiliza el método matricial llamado MAPA DE RIESGOS, para identificar la vulnerabilidad de un servicio o negocio a riesgos típicos. El método contiene los siguientes pasos: la localización de los procesos en las dependencias que intervienen en la prestación del servicio y la localización de los riesgos críticos y su efecto en los procesos del Negocio.

Estándares Para la Gestión de Riesgos

La gestión de riesgos de seguridad de la información es quizás el proceso más importante para el desarrollo, mantenimiento y mejora de un sistema eficaz de gestión de seguridad de la información. Las metodologías de análisis y/o evaluación de riesgos existentes ayudan en gran medida a las organizaciones a acelerar este proceso.

A continuación se mencionan algunas de las metodologías más utilizadas según (12)

- **NIST RMF**: Se trata de un marco donde la evaluación del riesgo de la información se define mediante un proceso de 6 pasos: clasificar, seleccionar, implementar, evaluar, autorizar y monitorizar. El enfoque es ligeramente diferente de otros que se identificaran a continuación. Este marco ha sido desarrollado por y para las entidades que forman el gobierno de los EE.UU., no obstante, se puede adaptar a cualquier empresa u organización.

- **SP800-30**: Es uno de los 800 informes publicados por NIST. En él se ofrece una guía muy detallada acerca de lo que se debe considerar dentro cualquier proceso de evaluación de riesgos de seguridad. Esta guía incluye listas de verificación detalladas, gráficos, diagramas de flujo y fórmulas de cálculo, así como las referencias a leyes y regulaciones de EE.UU.

- **ISO / IEC 27005**: Forma parte de la familia de normas ISO 27000 o, lo que es lo mismo, los estándares desarrollados por ISO destinados a proporcionar un marco de gestión de seguridad de la información utilizable por cualquier tipo de organización. La ISO 27005 sustituye a la antigua ISO / IEC 13335 y describe el proceso completo de gestión de riesgos dividiéndolo en 6 fases: Establecimiento del Alcance, Valoración de Riesgos (formada por las tareas de Análisis y Evaluación), Tratamiento de Riesgos, Aceptación de Riesgos, Comunicación de Riesgos y Monitorización y Revisión de Riesgos.

  Sus anexos incluyen ejemplos de diversos enfoques, así como listas de posibles amenazas, vulnerabilidades y controles de seguridad.

- **MAGERIT:** Se trata de una metodología desarrollada por el Consejo Superior de Administración Electrónica dependiente del MAP, destinada en un principio a ayudar a los organismos de la administración pública española a conocer el riesgo a que estaban sometidos sus sistemas de información, pero cuyas guías han sido adoptadas por otras entidades de derecho privado. MAGERIT describe los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de aspectos prácticos. En la actualidad se encuentra en su versión 2.

- **OCTAVE:** Es un conjunto de herramientas, técnicas y métodos para llevar a cabo evaluaciones de riesgo de seguridad de información, desarrolladas

por CERT y la Universidad Carnegie Mellon. Tiene diferentes versiones adecuadas para diferentes tamaños y el tipo de organizaciones: OCTAVE-Method está destinado a las grandes organizaciones, mientras que OCTAVE-S es para pymes. Por otra parte, OCTAVE - Allegro es una variación de OCTAVE-Method muy enfocada a los activos de información.

- **FAIR:** Método de evaluación que suele ser utilizado para realizar análisis de riesgos cualitativos y algo más sofisticados por lo que, en ocasiones, suele complementar otras metodologías. FAIR no está disponible por completo de manera pública y por tanto son pocos los usuarios expertos en la materia.

- **TARA:** Fue desarrollada por Intel para llevar a cabo sus evaluaciones de riesgos de seguridad y posteriormente decidió hacerla pública. Se centra en el seguimiento y la evaluación continua de los controles de seguridad, incluyendo documentación de cambios en los sistemas, la realización de análisis de impacto a los cambios asociados, y la premisa de informar sobre el estado de seguridad a los empleados o participantes de la organización de una forma regular.

- **EBIOS:** Es un conjunto completo de guías (además de una herramienta gratuita de software de código abierto), dedicada a los administradores de sistemas. Originalmente desarrollada por el gobierno francés, en la actualidad esta metodología se mantiene gracias a las aportaciones de un grupo de expertos de diversos orígenes. EBIOS se utiliza ampliamente en la administración pública, así como en el sector privado, tanto en Francia como en el extranjero. Es compatible con los principales estándares de seguridad de TI.

MAGERIT

(11), Finalidad: el análisis y gestión de los riesgos es uno de los aspectos claves por medio del cual se regula el Esquema Nacional de Seguridad en el ámbito de la administración de la Administración Electrónica en España (13), que tiene la finalidad de satisfacer el principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información.

MAGERIT es un instrumento para facilitar la implantación y aplicación del esquema de seguridad proporcionando los principios básicos y requisitos mínimos para protección de la información. El estándar MAGERIT es uno de los métodos de análisis y gestión de riesgos de ENISA elaborada por el Consejo Superior de Administración Electrónica en España, que tiene como objetivo: Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de detenerlos a tiempo, el ofrecer un método sistemático para realizar el análisis de los riesgos, además de ayudar a descubrir y planear las medidas oportunas para mantener los riesgos bajo control, y preparar a la organización para procesos de evaluación, auditoría, acreditación o certificación, según corresponda cada caso.

MAGERIT permite hacer el estudio de los riesgos que soporta un sistema de información y el entorno asociado a él, para ello propone realizar la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados. Los resultados del proceso de análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

Organización de las guías

El estándar MAGERIT versión 2 se ha estructurado en tres guías: el Método, el Catálogo de Elementos, y la Guía de Técnicas, a continuación se hablará en más detalle sobre el contenido de las mismas.

- **El método:** Describe los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de aspectos prácticos. La metodología se describe desde tres ángulos y está dividido en capítulos donde cada uno de ellos contiene:
    - El capítulo 2 describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación. Es una presentación netamente conceptual.
    - El capítulo 3 describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, entendiendo que no basta con tener los conceptos claros, sino que es conveniente reglamentar roles, actividades, hitos y documentación para que la realización del proyecto de análisis y gestión de riesgos, esté bajo control en todo momento.
    - ·El capítulo 4 aplica la metodología al caso del desarrollo de sistemas de información, en el entendimiento que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento, tanto los riesgos a que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema.
    - En el capítulo 5 desagrega una serie de aspectos prácticos, derivados de la experiencia acumulada en el tiempo para la realización de un análisis y una gestión realmente efectivos.

Figura 7. Procesos para gestión del riesgo

Fuente: http://www.securityartwork.es/wp-content/uploads/2012/03/magerit.jpg

- **El Catálogo de Elementos:** Que ofrece unas pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información.

- **El Catálogo**: persigue dos objetivos esenciales: el facilitar la labor de las personas que inician el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis y homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

- **La Guía de Técnicas**, que es una guía de consulta que proporciona algunas técnicas que se emplean habitualmente para llevar a cabo

proyectos de análisis y gestión de riesgos, dentro de ellas se encuentran: técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales, análisis coste-beneficio, diagramas de flujo de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi.

Es una guía de consulta que permite el avance por las tareas del proyecto, se le recomendará el uso de ciertas técnicas específicas, de las que esta guía busca ser una introducción, así como proporcionar referencias para que el lector profundice en las técnicas presentadas.

MAGERIT es utilizado por aquellas personas que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

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 Para realizar un análisis general, sobre las diversas dimensiones de seguridad (confidencialidad, integridad, disponibilidad,…), O un análisis de la continuidad, centrado en la disponibilidad del sistema, buscando reducir los tiempos de interrupción del servicio cuando sobrevienen desastres.

En cualquier caso, el análisis puede ser cualitativo o cuantitativo. EAR/PILAR ha sido parcialmente financiada por el Centro Criptológico Nacional.

Metodología

(14), Las herramientas EAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit.

Los activos están expuestos a amenazas que, cuando se materializan, degradan el activo, produciendo un impacto. Si se hace una estimación a la frecuencia con que se materializan las amenazas, se puede deducir el riesgo al que está expuesto el sistema. Degradación y frecuencia califican la vulnerabilidad del sistema.

El gestor del sistema de información dispone de salvaguardas, que o bien reducen la frecuencia de ocurrencia, o bien reducen o limitan el impacto. Dependiendo del

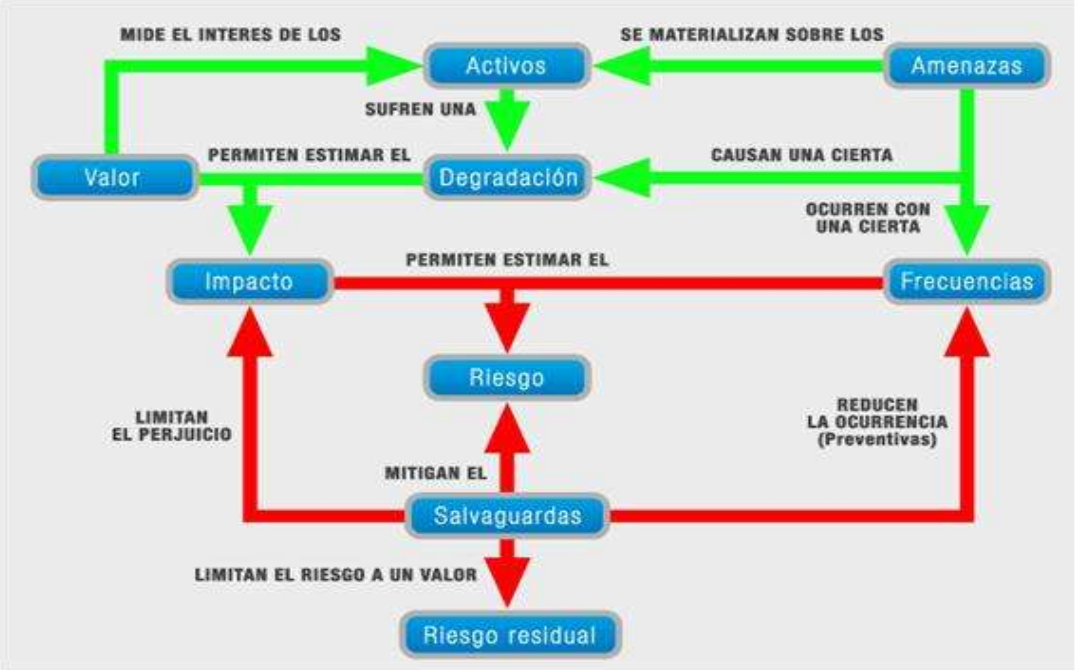
grado de implantación de estas salvaguardas, el sistema pasa a una nueva estimación de riesgo que se denomina riesgo residual.

PILAR (15) 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

Diagrama Funcional de Pilar

Figura 8. Diagrama Funcional de PILAR



Fuente: https://seguridadinformaticaufps.wikispaces.com/PILAR+-+Herramienta+para+An%C3%A1lisis+y+Gesti%C3%B3n+de+Riesgos

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

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.

La probabilidad de una amenaza es un asunto difícil de explicar. PILAR permite varias maneras de plasmar las posibilidades que una amenaza tiene de ocurrir.

Figura 9. Modelo de Amenazas PILAR

potencial	probabilidad	nivel	facilidad	frecuencia intervalo previsto entre ocurrencias
S pequeño	I improbable	B bajo	MD muy difícil	0.1 diez años
M medio	PP poco probable	M medio	D difícil	1 una vez al año
L grande	P probable	A alto	M medio	10 cada mes
XL extra grande	CS casi seguro	MA muy alto	F fácil	100 a diario

Fuente: https://seguridadinformaticaufps.wikispaces.com/file/view/2.JPG/329062198/2.JPG.

- **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 10. 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.

- **Niveles de Criticidad de los Riesgos.** PILAR estima los riesgos según una escala simple de seis valores:

Figura 11. Niveles de Criticidad de los Riesgos

Fuente: https://seguridadinformaticaufps.wikispaces.com/file/view/6.JPG/329062208/6.JPG.

Impacto y riesgo en PILAR

El impacto es un indicador de qué puede suceder cuando ocurren las amenazas.

El riesgo es un indicador de lo que probablemente suceda por causa de las amenazas.

El impacto y el riesgo se mitigan por medio de salvaguardas, viéndose reducidos a valores residuales.

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

En PILAR, se miden los impactos y los riesgos como sigue:

Figura 12. Medición de Impacto y Riesgo

	cualitativo	cuantitativo
impacto	nivel de valor	cantidad numérica
riesgo	nivel de criticidad	cantidad numérica

Fuente: https://seguridadinformaticaufps.wikispaces.com/file/view/7.JPG/329062212/7.JPG.

COBIT

Los términos de métricas, medición y medida en muchos de los casos han sido relacionados con los instrumentos utilizados mediante un método específico al acto mecánico de tomar una medición mediante escalas cualitativas o cuantitativas que determinan los valores de esa medición (16).

En general es así, pero los tres conceptos son diferentes, y serán tratados en este capítulo. Pero lo que no se puede admitir es que sea un acto mecánico, ya que el proceso de medición involucra muchas actividades. Inicia con la selección y definición de la característica que se quiere medir, posteriormente se definirá que métricas es posible usar para la medición, luego se definirá la escala de tipo cuantitativo o cualitativo y el método, y por último se procede a hacer al análisis de cómo se hará la medición.

- **Generalidades del Estándar Cobit.** Las mejores prácticas en auditoria recomiendan Cobit (17), como la herramienta estándar para tecnologías de información más utilizada en la ejecución de auditorías; a continuación se explica detalladamente algunos conceptos manejados por ésta y los dominios, procesos y actividades que lo conforman:

- Efectividad: se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- Eficiencia: se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- Confidencialidad: se refiere a la protección de información sensible contra divulgación no autorizada.
- Integridad: se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- Disponibilidad: se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- Cumplimiento: se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- Confiabilidad de la información: se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.
- Datos: los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, entre otros.
- Aplicaciones: se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
- Tecnología: la tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, entren otros.
- Instalaciones: recursos para alojar y dar soporte a los sistemas de información.

- Personal: habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

- **Niveles de Cobit.** La estructura del estándar Cobit se divide en dominios que son agrupaciones de procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible.

Tabla 1. Distribución de los dominios y procesos de COBIT

DOMINIOS	PROCESOS
PLANEACIÓN Y ORGANIZACIÓN (PO)	PO1 Definir un Plan Estratégico de TI. PO2 Definir la Arquitectura de Información. PO3 Determinar la dirección tecnológica. PO4 Definir la Organización y Relaciones de TI. PO5 Manejar la Inversión en TI. PO6 Comunicar las directrices gerenciales. PO7 Administrar Recursos Humanos. PO8 Asegurar el cumplir Requerimientos Externos. PO9 Evaluar Riesgos. PO10 Administrar proyectos. PO11 Administrar Calidad.
ADQUISICIÓN E IMPLEMENTACIÓN (AI)	AI1 Identificar Soluciones. AI2 Adquisición y Mantener Software de Aplicación. AI3 Adquirir y Mantener Arquitectura de TI. AI4 Desarrollar y Mantener Procedimientos relacionados con TI. AI5 Instalar y Acreditar Sistemas. AI6 Administrar Cambios
SERVICIOS Y SOPORTE (DS)	DS1 Definir niveles de servicio. DS2 Administrar Servicios de Terceros. DS3 Administrar Desempeño y Calidad. DS4 Asegurar Servicio Continuo. DS5 Garantizar la Seguridad de Sistemas. DS6 Identificar y Asignar Costos. DS7 Capacitar Usuarios. DS8 Asistir a los Clientes de TI. DS9 Administrar la Configuración. DS10 Administrar Problemas e Incidentes. DS11 Administrar Datos. DS12 Administrar Instalaciones. DS13 Administrar Operaciones
MONITOREO (M)	M1 Monitorear los procesos. M2 Evaluar lo adecuado del control Interno. M3 Obtener aseguramiento independiente. M4 Proveer auditoría independiente

Fuente: propia

- **Usuarios**
  - La Gerencia: Para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
  - Los Usuarios Finales: Quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.
  - Los Auditores: Para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.
  - Los Responsables de TI: Para identificar los controles que requieren en sus áreas.

También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

- **Características**
  - Orientado al negocio.
  - Alineado con estándares y regulaciones "de facto”.
  - Basado en una revisión crítica y analítica de las tareas y actividades en TI.
  - Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA).

- **Principios**

El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.

- Requerimientos de la información del negocio: Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios:
- Requerimientos de Calidad: Calidad, Costo y Entrega.
- Requerimientos Fiduciarios: Efectividad y Eficiencia operacional, Confiabilidad de los reportes financieros y Cumplimiento le leyes y regulaciones.

HETICAL HACKING

De acuerdo con (18) 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"

Para garantizar la seguridad informática se requiere de un conjunto de sistemas, métodos y herramientas destinados a proteger la información, es aquí donde entran los servicios del Ethical Hacking , la cual es una disciplina de la seguridad

informática que echa mano de una gran variedad de métodos para realizar sus pruebas, estos métodos incluyen tácticas de ingeniería social, uso de herramientas de hacking , uso de Metasploits que explotan vulnerabilidades conocidas, en fin son válidas todas las tácticas que conlleven a vulnerar la seguridad y entrar a las áreas críticas de las organizaciones.

METAEXPLOITS

Para empezar a hablar del metasploit, (19), lo definiremos como una herramienta GNU.

Escrita en perl y con utilización de diversos lenguajes de programación como C, Python, ASM ,etc, para el desarrollo, testeo, mejora y penetración a diversos sistemas, entre ellos Windows.

Metasploit se ejecuta bajo una consola CYGWIN y trabaja con una base de datos en la cual se encuentran toda la lista de exploits y vulnerabilidades, lo único que tenemos que indicarle a metasploit es que vulnerabilidad utilizaremos, que sistema atacaremos, que tipo de ataque utilizaremos y datos diversos que utilizara para atacar al host.

Se llama Metasploit Framework porque es todo un entorno de testeo para diversas plataformas, la cual trabaja con librerías, bases de datos, y diversos programas, shell codes, etc. Por tal deja de ser un simple software si no un framework. El FrameWork de **Metasploit** es una herramienta de penetración de código libre, desarrollado para ejecutar exploits a un objetivo remoto. Metasploit cuenta con la mayor base de datos de exploits públicos y probados y puede ser usado para detectar las vulnerabilidades de nuestros sistemas para protegerlos o usar esas vulnerabilidades para obtener acceso a sistemas remotos.

Un 'exploit' es un programa o técnica que aprovecha una vulnerabilidad. Los exploits dependen de los sistemas operativos y sus configuraciones, de las configuraciones de los programas que se están ejecutando en un ordenador y de la LAN donde están. Pero ¿qué es una vulnerabilidad? Una 'vulnerabilidad' es "algo" de un sistema informático que evitará que se pueda usar correctamente, o que permitirá que lo controlen personas no autorizadas. Hay muchos tipos de vulnerabilidades. Puede haber un error en la configuración del servicio o bien un error en la programación del servicio. Pueden estar creados en cualquier lenguaje. Los exploit para windows suelen estar hechos en C y/o ensamblador, mientras que los de unix pueden estar hechos también en perl por ejemplo, aunque suelen estar hechos en C.

NESUSS

Nessus es un programa que escanea vulnerabilidades de diversos Sistemas Operativos (Windows - Linux - Mac - Solaris, etc...), además de encontrar errores de configuraciones y vulnerabilidades, ya sean por falta de actualización del S.O, puertos que pueden llevar a sesiones meterpreter, procesos Web o fallos en softwares instalados (Apache, Mysql, entre otros).

BACTRACK

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 Backtrack 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.

GFI LAN GUARD

Es una solución de escáner de red y de seguridad, que permite analizar la red y puertos para detectar, evaluar y corregir vulnerabilidades de seguridad con el mínimo esfuerzo administrativo.

Esta herramienta actúa como un consultor virtual de seguridad ofreciendo:

- Administración de actualizaciones.
- Evaluación de vulnerabilidad.
- Auditoría de red.

Además le ayuda en el inventario, la gestión de cambios, el análisis de riesgo y probar el cumplimiento, proporciona una completa imagen de su configuración de red y le ayuda a mantener seguro y en conformidad el estado de la red.

Principales características:

- Administración de actualizaciones para sistemas operativos y aplicaciones Microsoft® y Max OS X.
- Implementa software a medida y de terceros y actualizaciones en toda la red.
- Administración de actualizaciones para otras aplicaciones (no Microsoft).
- Corrección automática de aplicaciones no autorizadas.
- Conexión a escritorio remoto.

- Evaluación de vulnerabilidad

Durante las auditorías de seguridad se realizan más de 50 mil evaluaciones de vulnerabilidad -escaneando la red IP por IP. Proporciona la capacidad de realizar análisis multi-plataforma (Windows, Mac OS, Linux) a través de todos los entornos, incluyendo Máquinas Virtuales y para analizar la configuración y estado de la seguridad de la red. Esta herramienta permite identificar y corregir cualquier amenaza antes de que los hackers puedan aprovecharlas.

Auditoría de red y software

La auditoría de red le da una visión completa de su red -cómo los dispositivos USB están conectados, qué software está instalado, comparticiones abiertas, puertos abiertos y contraseñas débiles en uso, y la información del hardware. Informes detallados del estado de la red. Los resultados del escaneo pueden ser fácilmente analizados utilizando filtros e informes, lo que permite asegurar de forma proactiva la red mediante el cierre de los puertos, eliminar usuarios o grupos que ya no están en uso, o desactivar puntos de acceso inalámbricos.

4.4 MARCO LEGAL

El creciente uso de las nuevas tecnologías ha propiciado la creación de un marco legal y jurídico (11) que protege a todas las partes interesadas en el uso de estas tecnologías y el intercambio y tratamiento de la información a través de ellas.

Cada día surgen nuevas formas de delito informático que pueden afectar a la seguridad de la información en nuestras empresas.

Por ello, cumplir con la legislación vigente en nuestro país es uno de los requisitos que se debe satisfacer, el cumplimiento de los objetivos planteados en este proyecto, su cumplimiento permite la protección de amenazas externas, además

de respetar los derechos de los clientes y proveedores y evitará infracciones involuntarias con sus respectivos costos.

Algunas de las leyes y normas de la legislación colombiana relacionada con seguridad de la información tomadas de (20):

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

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.

Objeto. tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

Ley No 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones

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.

Ley 599 de 2000: Los delitos consagrados en el Código Penal Colombiano, tienen plena aplicación, bajo el entendido en que se cumplan las condiciones establecidas para cada acto criminal, sin importar si se comete en medios tradicionales o electrónicos.

4.5 MARCO CONCEPTUAL

A continuación se definen algunos términos que serán mencionados y utilizados en el desarrollo del proyecto de acuerdo con (11).

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: Es una herramienta de diagnóstico que permite establecer la exposición real a los riesgos por parte de una organización. Este análisis tiene como objetivos la identificación de los riesgos (mediante la identificación de sus elementos), lograr establecer el riesgo total y posteriormente el riesgo residual luego de aplicadas las 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.

Evaluación de Riesgos: Este proceso incluye la medición del potencial de las pérdidas y la probabilidad de la pérdida, categorizando el orden de las prioridades.

Un conjunto de criterios puede ser usado para establecer una prioridad, enfocada en el impacto financiero potencial de las pérdidas, por ejemplo: riesgos críticos, que son todas las exposiciones a pérdida en las cuales la magnitud alcanza la bancarrota, riesgos importantes donde las exposiciones a pérdidas que no alcanzan la bancarrota, pero requieren una acción de la organización para continuar las operaciones, riesgos no importantes que son las exposiciones a pérdidas que no causan un gran impacto financiero.

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”.

SGSI: SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

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.

EAR PILAR: herramienta para el soporte a la tarea de Análisis y Gestión de los Riesgos de los Sistemas de Información, financiada por el Centro Cristológico Nacional (CCN), sigue la metodología Magerit, elaborada y publicada por la administración pública Española: 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.

Objetivos de Control y Riesgos: Los riesgos incluyen fraudes, errores, interrupción del negocio, y el uso ineficiente e inefectivo de los recursos. Los objetivos de control reducen estos riesgos y aseguran la integridad de la información, la seguridad, y el cumplimiento. La integridad de la información es resguardada por los controles de calidad del input, procesamiento, output y software.

Las medidas de seguridad incluyen los controles de seguridad de los datos, física y de programas. Los controles de cumplimiento aseguran la conformidad con las leyes y regulaciones, los estándares contables y de auditoría, y las políticas y procedimientos internos.

Actividades de Control: COBIT y SAC examinan procedimientos de control relativos al sistema automatizado de información de una entidad; COSO discute los procedimientos y actividades de control utilizados en toda la entidad. COBIT clasifica los controles en 32 procesos agrupados naturalmente en cuatro dominios aplicables a cualquier ambiente de procesamiento de información. SAC utiliza cinco esquemas de clasificación diferentes para los procedimientos de control de SI. COSO utiliza solo un esquema de clasificación para los procedimientos de

control del sistema de información (SI). La discusión de COSO sobre las actividades de control enfatiza en quién realiza las actividades y en lo operativo más que en los objetivos de informes financieros. COSO también enfatiza la deseabilidad de integrar las actividades de control con la evaluación de riesgos.

5. PROPUESTA SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE INFORMÁTICA DEL HOSPITAL SUSANA LÓPEZ DE VALENCIA

5.1 PLANIFICACIÓN - ESTABLECIMIENTO DEL SGSI

5.1.1 Alcance del Proyecto

El Área de Tecnologías de la Información y las Comunicaciones Hospital Susana López de Valencia de la ciudad de Popayán comprende una infraestructura de equipos computacionales y software para la interconexión de todas las dependencias y sedes de la institución, brindando la posibilidad de acceso a redes externas, incluyendo internet. Entre los edificios y áreas del Hospital Susana López de Valencia de la ciudad de Popayán que comprende la red de datos, se incluyen, la Administración central de los recursos tecnológicos y su interconexión con las áreas recientemente inauguradas y todas aquellas dependencias que utilicen los recursos tecnológicos ofrecidos por el área de TIC'S.

De esta manera, actualmente se cuenta con todo un soporte tecnológico, mediante un backbone en fibra óptica con todas las áreas y dependencias y un sistema de cableado estructurado en cada uno de los edificios, que cubre el Hospital Susana López de Valencia de la ciudad de Popayán con aproximadamente 450 puntos activos y una red corporativa que permite interconexión entre las distintas áreas y el acceso a INTERNET a través de dos enlaces, uno con Emtel y Claro Comunicaciones.

El SGSI, específicamente se aplicará al Área de Informática, ubicada en la sede principal y administrativa del Hospital Susana López de Valencia de la ciudad de Popayán y en particular al servidor y aplicación llamada Dinámica Empresarial por

ser el servicio más crítico puesto que maneja y controla los procesos de historias clínicas.

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 valuación 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 Hospital Susana López de Valencia de la ciudad de Popayán.

La propuesta será presentada ante la administración del área de Tecnologías de la Información y las comunicaciones del Hospital Susana López de Valencia de la ciudad de Popayán, para su posible implementación.

5.1.2 Metodología para recolección de información

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

- **Las técnicas de recopilación de datos**: son los procedimientos de medición o recopilación mediante los cuales es posible recopilar datos o mediciones exactas, es decir válidas, fiables y objetivos y por lo tanto de

utilidad para el objeto de estudio, dentro de las técnicas utilizadas encontramos las siguientes:

- **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 utilizó en las visitas guiadas por el personal de sistemas del Hospital Susana López de Valencia a 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**: esta 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 fue utilizado en las reuniones programadas que durante el desarrollo del mismo se realizaron con el 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.

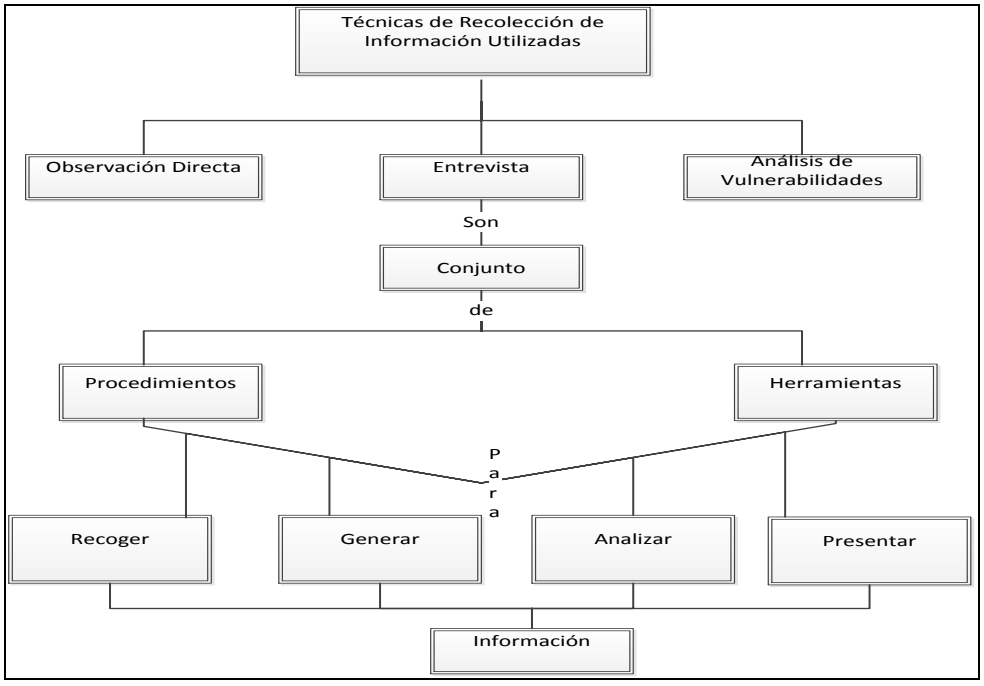
  Igualmente se hizo uso de la entrevista dirigida mediante una serie de encuestas y listas de chequeo, apoyándonos en muchas ocasiones en el uso de controles de ISO 27000 y de COBIT, a fin de poder obtener la mayor cantidad de información precisa y valida que nos facilitara la identificación de posibles fallas, falencias, vulnerabilidades y aspectos por mejorar que

rodean el uso de los recursos tecnológicos dentro del hospital Susana López de Valencia ESE Popayán.

- **Pruebas de Penetración y Ethical Hacking**: en este proceso se hizo uso de herramientas software (libres y comerciales), las cuales fueron ejecutas y probadas en los ambientes de producción (servidores y aplicaciones propias del core del negocio del hospital), bajo supervisión del personal a cargo de la administración de los recursos en el área de Informática y sistemas del Hospital y sobre todo fueron planeadas y ejecutadas en horarios con menor afectación o impacto en los recursos, los fines de semana y en horarios donde el tráfico y acceso a los recursos era menor.

En la figura 13, se puede observar, los instrumentos de recolección de información utilizados para la recolección de información en el presente proyecto

Figura 13. Técnicas de recolección de información utilizadas

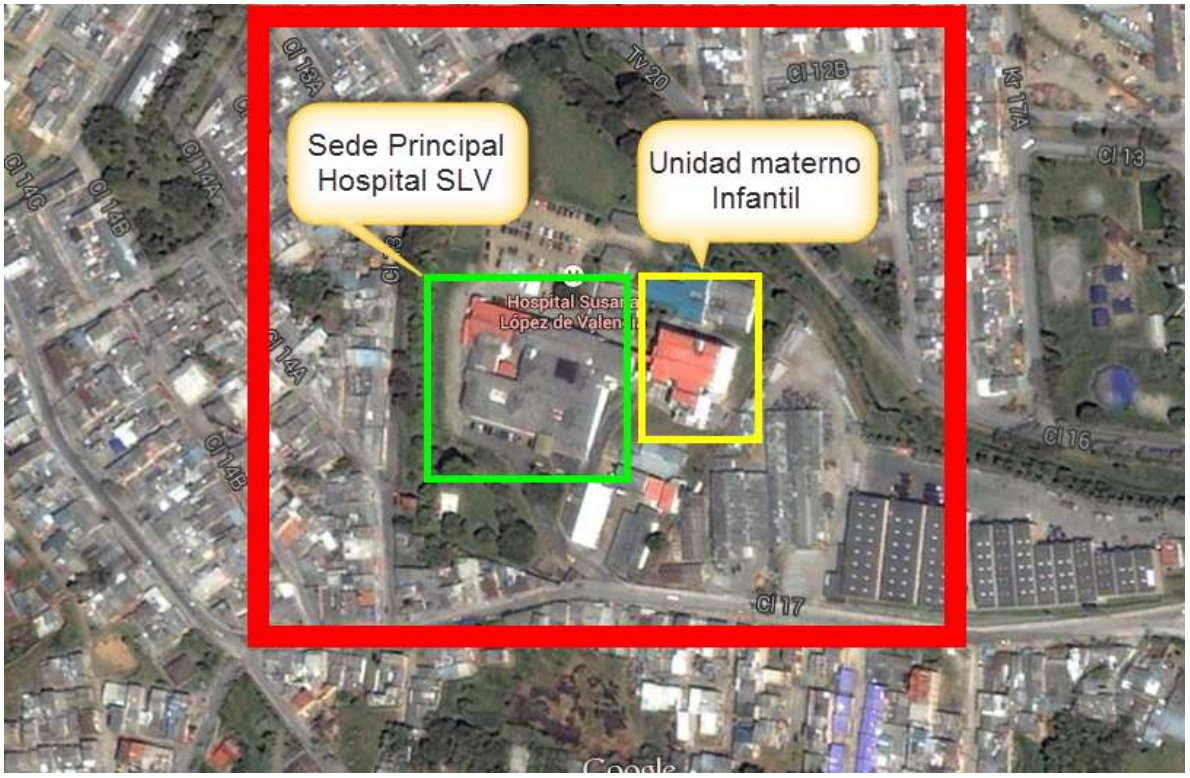


Fuente: Propia

5.1.3 Definición y descripción del entorno de aplicación.

En la figura 14 se puede apreciar una vista aérea de las instalaciones de la sede principal la nueva construcción dedicad a la atención materno infantil

Figura 14. Ubicación geográfica Hospital Susana López de Valencia



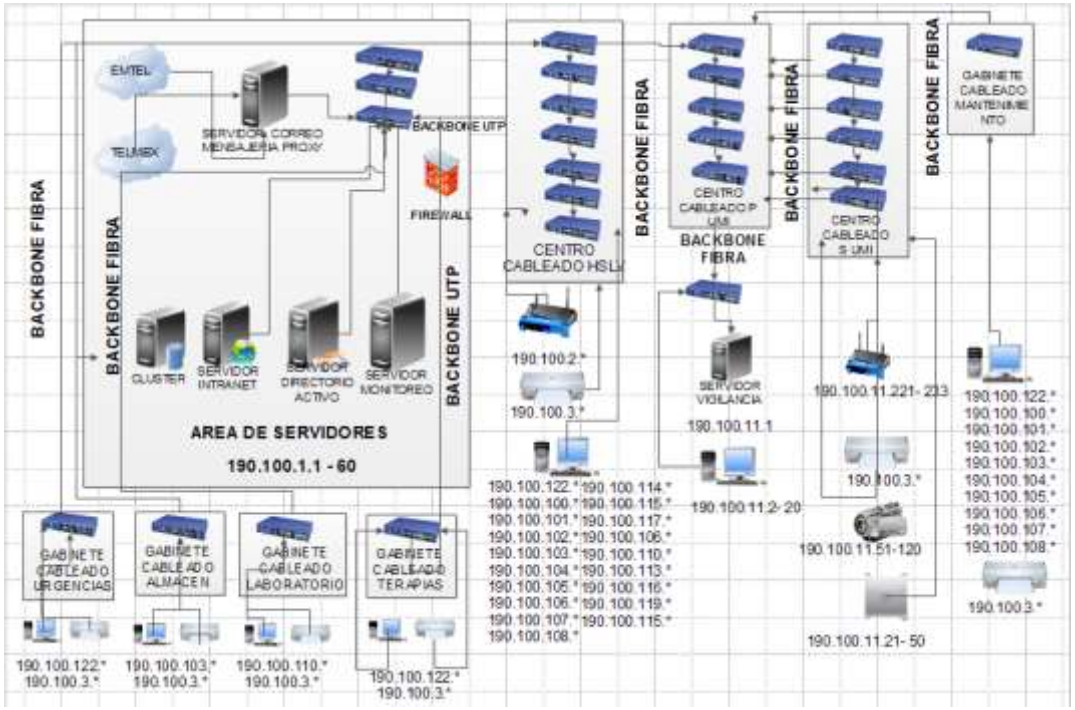
Fuente: https://www.google.com/maps/@2.4370374,-76.6190586,1375a,20y,15.81h/data=!3m1!1e3

Se tienen dos proveedores del servicio de internet en la actualidad, CLARO[3] con un canal de Banda Ancha de 60 Megas y EMTEL[4] con un canal de Banda Ancha de 10 Megas. El núcleo de la red (core) se encuentra en la sede principal, oficina de TI de donde se provee a toda la infraestructura del servicio de red. Para la conexión con las demás áreas o edificios dentro del Hospital, esta se realiza

[3] CLARO: Operador de Telmex Colombia S.A.
[4] EMTEL: Empresa Municipal de Telecomunicaciones S.A.

mediante Backbone de Fibra Óptica. Se hace uso de routers para conectar la sede principal y de switchs de core e interconexión con las demás áreas, en la actualidad el Hospital Susana López de Valencia de la ciudad de Popayán cuenta con un centro de cableado principal y de 8 subcentros de Cableado tanto de red como de voz tal como se puede observar en la Figura 15 y se especifica en la Tabla 2.

Figura 15. Infraestructura de Interconexión HSLV



Fuente: propia.

Tabla 2 Relación y Conexión entre Áreas Hospital Susana López de Valencia

Nombre del Área	Conexión	Tipo de Conexión
Granja de servidores	Subcentro Principal	Par Trenzado UTP
Gabinete Urgencias	Subcentro Principal	Fibra Óptica
Gabinete Almacén	Subcentro Principal	Fibra Óptica
Gabinete Laboratorio	Subcentro Principal	Fibra Óptica
Gabinete Terapias	Subcentro Principal	Fibra Óptica
Centro de Cableado HSLV	Subcentro Principal	Fibra Óptica
Centro de Cableado UMI 1	Backbone Principal	Fibra Óptica
Centro de Cableado UMI 2	Backbone Principal	Fibra Óptica
Gabinete Mantenimiento	Subcentro Principal	FO

Fuente: propia.

Así mismo se solicita la información del inventario tecnológico existente y de recurso humano encargado del área, el resumen se puede ver en la tabla No 3.

Tabla 3. Resumen Inventario Tecnológico/Humano

CATEGORÍA	ITEM	DESCRIPCIÓN / CANTIDAD
SOFTWARE	Sistemas operativos	Centos 5,4; Windows XP; Windows Vista; Windows Seven; Windows 8
	Software ofimática	Office 2003; Office 2007; Office 2010; 2013; Openoffice
	Software desarrollo	SQL Server 2008; Visual Studio; Visual Fox Pro 8; MYSQL, PHP 5.X
	Navegadores	Internet Explorer; Mozilla Firefox; Google Chrome
	Sendmail	
	Vnc servidor cliente	
	Firestarter	
	Pandion	
	Antivirus	Symantec Endoint Protetion
	Dinamica gerencial	Versiones Dinamica 2,0 version FOX ; Dinamica Gerencial 2,0; Dinamica Gerencial 3.5
	Plataforma hospital	
	Sql server	
	Thunderbird	
	Internet information server	
HARDWARE	Servidor eros	1
	Cámara de vigilancia	27 cámaras de vigilancia UMI, 16 cámaras edificio antiguo
	Servidor antivirus	1
	Servidor Linux	1
	Puntos de acceso	13 Puntos de acceso Inalámbrico; 10 Puntos de acceso inalámbrico edificio antiguo
	Teléfonos	100
	Pcs terminales	293 terminales Marca Dell
	Switch	26, 1 capa 3
	Servidor bases de datos	1
	Servidor ares	1
	Impresoras	71 Impresoras Marcas HP, Lexmark, Epson
COMUNICACIONES	Red local	
	Red telefónica	
	Conexión a internet principal	Claro 60 Megas
	Radios portátiles	

	Red inalámbrica	
	Conexión a internet de respaldo	Emtel 10 Megas
SISTEMAS DE RESPALDO ELECTRICO	Ups de respaldo	
	Planta eléctrica	
SEDES FISICAS	Hospital Susana López de valencia	
	Unidad materno infantil	
PERSONAL	Ingeniero de sistemas	Ing. Cristian Diego Gonzalez H. (Administrador de Red) Ing. Nelson Chacon (DBA)
	Ingeniero jefe de sistemas	Ing. Robert Camacho
	Auxiliar sistemas	Laura Martínez (Auxiliar de Soporte)
	Técnicos sistema soporte	Cesar Sierra (Técnico de Mantenimiento) Mario Martinez (Técnico Mantenimiento) Felipe Castillo (Tecnico de Soporte)
	Técnico sistemas desarrollo	Jhon Arevalo(Programador) Camilo Gómez(Programador)

Fuente: propia.

El objetivo de la red actual es permitir el acceso a todos los sistemas de información que se proporcionan desde la oficina de Tecnologías de la Información y las comunicaciones con una aceptable calidad de servicio, procurando hacer una convergencia del servicio con fines de monitorización y prevención.

Hay que Enfatizar que como se mencionó anteriormente, este proyecto busca realizar el análisis de Riesgos y Recomendaciones necesarias al área de TIC del Hospital Susana López de Valencia Popayán, siendo esta parte su área la encargada de administrar los servicios, y por ende cualquier dispositivo que intervenga en la prestación de los mismos.

En consecuencia se realizó un reconocimiento general del Hospital Susana López de Valencia E.S.E el cual se menciona en el marco contextual.

5.1.4 Políticas de Seguridad. El área de TIC (División de Tecnologías de la Información y las Comunicaciones) del Hospital Susana López de Valencia Popayán depende tanto de su personal y de sus activos para ofrecer servicios que aseguren el bienestar de sus usuarios o clientes o usuarios internos (personal médico, administrativo y de salud) y sus clientes externos (Quienes hacen uso de los servicios ofertados por el Hospital Susana López de Valencia Popayán), además de garantizar el funcionamiento de algunos procesos importantes para la misma institución. Debido a esto, se debe administrar dichos recursos con la debida diligencia y tomar las medidas adecuadas para protegerlos sobre cualquier fallo o lesión.

Entre las amenazas físicas que pueden encontrar en esta división se tienen, el acceso no autorizado, robo, fraude, desastres naturales, fallos técnicos y daños accidentales. Así mismo se tiene el caso de amenazas de ataques cibernéticos y de actividades maliciosas a través de internet, lo que puede llevar a causar lesiones graves a los servicios electrónicos y de las infraestructuras más críticas.

Las políticas de seguridad del área de TIC prevén la aplicación de salvaguardas para reducir el riesgo de lesiones a cualquier activo de la institución. Estas serán diseñadas para proteger a la red como tal, preservar la confidencialidad, integridad, disponibilidad y valor de los activos y asegurar la prestación continua de servicios.

Entre los propósitos de las políticas de seguridad de la información, se tienen (22):

- Proteger la Información.

- Establecer reglas para el comportamiento esperado por los usuarios, los administradores de sistemas, administración y personal de seguridad.
- Los activos deben ser protegidos de acuerdo a los requisitos de seguridad de base y la gestión continua de riesgos de seguridad.
- La Prestación continua de los servicios deben asegurarse a través de los requisitos de seguridad, incluida la planificación de continuidad del negocio y la gestión continúa de riesgos de seguridad.

5.1.5 Metodología de evaluación de riesgos. Como se mencionó anteriormente para el desarrollo de este proyecto se utilizará la metodología de análisis y evaluación de riesgos Magerit, a continuación se muestra un resumen guía de la utilización de la herramienta y posteriormente se desarrollará el análisis a partir de la utilización de la EAR PILAR.

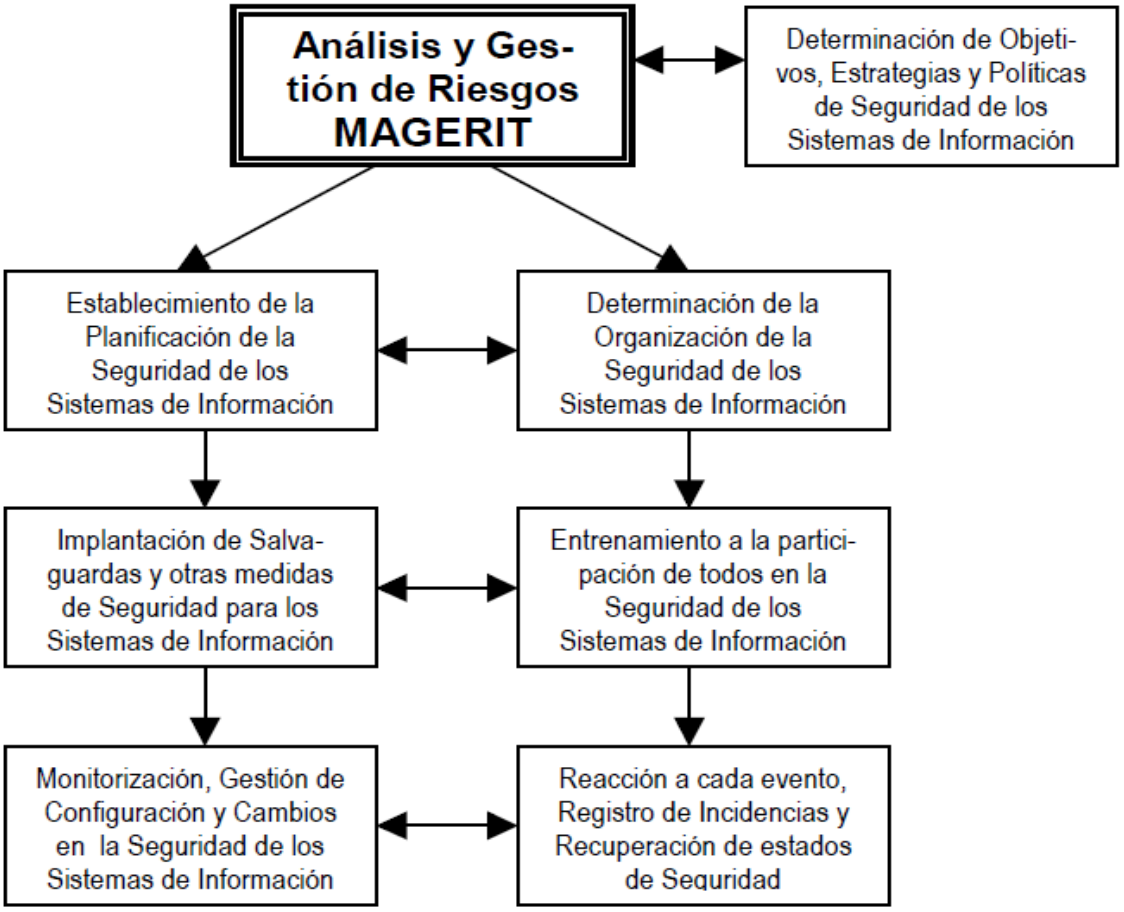
Los responsables y los usuarios de la tecnología de la información son conscientes de la necesidad de disponer de instrumentos tales como metodologías que ayuden a la investigación del estado de seguridad de los sistemas de información (SI) y a la selección de medidas de seguridad proporcionadas, tanto para disminuir las insuficiencias de los sistemas existentes, como para aquellos otros que precisen de reforma o de nuevo desarrollo. No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para así implantar las medidas proporcionadas. Para responder a esta necesidad, el Consejo Superior de Administración Electrónica ha elaborado la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAGERIT, 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. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes

para los ciudadanos, las empresas y la propia Administración Pública, pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en su utilización.

MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados que permitirán a la gestión de riesgos seleccionar e implantar las medidas de seguridad adecuadas para conocer, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios como se puede apreciar en la figura 16.

Este Análisis y Gestión de Riesgos determina la implantación de medidas de salvaguarda que responden al objetivo de mantener la continuidad de los procesos organizacionales soportados por los sistemas de información. Asimismo intenta minimizar tanto el coste global de la ejecución de dichos procesos como las pérdidas de los recursos asignados a su funcionamiento. El Análisis y Gestión de Riesgos es, en consecuencia, el “corazón” de toda actuación organizada de materia de seguridad y, por tanto, de la gestión global de la seguridad. Influye incluso en las fases y actividades de tipo estratégico (implicación de la dirección, objetivos, políticas) y condiciona la profundidad de las fases y actividades de tipo logístico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento

Figura 16. Ciclo de Fases de la Gestión Global de la Seguridad



Fuente: https://seguridadinformaticaufps.wikispaces.com/MAGERIT

De acuerdo a lo especificado en el libro de Magerit (23) llamado el método, la metodología indica que se deben desarrollar dos grandes tareas:

- Análisis de Riesgos
- Gestión del Riesgo

Análisis de Riesgos, permite determinar qué tiene la Organización y estimar lo que podría pasar, en esta tarea se desarrollan las siguientes actividades:

- **Activos:** que no son sino los elementos del sistema de información (o estrechamente relacionados con este) que aportan valor a la Organización
- **Amenazas**: que no son sino cosas que les pueden pasar a los activos causando un perjuicio a la Organización
- **Salvaguardas:** (o contra medidas), que no son sino elementos de defensa desplegados para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

- el impacto: lo que podría pasar
- el riesgo: lo que probablemente pase.

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza.

Gestión de riesgos: Que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las

mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la dirección asume.
Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

A continuación se desarrollaran las actividades propuestas por la metodología magerit para el análisis y gestión de riesgos, aunque para este caso se apoyará en la herramienta EAR PILAR la cual ayudara a realizar todo el proceso de una manera más rápida, organizada y controlada.

Para la Identificación de riesgos, se inició un proyecto en PILAR, en Análisis y Gestión de Riesgo, Realizando un Análisis Cualitativo ver figura 17, el cual valora los activos asignándoles un valor relativo. Al crear dicho proyecto, primero se definen los datos del mismo, esta parte se muestra en la siguiente Figura.

Figura 17. Datos Proyecto Herramienta PILAR

Fuente: Propia

5.1.6 Identificación de Activos. Para la identificación de los activos se plantearon una serie de actividades como visitas a las instalaciones y utilizar diferentes técnicas para el levantamiento de información, entre ellas: la Inspección visual a las áreas de tecnología, la aplicación de encuestas y la realización de entrevistas dirigidas al personal del área de informática del Hospital.

5.1.6.1 Inspección visual de los activos. Los resultados obtenidos de la inspección visual de los activos se clasificaron según su ubicación ya que el hospital cuenta con dos instalaciones el edificio antiguo y la UMI ver figura 18 (Unidad Materno Infantil) que es un nuevo edificio con tecnología de punta.

5.1.6.2 Inspección Visual Edificio Antiguo. En la figura 18 se muestra la entrada al área de servidores

Figura 18. Entrada área de servidores

Fuente: Propia

- Al ingresar a la sala de servidores se encuentra con una cámara de video que apunta a la puerta como medida de seguridad única.
- Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos.

En la Figura 19 se encontró un elemento llamado (cortinas), que por su composición puede causar un incendio dentro de la sala de servidores, al producirse un corto circuito.

Figura 19. Cortinas sala de servidores

Fuente: Propia

Se encuentra a uno de los servidores soportando dos Módems los cuales deben estar en una plataforma que los soporte y no el servidor, el cableado de los módems se encuentra de una manera desordenada y sin marquillas. En este servidor no cuenta con marquillas de identificación. La Figura 20 muestra la evidencia encontrada.

Figura 20. Evidencia en servidor

Fuente: Propia

En la Figuras 21 y 22 se observa dos servidores marca Dell, una consola por la cual se puede realizar el monitoreo de todos los servidores que se encuentran en esta sala.

Se puede identificar que el espacio entre cada servidor es muy limitado para que fluya el aire. Ya que se cuenta con un espacio suficiente se podrían separar un poco para mejorar la ventilación entre estos equipos y así se evita que los dispositivos se sobre calienten, disminuyan su velocidad de procesamiento y que llegado el caso que se puedan apagar por sobrecalentamiento.

La consola para el rack y monitoreo de los servidores es una pantalla con teclado y mouse para trabajar sobre los servidores en algunos procesos de configuración, el cual debería de tener una llave para poder ser abierto este rack.

Figura 21. Consola de administración servidores

Figura 22. Servidores Dell

Fuente: propia

En la Figura 23 se encuentra uno de los servidores sobre una mesa de madera. Este elemento no puede estar en la sala de servidores por ser un elemento vulnerable al fuego.

Se encuentra un disco externo junto a este servidor y no cuenta con una marquilla de identificación de aplicaciones instaladas o lo que está soportando, además puede ser utilizado para sacar información sensible de alguno de los servidores.

Figura 23. Mesa de madera en área de servidores

Fuente: Propia

- Sistema de eléctrico en la sala de servidores se encuentra soportado por una ups con baterías secas.
- Las tomas no se encuentran con las marcas de electricidad regulada.
- Los cables de datos se encuentran por enredados en los cables de energía siendo esto uno de los generadores de ruido en el cableado de datos.
- 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.
- La ups no está sobre una base adecuada.

La evidencia de estos hallazgos encontrados se puede observar en la Figura 24

Figura 24. Evidencia sistema eléctrico área de servidores

Fuente: Propia

En la Figura 25 se encuentra el tablero de control eléctrico regulado y este se encuentra dentro de la sala de servidores, como un elementó de mucho cuidado.

Figura 25. Tablero de control eléctrico área de servidores

Fuente: Propia

En la Figura 26 se encuentra el sistema de aire acondicionado de la sala de servidores. El cual se encuentra en la parte superior de una de las paredes y apuntando su salida al frente del armario donde se encuentran los servidores.

Figura 26. Aire acondicionado área servidores

Fuente: Propia

En la Figura 27 se encuentra el desfogué del agua del aire acondicionado. Este se encuentra tapado por una tabla de madera y no metálica para evitar que se pueda causar un accidente dentro de la sala de servidores.

Figura 27. Desfogue aire acondicionado área de servidores

Fuente: Propia

Con lo que no se cuenta dentro de esta sala de servidores para que sea un centro de datos en las mejores condiciones en la protección de los datos.

- No cuenta con un extractor de calor.
- No cuenta con medidores de temperatura y humedad.
- No cuenta con un sistema de detección contra incendios o de humo.
- La puerta no está protegida con un retardante contra el fuego.
- El sistema de marquillas en los servidores no es la adecuada.
- El sistema de marquillas en los cables de datos no se encontró.
- El sistema de marquillas en los cables eléctrico no es el más correcto en si cuenta con el sistema de energía regulada.
- No cuenta con un protocolo de acceso a la sala de servidores ni quiénes son los autorizados, ni registro de entrada, el para qué ingreso y a qué horas salió de la sala.

En la Figura 28 se encuentra uno de los extintores que se encuentran en la entrada de la sala de los servidores. Cumpliendo así con una de las normas de control contra incendios.

Figura 28. Extintor área de servidores

Fuente: Propia

En la Figura 29 se puede observar los switches que soportan la transmisión de los datos de la red del hospital. Esta es una de las más importantes áreas de informática ya que por estos dispositivos se interconectan todas las áreas del hospital y se maneja el core del negocio.

Cuenta con los dispositivos de ups para evitar que se interrumpan la transmisión de datos en estos dispositivos a la sala de servidores.

Figura 29. Switches Centro de Cableado

Fuente: Propia

La Figura 30 indica el ingreso de todos los cables de hacen la interconexión de cada una de las áreas del hospital y al fondo a la derecha se observa un extractor de calor el cual no se encuentra en funcionamiento durante el día de trabajo por generar mucho ruido. También se puede observar que cada una de los cables se encuentra con sus marquillas.

Figura 30. Distribución de cableado

Fuente: Propia

En la Figura 31 se observa uno de los dispositivos de comunicación el cual recibe los conectores de fibra óptica el cual tiene el backbone entre los switches del antiguo edificio y la UMI.

Figura 31. Distribución Backbones Fibra Óptica

Fuente: Propia

En la Figura 32 se observa la distribución de los monitores, teclados y mouse en el sitio de trabajo del personal asistencial, en horas laborales claramente se puede hacer una recomendación en la que este personal no debe tener bebidas muy cerca de los dispositivos porque se puede causar un accidente a los equipos de trabajo.

Figura 32. Usuarios del Área de Atención Asistencial

Fuente: Propia

En la Figura 33 se puede observar el uso de un protector para los cables cuyo objetivo es evitar que estos sean causantes de algunos accidentes al enredarse con cualquier elemento.

Figura 33. Manejo de Cables

Fuente: Propia

En la Figura 34 se observa cómo están ubicadas las CPU por debajo del escritorio en una forma no tan conveniente tanto para el usuario y su equipo, por la incomodidad que le causa, y que accidentalmente podría desconectarlo.

Figura 34. Ubicación inadecuada de equipos

Fuente: Propia

Los tableros de algunos circuitos se encuentran en el área de atención hospitalaria y están debidamente marcados como se muestra en la Figura 35

Figura 35. Tableros de circuitos área asistencial

Fuente: Propia

En la Figura 36 se puede observar algunos de los sistemas de video cámaras para salvaguardar la información del Hospital Susana López De Valencia

Figura 36. Cámaras de vigilancia área asistencial.

Fuente: Propia

5.1.6.3 Inspección visual recursos informáticos en el edificio de la UMI (Unidad Materno Infantil). En la Figura 37 se encuentra con unos sistemas de seguridad de última generación como una cámara que gira los 360º y un detector de metales y otros elementos que una persona en particular no debería estar cargando como lo son armas de fuego, cuchillos entre otros.

Figura 37. Equipos de seguridad entrada UMI

Fuente: Propia

En la Figura 38 se encuentra el sistema de control de acceso por tarjeta magnética la cual está registrada a una persona con los privilegios de entrar al área de ups, área de interconexión de todo el edificio de la UMI.

Figura 38. Control tarjeta magnética

Fuente: Propia

En la Figura 39 se muestra una de las puertas del edificio de la UMI por la cual se ingresa al área de energía regulada y cuenta con un sistema de verificación de ingreso.

Figura 39. Control Biométrico cuarto técnico

Fuente: Propia

En la Figura 40 se encuentran los paneles de control de cada una de las UPS que son el soporte del edificio para todos los sistemas de información de la UMI.

Figura 40. Paneles de control UPS UMI

Fuente: Propia

En la Figura 41 se encuentra que cada una de las ups en su forma, tamaño y su distribución en el cuarto destinado para las mismas, una al lado de la otra separadas por un regulador; Además estas ups se pueden monitorizar vía red accediendo a cada una de ellas para consultar su estado y su comportamiento.

Figura 41. UPS UMI

Fuente: Propia

En la Figura 42 se puede observar cómo llegan cada uno de los cables eléctricos que son soportados en una escalerilla metálica y entran a los tableros en el cual quedarán marcados de acuerdo con la distribución de los circuitos en el plano eléctrico.

Figura 42. Distribución cables eléctricos área de UPS UMI

Fuente: Propia

En la Figura 43 se encuentra los armarios donde se encuentran los Patch panel, Switches, Router y equipos de voz. Además en este cuarto no se observa ningún computador solo los dispositivos de trasporta de datos de la UMI.

Figura 43. Armarios de distribución centro de cableado UMI

Fuente: Propia

En la Figura 44 se puede observar cómo están distribuidos cada uno de los cables de red que llegan a los paneles para ser identificados uno a uno y así poder saber de donde es cada uno de ellos y a qué servicio pertenece dentro de la UMI.

Figura 44. Distribución de cables en centro de cableado UMI

Fuente: Propia

En la Figura 45 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 45. Soporte red de cableado UMI

Fuente: Propia

En la Figura 46 se identifican los elementos contra incendios que deben existir en cada cuarto de equipos de comunicaciones y de red en el edificio de la UMI como norma de seguridad.

Figura 46. Elementos de seguridad contra incendios UMI

Fuente: Propia

En la Figura 47 se muestra las señales ubicadas la sala donde están centralizados todos los circuitos en la subestación eléctrica.

Figura 47. Señales de advertencia Subestación Eléctrica

Fuente: Propia

En la Figura 48 se observan las marquillas de cada uno de los armarios en los cuales se advierte el peligro de que cada uno de estos dispositivos maneja altos voltajes de electricidad.

Figura 48. Marquillado de Armarios

Fuente: Propia

En la Figura 49 se observa cómo están constituidos cada una de las cajas de controles que conforman el área de la subestación además estas son monitorizadas por estar conectadas a una red de sensores los cuales están programados a un software con una serie de alarmas para mantener el control de la subestación en completo funcionamiento.

Figura 49. Controles subestación eléctrica

Fuente: Propia

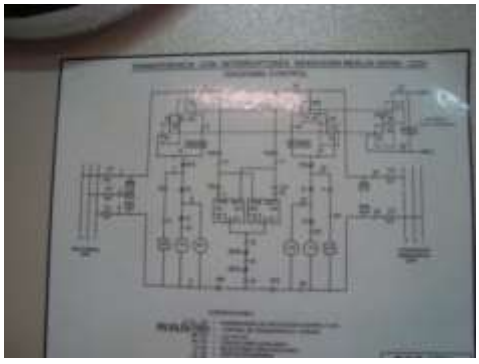
En la Figura 50 se observan las transferencias del edificio UMI las cuales se encuentran en automático y estas se realizan a los 8 segundos de generar el corte del fluido eléctrico esto hace que las UPS no se cuelguen de su capacidad que soporta.

Figura 50. Transferencias Subestación Eléctrica

Fuente: Propia

En la Figura 51 se encuentra uno de los planos de las tres transferencias con las que cuenta el centro hospitalario. Se aclara que las otras dos también cuentan con sus planos.

Figura 51. Planos eléctricos en las transferencias



Fuente: Propia

En la Figura 52 se observa la identificación de los circuitos de la subestación eléctrica de la UMI.

Figura 52. Identificación circuitos subestación eléctrica UMI

Fuente: Propia

En la Figura 53 se puede observar los paneles de circuitos del primer edificio del hospital. Estos eran análogos y no se podrían monitorizar remotamente.

Figura 53. Circuitos estación eléctrica edificio antiguo

Fuente: Propia

En la Figura 54 se puede observar los controles de trasferencia del circuito viejo además todos los controles son análogos una de las opciones de la trasferencia es automática.

Figura 54. Controles de transferencia edificio antiguo

Fuente: Propia

En la Figura 55 se encuentra el transformador que soporta la subestación vieja el cual esta refrigerado por aceite.

Figura 55. Transformador subestación eléctrica edificio antiguo

Fuente: Propia

En la Figura 56 se observa el transformador de la subestación del edificio nuevo que es la UMI. El cuál es el soporte de los circuitos del edificio. Este transformador es de una composición de refrigeración en seco.

Figura 56. Transformador subestación eléctrica UMI

Fuente: Propia

La Figura 57 muestra el panel de control de las tierras de la subestación eléctrica de la UMI.

Figura 57. Tierras

Fuente: Propia

En la Figura 58 se observa el panel de control de la planta eléctrica de la UMI el cual es digital y se pueden realizar las acciones de encendido, apagado y monitorizar su funcionamiento.

Figura 58. Consola de administración subestación eléctrica UMI

Fuente: Propia

En la Figura 59 se observa el tanque de combustible de la planta eléctrica vieja el cual presenta una fuga de combustible. Se le recomienda al administrador del servicio de energía del Hospital que le realice el mantenimiento correctivo antes de que se pueda causar un accidente de grandes proporciones.

Figura 59. Tanque de combustible subestación eléctrica edificio antiguo

Fuente: Propia

En la Figura 60 se pueden observar unas de las más grandes fallas de se pudieron encontrar en el edificio de la UMI en su subestación, en donde en la parte superior de la subestación 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 el edificio.

Se recomienda la desviación de estos ductos de agua por otro lado y que queden lejos de la subestación para evitar algún desastre.

Figura 60. Tuberías subestación eléctrica UMI

Fuente: Propia

El primer paso fue generar un plano de la topología de la red para determinar la ubicación de los activos. El plano de la red de la Institución se muestra en la como se puedo observar en la figura 15

5.1.6.4 Activos Área de Informática Hospital Susana López. El primer paso para la realización del análisis de riesgos en el Hospital Susana López de Valencia fue identificar los activos esenciales para el funcionamiento del core del negocio de esta Institución. Para este fin se realizaron entrevistas a los ingenieros encargados del área de T.I. y se realizó una visita a los centros de cableado, área de servidores y las diferentes áreas funcionales del hospital. El resultado de este proceso fue la siguiente clasificación de activos.

[BK] BACKUP: Este activo representa las copias de seguridad de la información de la base de datos que se realizan de forma automática cada 8 horas y se guarda en un disco duro de un servidor, además se realiza una copia diaria en DVD y una semanal externa que se entrega al jefe del área de Informática, Este activo es importante para la institución en cuanto a que debe protegerse el acceso a las copias de seguridad porque contienen los datos de historia clínica y otros documentos que son de carácter confidencial por ley.

[SO] SISTEMAS OPERATIVOS: Este activo agrupa todos los sistemas operativos presentes en los equipos del hospital como son Windows server 2003, Windows XP, Windows Vista, Windows Seven, 8 y Centos los cuales poseen licencias empresariales.

[OF] SOFTWARE OFIMÁTICO: Este activo agrupa todos los paquetes ofimáticos instalados en los equipos del hospital como son Office 2003, Office 2007, Office 2010 y open office los cuales poseen sus respectivas licencias.

[**DE] SOFTWARE DE DESARROLLO**: Este activo agrupa todos los paquetes software que se utilizan para el desarrollo de aplicaciones en la institución como son Microsoft Visual Studio 2008, Microsoft Visual Fox pro 8.0, Microsoft SQL server 2008 los cuales cuentan con sus respectivas licencias y paquetes de licencia GPL como MYsql, PHP.

[NA] NAVEGADORES: Agrupa todos los navegadores instalados en los equipos del hospital como son: Internet Explorer, Mozilla Firefox, Google Chrome.

[SM] SENDMAIL: Es el "agente de transporte de correo" (MTA - Mail Transport Agent) en Internet, cuya tarea consiste en "encaminar" los mensajes correos de forma que estos lleguen a su destino y se configuro para prestar el servicio de correo interno a los funcionarios del Hospital.

[UV] VNC SERVIDOR CLIENTE: VNC es un programa de software libre basado en una estructura cliente-servidor el cual permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente y se utiliza en el hospital para acceder remotamente a los servidores desde la oficina de Informática.

[FS] FIRESTARTER: Firestarter es una herramienta de cortafuegos personal libre y de código abierto que usa el sistema (iptables/ipchains) Netfilter incluido en el núcleo Linux y se configuro satisfacer los requerimientos mínimos de seguridad de la red del hospital.

[EJ]: EJABBERD es un servidor de mensajería instantánea (M.I) de código abierto (GNU GPL) para plataformas Unix (BSD, GNU/Linux, etc), Microsoft Windows y otras.

[PA] PANDION: Un cliente de mensajería instantánea es una aplicación que permite al usuario hacer uso de la mensajería instantánea.

[AN] ANTIVIRUS: Es una herramienta cuyo objetivo es detectar y eliminar virus informáticos. En el hospital se encuentra instalado el antivirus Symantec Endpoint Protection.

[DG] DINAMICA GERENCIAL: DGH es un Sistema Modular Completamente Integrado para el Manejo Médico, Operativo y Financiero para IPS Públicas y Privadas. Consta de más de 35 módulos que integran totalmente el Área Científica con la Facturación y Contabilidad. Es decir, desde el mismo acto médico (Historia Clínica Digital) se afecta en forma automática todo el sistema de información. DGH cumple con todas las normas exigidas por la Ley para el manejo Financiero, Facturación Ley 100 e Historia Clínica, además que cumple con estándares internacionales como HL7, XML, DICOM, TELEMEDICINA, entre otros. Dinámica Gerencial fue comprada por el hospital y es el programa principal de interacción de los usuarios del hospital con las bases de datos de información.

[PH] PLATAFORMA DEL HOSPITAL: Es una aplicación creada por el desarrollador de aplicaciones del hospital para satisfacer necesidades de información propias de la institución.

[SQ] SQL SERVER: Microsoft SQL Server es un sistema para la gestión de bases de datos producido por Microsoft.

[TB] THUNDERBIRD: Es un cliente de correo electrónico el cual permite a los funcionarios tener un acceso fácil a sus correos internos.

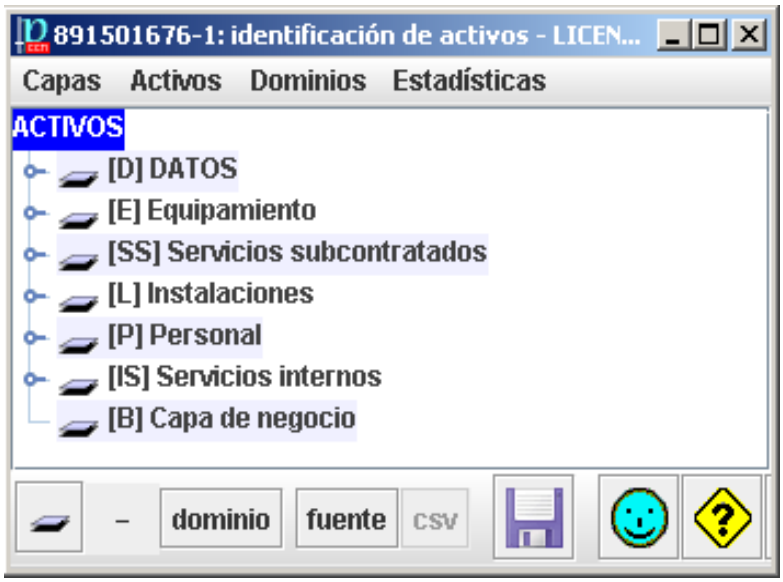
[IIS] INTERNET INFORMATION SERVICES (IIS): Es un servidor web y un conjunto de servicios para el sistema operativo Microsoft Windows. Este servicio convierte a una PC en un servidor web para Internet o una intranet, es decir que en las computadoras que tienen este servicio instalado se pueden publicar páginas web tanto local como remotamente. Este servidor se instaló para permitir la creación del sitio web que utiliza la aplicación Dinámica Gerencial para sus actualizaciones.

5.1.6.5 Identificación de Activos en PILAR. A continuación se inicia la Identificación de los activos en la herramienta PILAR, para esta sección se siguen los siguientes pasos:

- Se pulsa en A. Análisis de Riesgos > A.1. Activos > A.1.1. Identificación".
- Se despliega una nueva Ventana (*Identificación de Activos*)
- Se Pulsa en Capas > Capas estándar
- Se Presenta 7 Capas:
    - Capa de Negocio
    - Servicios Internos
    - Equipamiento
    - Servicios Subcontratados
    - Instalaciones
    - Personal
    - Datos

Estas capas son mostradas en la figura 61.

Figura 61. Identificación de Activos

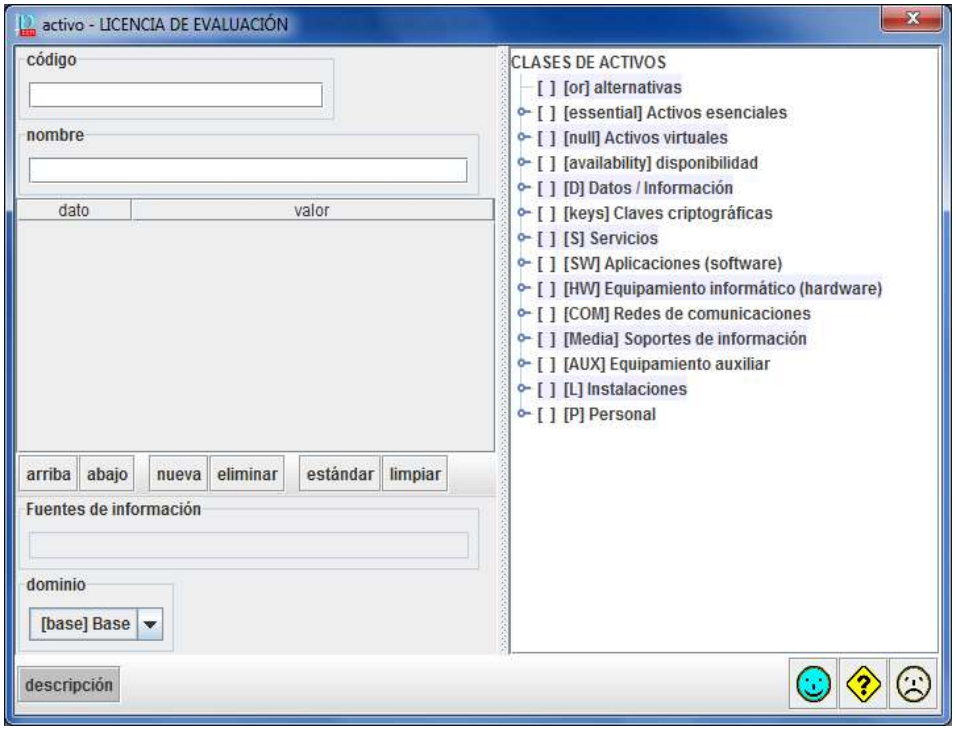


Fuente: Propia

- Los Activos se fueron agregando a cada una de las anteriores capas según correspondieron, siguiendo el proceso a continuación: Se selecciona la capa donde se quiere incluir un activo determinado, se pulsa Activos > Nuevo Activo > Nuevo. La Herramienta despliega la siguiente Ventana.

  Donde para cada Activo se debe ingresar un Código que lo identifique y un Nombre descriptivo del mismo, además de seleccionar en la parte derecha de la ventana la *Clase o Caracterización del Activo* (véase figura 61).

Figura 62. Identificación de un Activo



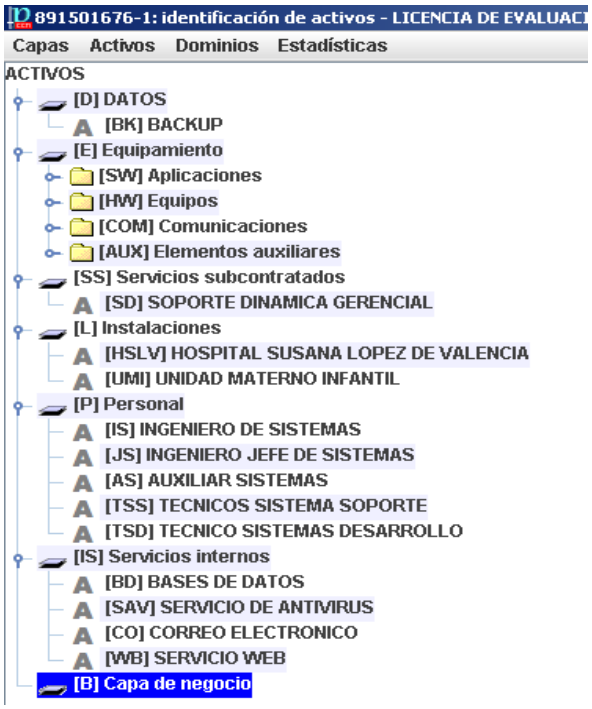
Fuente: Propia

Para cada activo se realizó el mismo procedimiento, efectuando el proceso solo para los activos que se consideraron más importantes o críticos debido a que la herramienta tiene un número limitado de los activos que se pueden registrar.

Entre los equipos que se identificaron se encuentran los Servicios ofrecidos por la Universidad del Cauca (de Negocio e Internos), aplicaciones que controlan dichos servicios, Equipos Hardware donde se albergan los servicios (Servidores), Equipos de Comunicaciones (para las conexiones de red), Instalaciones (Oficinas o lugares donde se almacenan dichos servidores) y el personal (los administradores u operarios encargados de los servicios y equipos).

A continuación en la Figura 63, se muestra la gráfica total de los activos identificados:

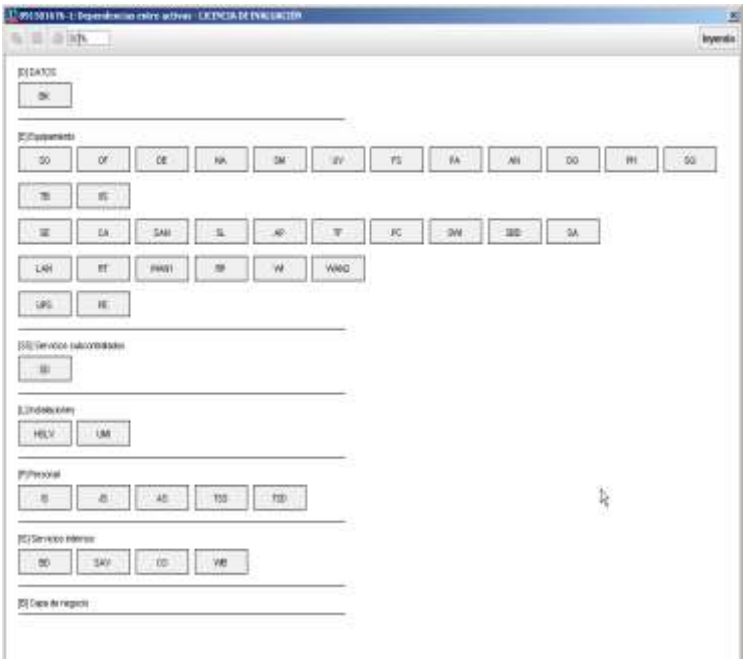
Figura 63. Activos Identificados



Fuente: Propia

El mapa de los activos identificados se muestra a continuación en la Figura 64

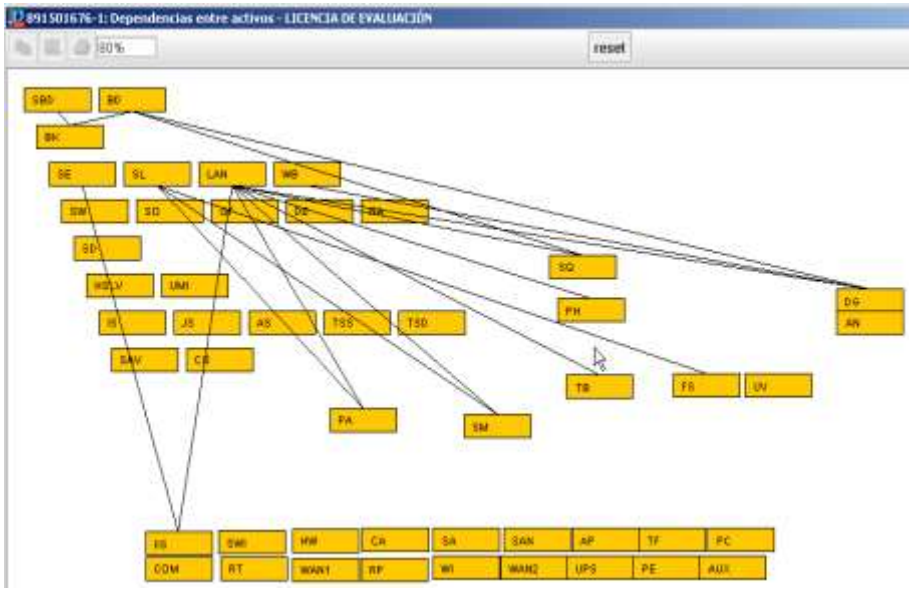
Figura 64. Mapa de Activos HSLV Popayán



Fuente: Propia

A continuación se muestra la interconexión de los activos identificados en el Hospital Susana López de Valencia Popayán – División de TIC (véase figura 65).

Figura 65. Diagrama de Interconexión y Dependencia de Activos



Fuente: Propia

5.1.6.6 Valoración de los Activos. Los activos son importantes para una organización y, por lo tanto, tienen un valor. En el caso de los activos de los sistemas de información, esta valoración se debe realizar según cada una de sus dimensiones. Una vez pulsada la opción de valoración, le aparecerá la pantalla de Gestión de Valoración de los Activos donde podrá definir el valor de los activos, según el impacto que tendría en la organización la merma en alguna de sus dimensiones.

Después de ingresar los activos y clasificarlos se realiza la ponderación mediante un análisis cualitativo de los mismos. Se realiza la ponderación en base a cinco aspectos fundamentales que son:

- **“[I]” (INTEGRIDAD DE LOS DATOS):** Que pondera el impacto que tendría en la organización el hecho de que la información que se maneja para prestar el servicio fuera incorrecta o incompleta.

- **“[C]” (CONFIDENCIALIDAD DE LOS DATOS):** Que pondera el impacto que tendría en la organización el hecho de que la información que se maneja para prestar el servicio fuera accedida por personas no autorizadas.

- **“[A]” (AUTENTICIDAD DE LOS DATOS):** Que pondera el impacto que tendría en la organización el hecho de que no se pueda saber a ciencia cierta quién ha accedido a la información que se maneja para prestar el servicio.

- **“[T]” (TRAZABILIDAD DE LOS DATOS):**Que pondera el impacto que tendría en la organización el hecho de que no se pueda saber qué se ha hecho con la información que se maneja para prestar el servicio o no se pudiera conocer quién hace qué y cuándo con el servicio.
- **“[D]” (DISPONIBILIDAD):** Que pondera el impacto que tendría en la organización el hecho de que se dejara de prestar el servicio.

De esta ponderación se obtuvo que los activos más críticos para la institución son:

En la categoría de aplicaciones SQL SERVER, DINAMICA GERENCIAL Y EL BACKUP ya que estos utilizan la información de historia clínica y financiera de la institución y estas últimas son el core del negocio de la institución. La siguiente Figura 4.65, muestra la ponderación obtenida para este grupo de activos.

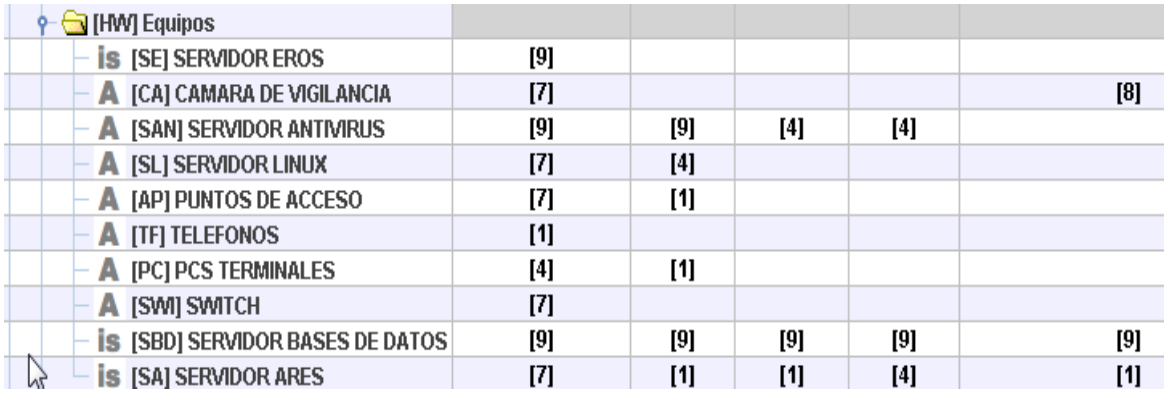
Figura 66. Ponderación de Activos Aplicaciones

[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 SERVIDOR 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: Propia

En la categoría de equipos los activos más críticos son servidor de base de datos ya que este contiene las aplicaciones de gestión de base de datos y el servidor de antivirus ya que es muy importante que evitar que se pueda propagar un virus por medio de la red y afectar el funcionamiento del sistema de información. Se puede observar también que el servidor eros tiene una alta ponderación en cuanto a disponibilidad ya que es el controlador de dominio y permite el ingreso a los terminales a los usuarios. La ponderación para este grupo de activos se muestra en la Figura 67.

Figura 67. Ponderación activos equipos

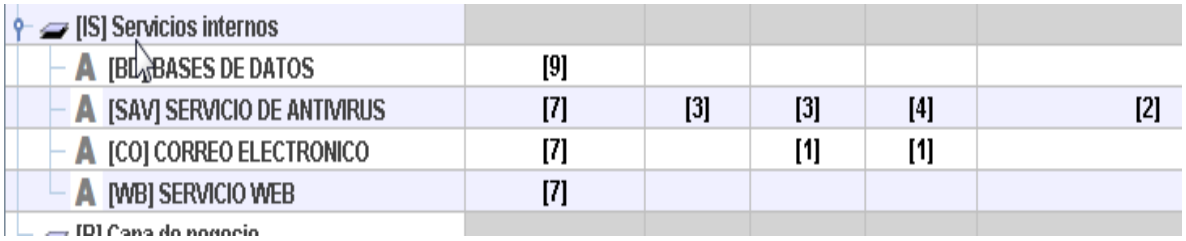


[HW] Equipos					
[SE] SERVIDOR EROS	[9]				
[CA] CAMARA DE VIGILANCIA	[7]				[8]
[SAN] SERVIDOR ANTIVIRUS	[9]	[9]	[4]	[4]	
[SL] SERVIDOR LINUX	[7]	[4]			
[AP] PUNTOS DE ACCESO	[7]	[1]			
[TF] TELEFONOS	[1]				
[PC] PCS TERMINALES	[4]	[1]			
[SWI] SWITCH	[7]				
[SBD] SERVIDOR BASES DE DATOS	[9]	[9]	[9]	[9]	[9]
[SA] SERVIDOR ARES	[7]	[1]	[1]	[4]	[1]

Fuente: Propia

En la categoría de servicios son los servicios de bases de datos y antivirus ya que de ellos depende la disponibilidad y estabilidad del sistema de información por las razones mencionadas en las categorías anteriores. La ponderación para este grupo de activos se muestra en la Figura 68.

Figura 68. Ponderación activos Servicios internos



[IS] Servicios internos					
[BD] BASES DE DATOS	[9]				
[SAV] SERVICIO DE ANTIVIRUS	[7]	[3]	[3]	[4]	[2]
[CO] CORREO ELECTRONICO	[7]		[1]	[1]	
[WB] SERVICIO WEB	[7]				
[P] Capa de negocio					

Fuente: Propia

Se debe tener en cuenta que las áreas de servidores cuentan con dos circuitos eléctricos de respaldo, ups y el hospital cuenta con plantas eléctricas de respaldo. Los servidores de bases de datos tienen una configuración en clúster para respaldar la caída de un servidor. De esta forma se determina que los activos

relacionados con la base de datos son los más críticos porque el acceso a esta debe tener una alta disponibilidad.

5.1.7 Identificación de Amenazas. Se realizó una evaluación de amenazas basado en la frecuencia de materialización de la amenaza para lo cual se define la frecuencia como:

Frecuencia: Cuando una amenaza se valora, permite definir la posibilidad de que ocurra en función de la cantidad de veces que se puede materializar dicha amenaza en un año (esta es la opción por defecto) y se utilizó la siguiente escala:

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

Como se puede observar en la Figura 69 el activo Backup es el que presenta mayores posibilidades de materialización de amenazas ya que el acceso no autorizado puede materializarse todos los días y tiene varias amenazas con frecuencia de 10 que significa que se pueden materializar en cada mes.

Figura 69. 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: Propia

Con respecto a los activos de aplicaciones la amenaza más frecuente es los errores de mantenimiento o actualización de software como se muestra en la Figura 70 debido a que se producirían cuando se realice mantenimiento programado sobre los equipos o por a una falla de las aplicaciones de los mismos.

Figura 70. Amenazas activos aplicaciones

[E] Equipamiento	
[SW] Aplicaciones	
[SO] SISTEMAS OPERATIVOS	
[I.5] Avería de origen físico o lógico	1
[E.1] Errores de los usuarios	1
[E.2] Errores del administrador del sistema / de la seguridad	1
[E.8] Difusión de software dañino	1
[E.9] Errores de [re-]encaminamiento	1
[E.10] Errores de secuencia	1
[E.15] Alteración de la información	1
[E.18] Destrucción de la información	1
[E.19] Fugas de información	1
[E.20] Vulnerabilidades de los programas (software)	1
[E.21] Errores de mantenimiento / actualización de programas (software)	10

Fuente: Propia

Con respecto a los activos de equipos la amenaza más frecuente es la caída del sistema por agotamiento de recursos como se muestra en la figura 71, ya que de estos los más esenciales como son los servidores y switches principales se encuentran en áreas con acceso solo al personal autorizado por lo cual la amenaza depende de los recursos instalados en los equipos.

Figura 71. Amenazas activos equipos

[HW] Equipos	
[SE] SERVIDOR EROS	
[N.1] Fuego	0,1
[N.2] Daños por agua	0,1
[N.*] Desastres naturales	0,1
[I.1] Fuego	0,5
[I.2] Daños por agua	0,5
[I.*] Desastres industriales	0,5
[I.3] Contaminación mecánica	0,1
[I.4] Contaminación electromagnética	1
[I.5] Avería de origen físico o lógico	1
[I.6] Corte del suministro eléctrico	1
[I.7] Condiciones inadecuadas de temperatura o humedad	1
[E.2] Errores del administrador del sistema / de la seguridad	1
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1
[E.24] Caída del sistema por agotamiento de recursos	10

Fuente: Propia

En los activos de comunicaciones la amenaza más frecuente es la denegación de servicio como se muestra en la Figura 72 ya que puede ocasionar la caída de servicios en diferentes partes de la empresa.

Figura 72. Amenazas activos comunicaciones

[COM] Comunicaciones	
[LAN] RED LOCAL	
[I.8] Fallo de servicios de comunicaciones	1
[E.2] Errores del administrador del sistema / de la seguridad	1
[E.24] Caída del sistema por agotamiento de recursos	1
[A.7] Uso no previsto	1
[A.24] Denegación de servicio	10
[A.26] Ataque destructivo	1

Fuente: Propia

Con respecto a los activos de servicios internos las amenazas más frecuentes son la caída del sistema por agotamiento de recursos como se muestra en la Figura 73 ya que depende de los recursos del equipo donde se encuentra instalado el

servicio y denegación de servicio porque está expuesto a ataques software como hardware.

Figura 73. Amenazas activos Servicios internos

[IS] Servicios internos	
[BD] BASES DE DATOS	
[E.1] Errores de los usuarios	1
[E.2] Errores del administrador del sistema / de la seguridad	1
[E.18] Destrucción de la información	1
[E.24] Caída del sistema por agotamiento de recursos	10
[A.18] Destrucción de la información	1
[A.24] Denegación de servicio	10

Fuente: Propia

5.1.8 Identificación de Vulnerabilidades. La identificación de vulnerabilidades se realizó mediante una visita a las instalaciones para realizar una inspección visual de los activos, entrevistas con el personal encargado del manejo de los recursos informáticos y la utilización de herramientas de ethical hacking y análisis de vulnerabilidades.

5.1.8.1 Entrevista al personal responsable de los recursos informáticos. Se crearon listas de verificación basadas en el Estándar EIA/TIA 568ª, TIA 942 para Centros de Datos y en el reglamento RETIE[5] las cuales se utilizaron para evaluar los activos en las áreas donde se ubican los activos principales para el funcionamiento del core del negocio

[5] Reglamento Técnico de Instalaciones Eléctricas (RETIE) expedido por el Ministerio de Minas y Energía

5.1.8.2 Lista de verificación sala de servidores. En la Tabla 4, 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 están acordes.		x
La función del “back-bone” es proveer interconexión entre los armarios de telecomunicaciones y las salas de equipos y entre las salas de equipos y las instalaciones de entrada.	x	
Cuenta con señales de seguridad donde al vierta peligro de corto circuito.		x
TIERRA CONFIABLES		
Los gabinetes y los protectores de voltaje están conectados a una barra de cobre de polo a tierra.	x	
ENERGIA ININTERRUMPIDA. 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 marcha.		x

Con este resultado se obtuvieron las siguientes conclusiones de la Sala de servidores en el Hospital Susana López de Valencia del listado de Verificación.

- En el área de alojamiento de los servidores del Hospital Susana López de Valencia, de acuerdo con la lista de verificación, se concluye que cumple en gran parte en la que se preguntaron por: La distribución para los equipos, sistemas de seguridad, iluminación, sistemas eléctricos, de red, equipos de respaldo, áreas de energía interrumpida, factores climáticos del recinto; cumplen con las especificaciones de acuerdo con la norma estándar EIA/TIA 568A, TIA 942 para Data Center o sala de servidores.
- En cuanto a las especificaciones con las que no cumplió la sala de servidores del Hospital Susana López de Valencia, de acuerdo con el listado de verificación son: sistemas de alarmas, sistemas de control de acceso a la sal de servidores, los cuales son de gran importancia para cualquier empresa el de saber quién ingreso al sitio y para que ingreso. Todo esto lo solicita la norma que se referencia anteriormente.

- Además cuentan con un sistema de energía interrumpida de los soporta mientras hay cortes del fluido eléctrico para que los equipos no fallen mientras hay el corte de energía.

5.1.8.3 Lista de Verificación Centro de Cableado (Área de Switches). En la Tabla 5 se muestran los resultados de la entrevista realizada al personal responsable del manejo del centro de cableado principal.

Tabla 5. Resultados entrevista personal 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	x	

cuarto.		
Equipos de respaldo para todos los elementos que interviene en el funcionamiento.	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.		
CABLEADO ELÉCTRICO		
El cable esta con la conformidad con los estándares de		x

seguridad contra incendios: UL VW-1,IEC 332-1.		
Estabilizadores de tensión.	x	
Transformadores de aislación.	x	
Los puntos eléctricos dentro de las áreas son los adecuados y están acordes a la norma.	x	
La función del “back-bone” es proveer interconexión entre los armarios de telecomunicaciones y las salas de equipos y entre las salas de equipos y las instalaciones de entrada.	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

Con este resultado se obtuvieron las siguientes conclusiones del Centro de cableado del Hospital Susana López de Valencia del listado de verificación.

- Los equipos se encuentran distribuidos en área donde su funcionamiento no va ser interrumpido por una eventualidad de catástrofe como inundaciones, o tormentas eléctricas que pueden caer directamente a ellos.
- Los equipos pueden ser intervenidos directamente por los técnicos de mantenimiento o por proveedores externos de servicios de acuerdo a la necesidad.
- Que la sala de Switches no cuenta con los sistemas mínimos de seguridad al ingresar.
- No cuenta con los equipos mínimos de refrigeración de la sala de Switches, para evitar que se sobrecalienten los equipos.
- Cuenta con la toma eléctrica necesaria y con respaldo de ups para que los dispositivos estén en funcionamiento cuando hay cortes de fluido eléctrico.

5.1.8.4 Lista Verificación Sistemas Eléctricos y UPS - Listado De Verificación. En la Tabla 6 se muestran los resultados de la entrevista realizada al personal responsable de los equipos eléctricos y de respaldo.

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 circuitos en todo el edificio.	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 además cuentan con los planos de cada una.	X	
Los tomas de la red regulada y normal están marcados con naranja para regulada y blanco para normal en todas las oficinas del edificio.	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	

Al Ingresar a la sala de UPS 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	
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	X	

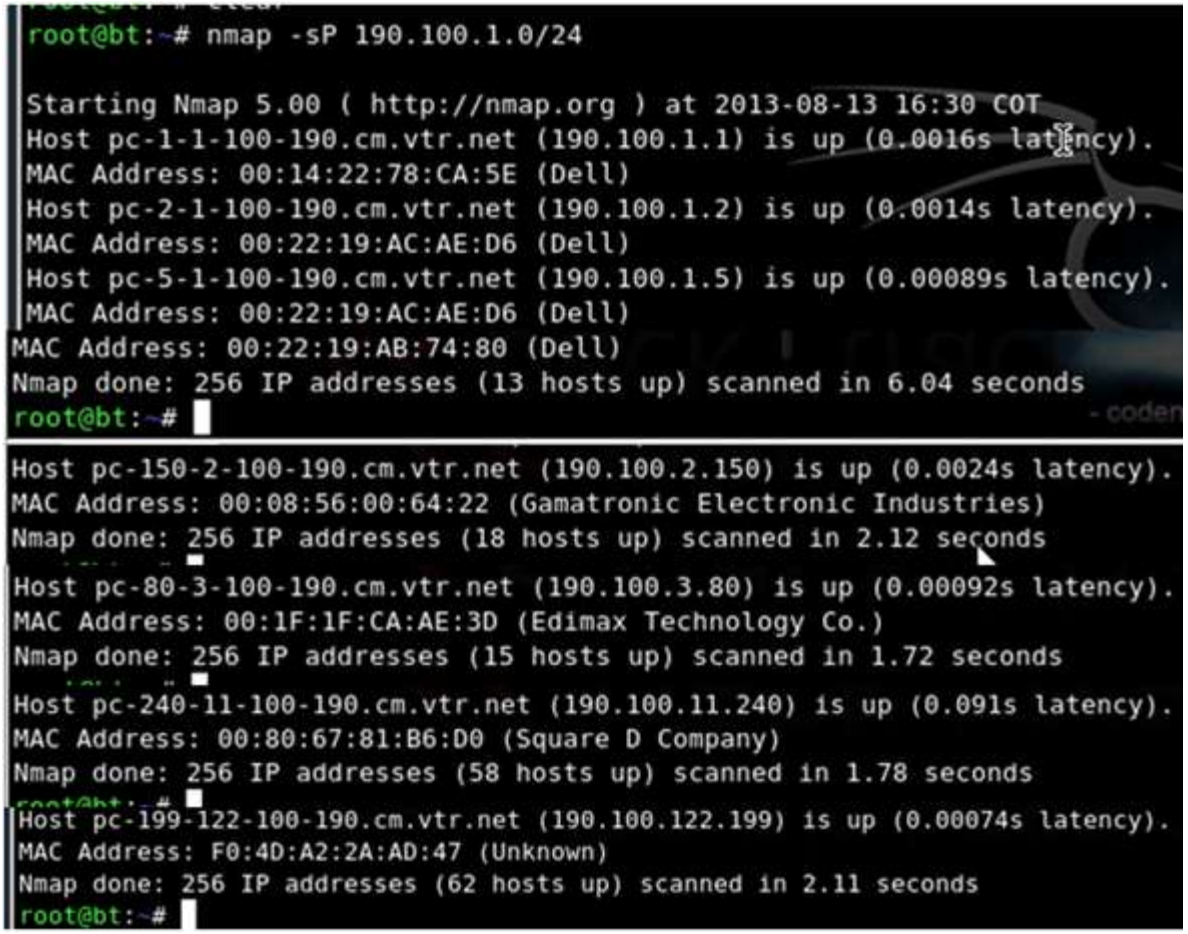
están acordes a la norma.		
Cuenta con señales de seguridad donde al vierta peligro de corto circuito	X	
TIERRA CONFIABLES		
Debe ser una barra de cobre, de 6 mm de espesor y 100 mm de ancho mínimos. El largo puede variar, de acuerdo a la cantidad de cables que deban conectarse a ella.	X	
Continuidad 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

Con estos resultados se obtuvieron las siguientes conclusiones del Sistema eléctrico del Hospital Susana López de Valencia del listado de verificación.

- El área de eléctrica cuenta con los dispositivos automáticos los cuales al generarse un corte en el fluido eléctrico y mantener los dispositivos del hospital en completo funcionamiento.
- Cuenta con unos trasformadores los cuales le regulan el fluido eléctrico que entra al hospital los cuales uno de ellos cuenta con refrigeración en aceite y el otro en refrigeración en seco.
- Cuenta con cada uno de los circuitos independientes y sus paneles de control tanto en la infraestructura como en medio impresos.
- Una de las subestaciones cuenta con un sistema de monitoreo vía conexión remota y esta hace parte del nuevo edificio de la UMI. En donde el administrador entra y monitorea cada uno de los circuitos de la UMI.
- La trasferencia se realiza en la subestación de la UMI en unos 8 segundos del pues que se halla hecho el corte eléctrico.
- Cuenta con un sistema de energía regulada y el otro normal cada uno de ellos están marcados por los tomas de colores: Naranja que es para la red regulada.
- Cuenta con un personal encargado de esta área que es una de las más importantes.

5.1.8.5 Pruebas de Análisis de Vulnerabilidades y Ethical Hacking. Mediante el uso del live cd de Bactrack se realizaron pruebas de vulnerabilidad, en la primera prueba se usó nmap para ver las direcciones IP en uso en los diferentes rangos de la red como se muestra en la Figura 74. Al realizar las pruebas se encuentra que es fácil encontrar el número de direcciones IP de la red.

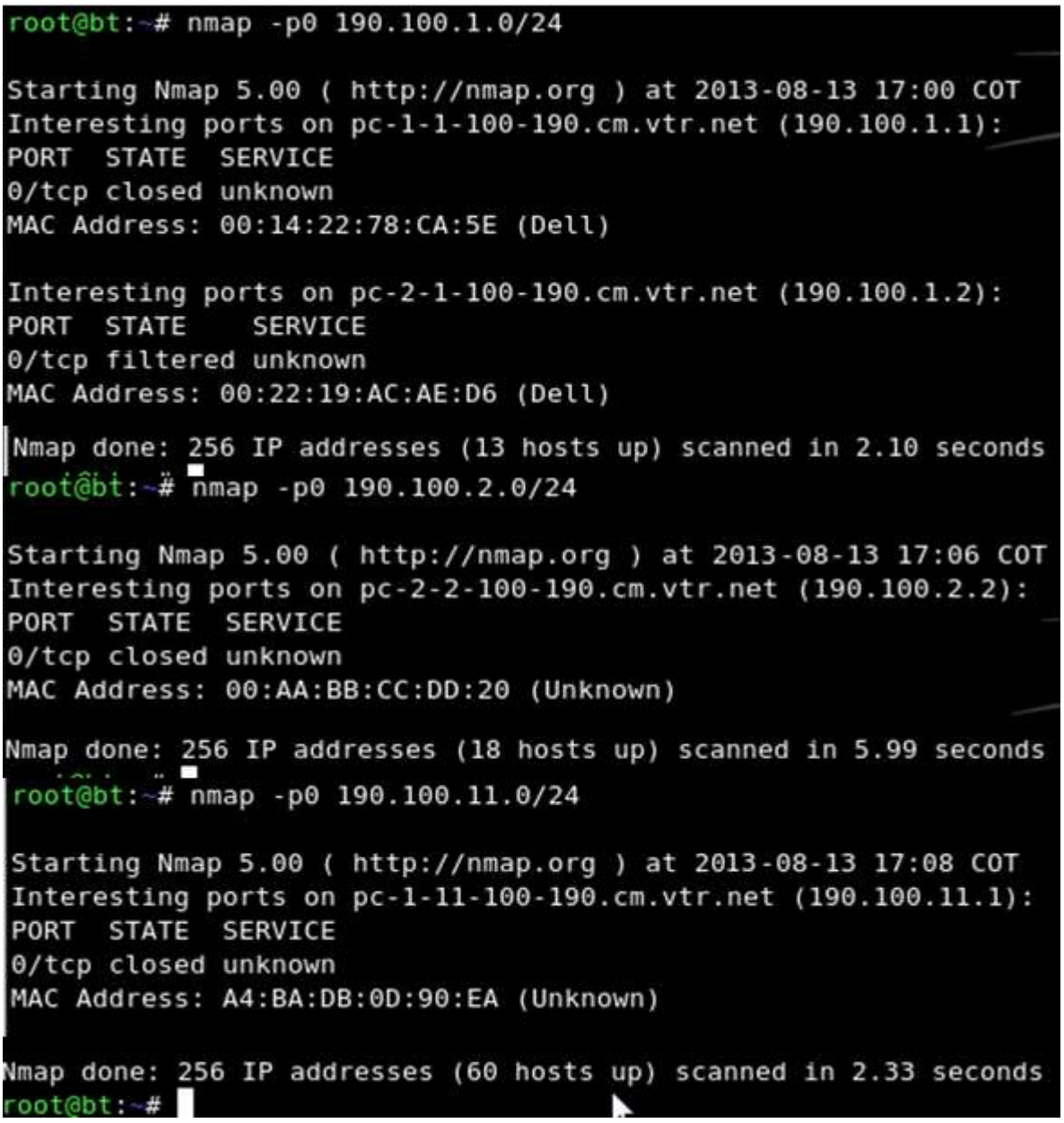
Figura 74. Escaneo IPS disponibles



Fuente: Propia

De la misma forma se realiza un escaneo de las direcciones físicas de la red como se muestra en la Figura 75.

Figura 75. Prueba de escaneo direcciones físicas

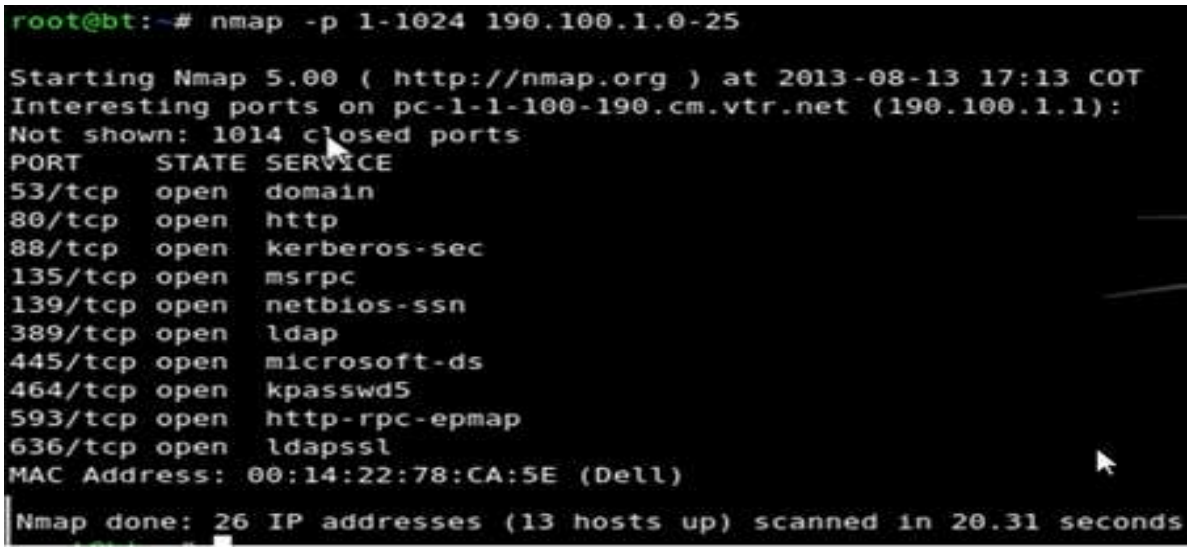


Fuente: Propia

Se realizó un escaneo de los puertos en los cuatro servidores y se encuentra que existen muchos puertos abiertos que no tienen uso definido para lo cual se

recomienda realizar un análisis de tráfico y cerrar los puertos no necesarios (véase figura 76)

Figura 76. Prueba de escaneos de puertos en los servidores



Fuente: Propia

Se realizó la prueba para detectar el sistema operativo como se muestra en la Figura 77. De este escaneo se encontró que hay que cambiar los banners para evitar dar información sobre el sistema operativo de los servidores

Figura 77. Escaneo detección sistema operativo

Fuente: Propia

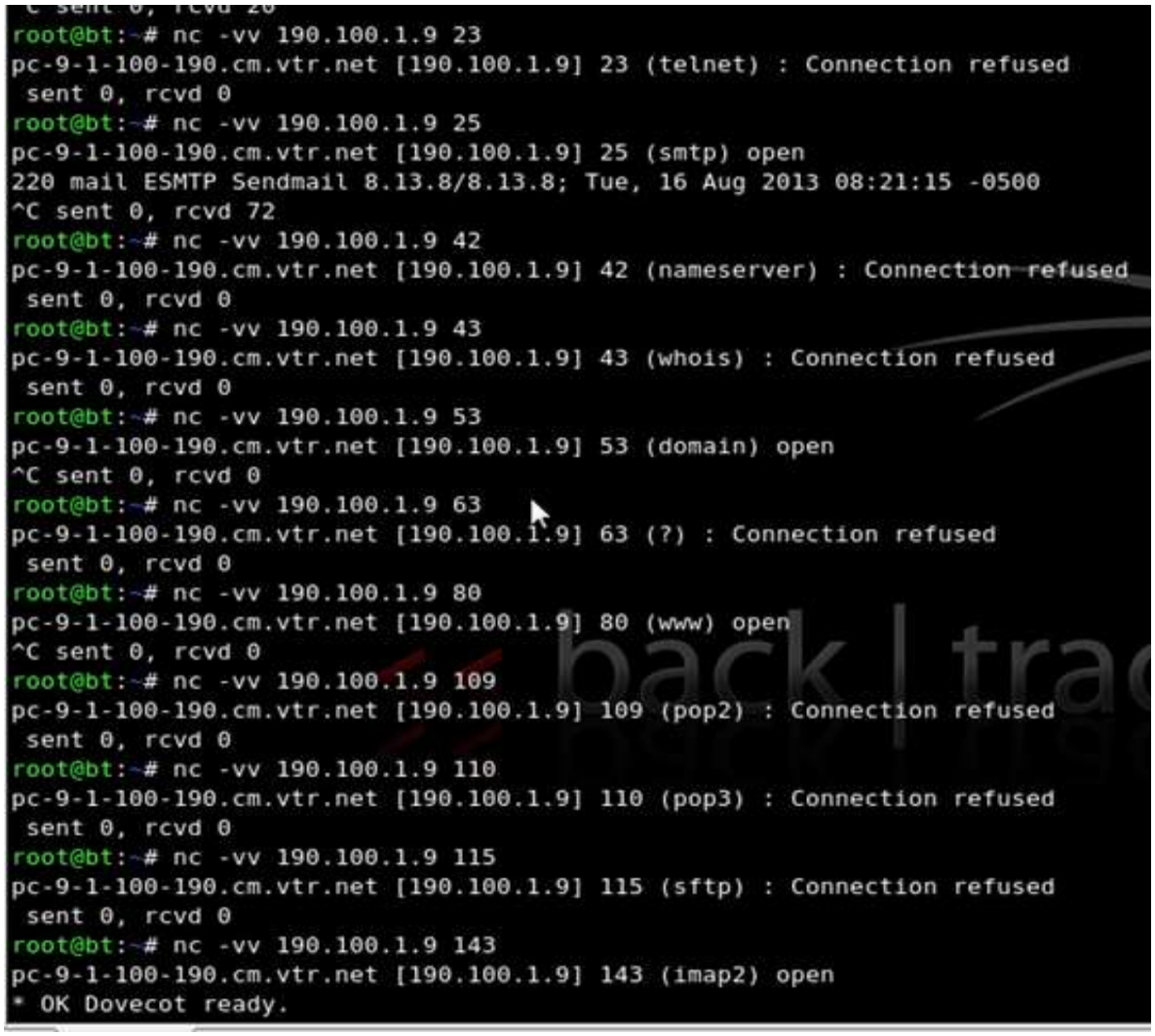
Se utilizó xprobe para determinar el SO y se comprobó que se encuentra información sobre el sistema operativo de los servidores como lo muestra la Figura 78.

Figura 78. Pruebas detección SO con Xprobe

Fuente: Propia

Con la herramienta netcat también muestra los puertos y servicios configurados en los servidores como sendmail, dominio, web lo cual se puede observar en la Figura 79.

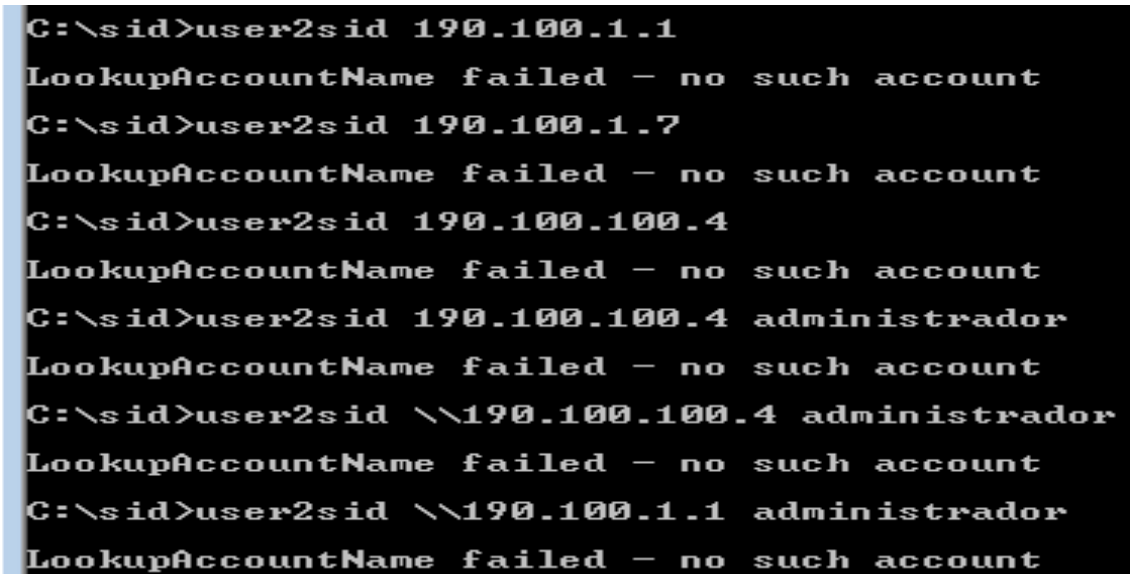
Figura 79. Análisis de puertos con netcat



Fuente: Propia

Se utilizó user2sid para hallar usuarios y no dio resultados positivos para hallar la cuenta de usuarios como se muestra en la Figura 80.

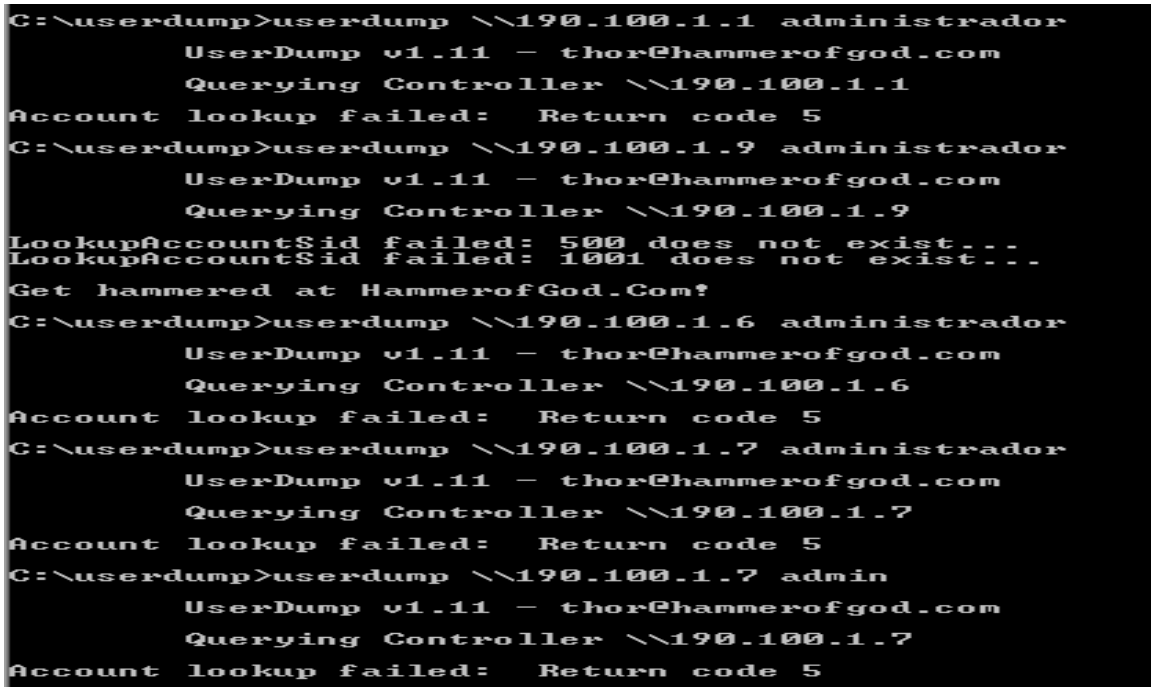
Figura 80. Uso de user2sid



Fuente: Propia

El escaneo para encontrar los usuarios presentes en la red con userdump no entrego resultados lo cual indica que se tiene un cierto nivel de protección como se muestra en la Figura 81.

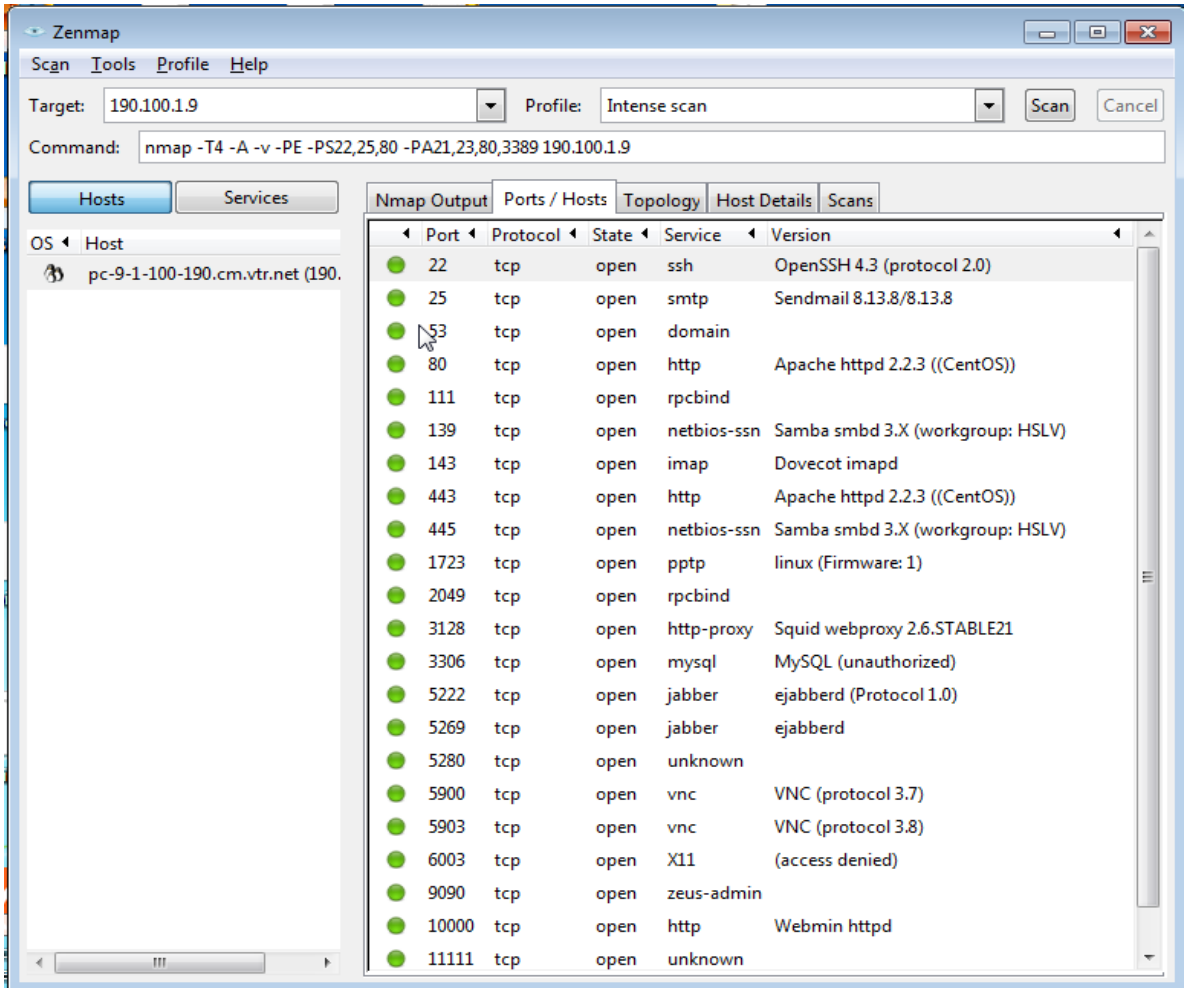
Figura 81. Uso de userdump



Fuente: Propia

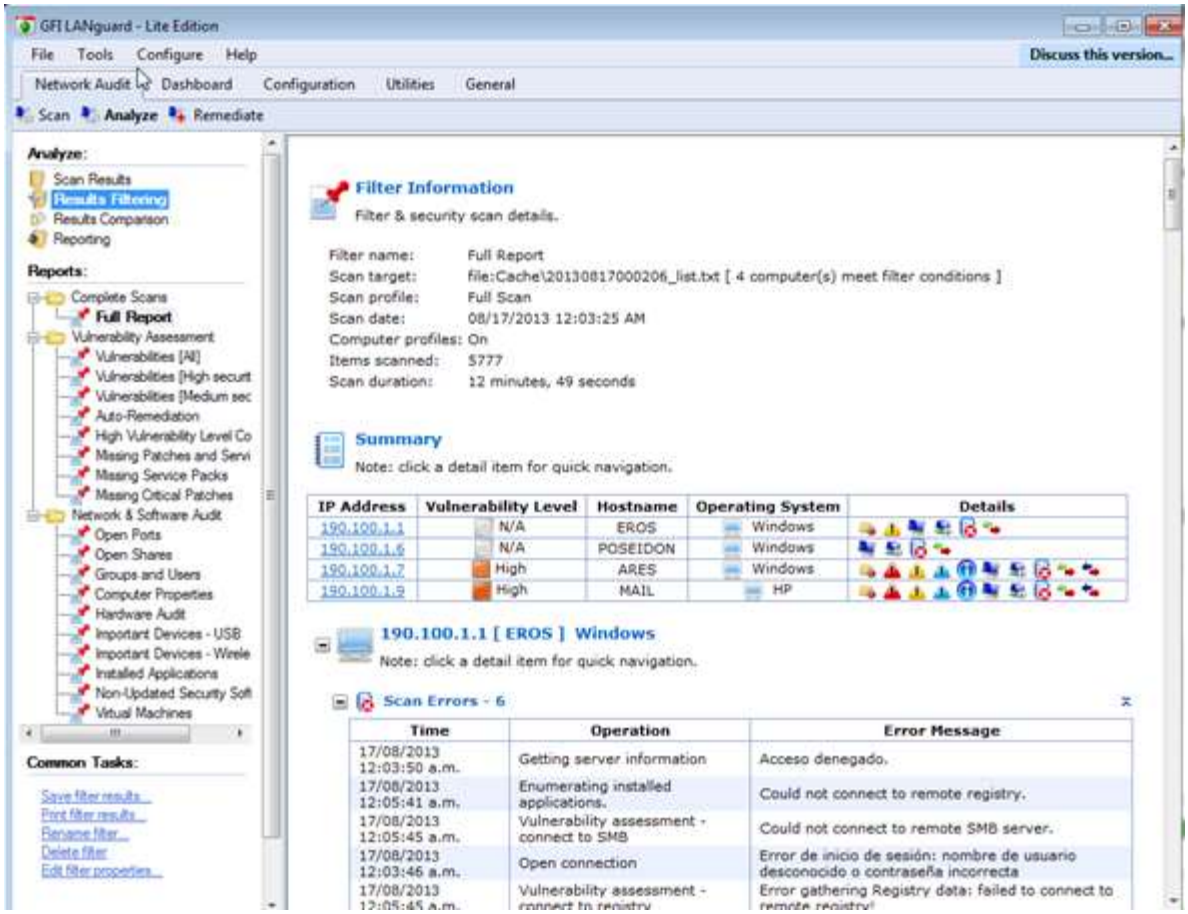
Por último se utilizaron las herramientas de Nmap, Gfilanguard y Nessus para encontrar vulnerabilidades cuyas evidencias se muestran en las figuras 82 a 85. Estas pruebas confirmaron los resultados obtenidos mediante las otras herramientas en la cual se reportan puertos abiertos, falta de actualizaciones en los sistemas operativos, banners sin editar para no permitir identificación. De estas herramientas se generaron reportes los cuales se pueden consultar en los anexos.

Figura 82. Escaneo de vulnerabilidades con nmap



Fuente: Propia

Figura 83. Escaneo de vulnerabilidades con Gflanguard



Fuente: Propia

Figura 84. Escaneo de vulnerabilidades con Nessus

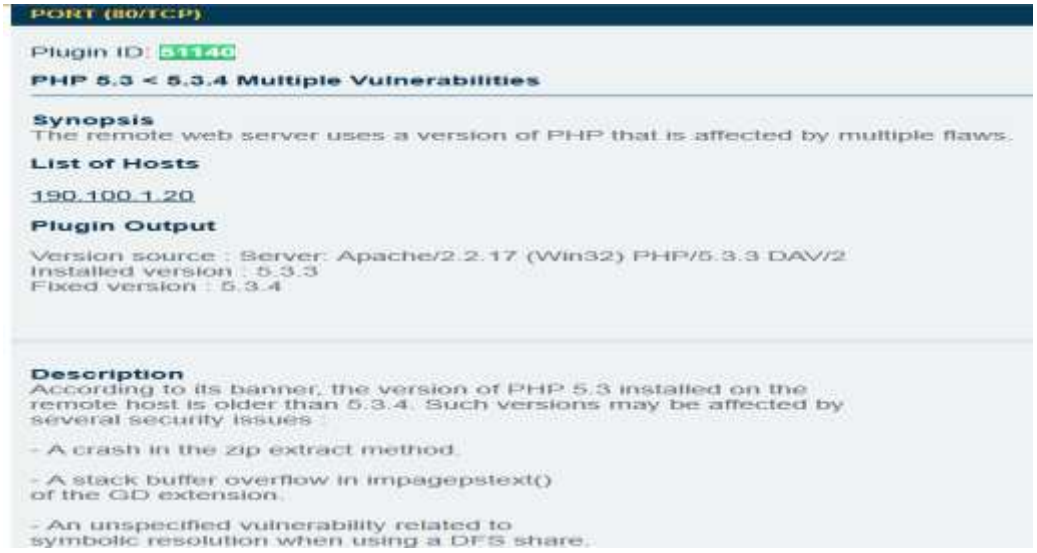
List of Plugin IDs

The following plugin IDs have problems associated with them. Select the ID to review more detail.

PLUGIN IDs	# OF ISSUES	PLUGIN NAME	SEVERITY
53514	3	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	High Severity problem(s) found
52717	1	PHP 5.3 < 5.3.6 Multiple Vulnerabilities	High Severity problem(s) found
51140	1	PHP 5.3 < 5.3.4 Multiple Vulnerabilities	High Severity problem(s) found
48244	1	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	High Severity problem(s) found
47709	1	Microsoft Windows 2000 Unsupported Installation Detection	High Severity problem(s) found
45004	1	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	High Severity problem(s) found
42052	1	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	High Severity problem(s) found
41028	3	SNMP Agent Default Community Name (public)	High Severity problem(s) found
41014	1	PHP < 5.2.11 Multiple Vulnerabilities	High Severity problem(s) found
35362	1	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	High Severity problem(s) found
35043	1	PHP 5 < 5.2.7 Multiple Vulnerabilities	High Severity problem(s) found
34460	2	Obsolete Web Server Detection	High Severity problem(s) found
32123	1	PHP < 5.2.6 Multiple Vulnerabilities	High Severity problem(s) found

Fuente: Propia

Figura 85. Reporte de vulnerabilidades Nessus



PORT (80/TCP)

Plugin ID: 51140

PHP 5.3 < 5.3.4 Multiple Vulnerabilities

Synopsis
The remote web server uses a version of PHP that is affected by multiple flaws.

List of Hosts

190.100.1.20

Plugin Output

Version source : Server: Apache/2.2.17 (Win32) PHP/5.3.3 DAV/2
Installed version : 5.3.3
Fixed version : 5.3.4

Description
According to its banner, the version of PHP 5.3 installed on the remote host is older than 5.3.4. Such versions may be affected by several security issues :

- A crash in the zip extract method.

- A stack buffer overflow in impagepstext() of the GD extension.

- An unspecified vulnerability related to symbolic resolution when using a DFS share.

Fuente: Propia

5.1.8.6 Análisis de vulnerabilidades Herramientas Ethical Hacking. Después de identificar los activos críticos y realizar las pruebas de vulnerabilidad sobre ellos se aplicó Cobit para identificar los controles y observaciones que son necesarias implementar en la institución.

Del análisis de vulnerabilidades hecho en Nessus, Inspección visual y Cobit se clasificaron las amenazas, riesgos y vulnerabilidades más importantes y la solución recomendada. Estos datos están consignados en la tabla 7.

Tabla 7. Resumen de Vulnerabilidades, amenazas y riesgos

Amenaza	Se observa que al tener acceso a la sala de servidores no hay una puerta de madera y no cuenta con un sistema retardante contra el juego en caso de incendio…además no cuenta con un sistema de acceso biométrico	Se recomienda cambiar la puerta por una que tenga retardante contra el juego, implementar el sistema de acceso biométrico para evitar el acceso sin autorización.
Riesgo	En la sala de servidores se encuentra un ventanal con vidrio que no es de seguridad el cual podría ocasionar un incidente en la sala de servidores por una persona mal intencionado en contra de la organización.	Se recomienda en la parte informática correspondiente a la sala de servidores instalar una ventana con vidrio capaz de soportar gran presión, o sellarlo con muro para evitar el riesgo.
Riesgo	Se encontró en la sala de servidores, materiales como: cartón, madera, cortinas en	Se recomienda evacuar de esta instalación este tipo de material ya que sería un

	tela…las cuales al generarse un corto o un incidente provocado por personas mal intencionadas puede ocasionar un incendio.	riesgo para la sala de servidores…y con esto evitar pérdidas materiales de información y recursos.
Riesgo	Se encontró en sala de servidores un servidor que está soportando dos modem además el cableado de uno de ellos no está en la ubicación adecuada y puede producir un incidente al ser enredado ya sea con un elemento o una persona.	Se recomienda que estos dos dispositivos sean ubicados en una base correcta y no encima del servidor, el cable no puede estar tirado en el piso.
Riesgo	Se encontró un servidor ubicado en una mesa de madera el cual no es recomendable ya que se puede iniciar un incendio por un corto.	Se recomienda una base o soporte de metal con buena resistencia.
Riesgo	Se encontró una silla de plástico (Rimax) lo cual no es de conveniencia para la sala de servidores porque este material es un buen conductor en caso de provocación de incendio.	Se recomienda retirar esta silla o en el caso de ser muy necesaria cambiarla por una metálica.
Riesgo	Se encontró que en el área no existen los dispositivos detectores de calor, de humedad ni contraincendios.	Se recomienda la adquisición y instalación de estos dispositivos que son de vital importancia para el área de

		servidores.
vulnerabilidad	Se encontró que los servidores no cuentan con etiquetas que los identifiquen de acuerdo a sus aplicaciones y servicio que prestan cada uno.	Se recomienda etiquetar los servidores de acuerdo a sus aplicaciones.
Riesgo	Se encontró que en la sala de swiches hay una ventana de vidrio sin la resistencia adecuada lo cual puede ser violado el ingreso a la instalación.	Se recomienda cambiar la resistencia del vidrio o sellarla en material para mayor seguridad.
Riesgo	Se encontró que no cuenta con un sistema de cámara de video que vigile el ingreso de personal a la sala de swiches.	Se recomienda implantar un sistema de cámara de video que registre el ingreso a la sala de swiches.
Riesgo	Se encuentra que en la sala de swiches no hay un sistema regulación de temperatura en calor aire acondicionado y humedad.	Se recomienda implementar el sistema de manejo e temperaturas.
vulnerabilidad	Se encontró en las dos áreas swiches y servidores que no hay un cumplimiento con el aseo periódico o continuo.	Se recomienda determinar una rutina de aseo para cada una de las salas y responsabilizar a una persona en particular para esta tarea.
vulnerabili	Se encontró en el área de Informática que hay determinado	Se recomienda mejorar la presentación de la sala,

dad	desorden en el cableado, enchufes mal ubicados con poca organización.	organizar el cableado y cambiar la ubicación de los enchufes de forma que no estorben ni provoquen tropiezos con las personas.
Riesgo	En la parte existencial se observa que los usuarios de los equipos toman bebidas y comen al estar interactuando con los dispositivos de trabajo.	Se recomienda que el personal tenga conocimiento de la importancia de evitar derrame de bebidas sobre equipos de trabajo.
Riesgo	Se encontró que no hay configurado un sistema de protector de pantallas en un lapso de tiempo de inactividad del servicio del core del negocio.	Se recomienda implementar esta configuración para proteger las actividades o ingreso, perdida de información de personas mal intencionado.
vulnerabilidad	Se encontró que los equipos en la áreas de enfermería primordialmente en hospitalización se hallan mal ubicados y el cableado de estos se puede enredar y causar des conectividad y posible incidente con el personal.	Se recomienda mejorar la ubicación de los equipos y evitar inconvenientes.
riesgo	Se encontró una fuga en el tanque de combustible de la planta eléctrica vieja el cual presenta una fuga de	Se recomienda cuanto antes hacer el cambio de planta para evitar un incidente que pueda causar daños

	combustible.	considerables.
Riesgo	Se encontró en la parte superior de la subestación de la UMI 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 el edificio.	Se recomienda la desviación a tiempo de estos viaductos de agua. Se recomienda una ubicación más lejana a la subestación para prevenir cualquier desastre.
Riesgo	No cuenta con un procedimiento o política de control que permita llevar 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	Se encuentra que no se tiene un procedimiento o una política para llevar el control de las copias de seguridad de la información.	Se recomienda la creación de una política para cumplir con el objetivo de este control.
Riesgo	Se verifica que el hospital no tiene 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 verifica que no se tiene ningún control en la utilización de los recursos computacionales.	Se recomienda la creación de una política para cumplir con el objetivo de este control.

Riesgo	En el requerimiento de soporte no se encuentra un contrato que obligue el proveedor a brindar soporte a dinámica gerencial.	Se recomienda elaborar un contrato que responsabilice al proveedor a cumplir con este requerimiento para dinámica gerencial.
Riesgo	Se encontró que el firewall presenta un contrato de soporte con término de un año.	Se recomienda evaluar este término y pedir la prórroga del mismo al ente proveedor.
Vulnerabilidad	Se encuentra en su estado actual 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.	Se recomienda un procedimiento formal para llevar a cabo 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 por página web.	Se recomienda la elaboración del documento formal que responsabilice al proveedor de este procedimiento
Vulnerabilidad	Se encontró que para un nuevo empleado o encargado de este procedimiento se hace una capacitación personal sobre el software del soporte de peticiones como entrar a la página para realizar la solicitud.	Se recomienda un procedimiento formal con el fin de que el encargado conozca los alcances y beneficios de este procedimiento y el valor de importancia para los activos

		que lo requieren.
Riesgo	se encuentra que no existe 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	Que 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 le recomienda la creación de un formato en el cual se enmarque cómo será la los pasos a tener en cuenta antes de realizar tal actividades, los inconvenientes que se tuvieron. Y cuales serían las posibles alternativas a seguir y quien las realizo
Vulnerabilidad	Los equipos que se adquieren nuevos en muchas ocasiones no se les realizan las pruebas pertinentes por el personal encargado sino que se instalan	Se recomienda implementar un formato en donde se evanecían los cabios realizados de los equipos

	en el ambiente directamente.	
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 le 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	No hay un plano completo de la red de datos en el hospital Se conoce la red de datos empíricamente la distribución de la red	Se le recomienda al área de informática generar unos formatos y los procedimientos que se deben tener en cuenta antes de realizar alguna actividad de estas. Solo para contar con las evidencias de los procedimientos realizados para posteriores cambios.
	Si es se hace necesario la activación del servicio de Windows NT por el core del negocio ya que cuenta con un servidor web. Todo esto no cuenta con los formatos de solicitud para la activación de estos servicios	Se le recomienda al área de informática generar unos formatos y los procedimientos que se deben tener en cuenta antes de realizar alguna actividad de estas. Solo para contar con las evidencias de los procedimientos realizados para posteriores cambios.

Con la identificación de las vulnerabilidades, riesgos y amenazas más importantes se construyeron las políticas y procedimientos de seguridad las cuales se encuentran en la carpeta de anexos.

5.1.8.7 Análisis de Vulnerabilidades. Resultados de las pruebas de ethical hacking, entrevistas y desarrollo de encuestas

Tabla 8 Resultado Análisis de Vulnerabilidades

Item	# Activos Vulnerables	Nombre Plugin	Gravedad (Alta, Media, Baja)	Vulnerabilidad	Descripción	SOLUCIÓN
41028	3	Por defecto del agente SNMP de nombre de comunidad (público)	Alta gravedad (s) que se encuentran	El nombre de comunidad SNMP del servidor remoto se puede adivinar. Dispositivo: 190.100.1.20	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.

Item	# Activos Vulnerables	Nombre Plugin	Gravedad (Alta, Media, Baja)	Vulnerabilidad	Descripción	SOLUCIÓN
53514	3	MS11-030: Una vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código (2509553) (ver a distancia)	Alta gravedad (s) que se encuentran	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: 190.100.1.11 190.100.1.10 190.100.1.1	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 explotado 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

Item	# Activos Vulnerables	Nombre Plugin	Gravedad (Alta, Media, Baja)	Vulnerabilidad	Descripción	SOLUCIÓN
34460	2	Web de detección de servidores obsoletos	Alta gravedad (s) que se encuentran	El servidor web remoto es obsoleto. Dispositivos: 190.100.1.7	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.

En la Tabla 8 se encuentra apartes de los registros del análisis de vulnerabilidades (documento completo ver Anexo B), donde es posible determinar:

- **ITEM:** Numero de resultado arrojado por la herramienta en el análisis.
- **# EQUIPOS QUE VULNERA:** Numero de equipos encontrados y que son factibles de amenaza.
- **NOMBRE PLUGIN:** Nombre del plugin utilizado para realizar los test.

- **GRAVEDAD:** Nivel de escala para determinar la gravedad de la amenaza, la cual puede oscilar entre los siguientes valores: Alta, Media y Baja.
- **VULNERABILIDAD:** Como su nombre lo indica, nos presenta la documentación de la vulnerabilidad encontrada.
- **DESCRIPCIÓN:** Resumen de la vulnerabilidad encontrada.
- **SOLUCIÓN:** Posibles soluciones a la vulnerabilidad encontrada.

5.1.8.8 Análisis de Vulnerabilidades A partir de Controles COBIT

Tabla 9. Análisis de Vulnerabilidades A partir de Controles COBIT

Objetivo de Control	Actividad de Control	Prioridad de la Actividad de Control	Estado Actual de Actividad de Control	Prueba de control	Mejoras a la Actividad de Control	Propietario del Control	Frecuencia	Detectivo/ Prevent.	Manual / Auto.	Quien Verifica	Como se Evidencia	Observación
IR-20-1-b	Las excepciones al proceso normal están en el sistema, revisado por la dirección, y se resolvieron rápidamente. Cobertura: Parcial	Media	Se cuenta con un aplicativo de solicitud soportes.	Se verifica que está en producción.	Generar estadísticas de la información almacenada en las bases de datos del aplicativo.	Área de informática	D	D	A	Robert	Con los registros de la bases de datos del aplicativo	Se recomienda generar estadísticas de la información almacenada en las bases de datos del aplicativo.

Objetivo de Control	Actividad de Control	Prioridad de la Actividad de Control	Estado Actual de Actividad de Control	Prueba de control	Mejoras a la Actividad de Control	Propietario del Control	Frecuencia	Detectivo/ Prevent.	Manual / Auto.	Quien Verifica	Como se Evidencia	Observación
IR-20-3-uno	Se comprueba la legibilidad de los datos guardados en las copias de seguridad, mediante la restauración y comprobación periódica de estas. Cobertura: Parcial	Alta	Se realizan copias de la base de datos, y se restauran cuando se requiere.	No se lleva control para esta actividad.	La creación de una política de Backus	Cristian González	M	P	M	Robert		Se recomienda la creación de una política para cumplir con el objetivo de este control.

Objetivo de Control	Actividad de Control	Priori dad de la Activi dad de Control	Estado Actual de Actividad de Control	Prueba de control	Mejoras a la Actividad de Control	Propieta rio del Control	Frecuencia	Detectivo/ Prevent.	Manual / Auto.	Quien Verifica	Como se Eviden cia	Observación
IR-40-5-uno	Todo el software y los datos se omprueban en busca de virus antes de ser cargados en el sistema de la entidad.	Media	Se tiene antivirus con sus funciones de detección habilitadas en los terminales y se establece que los usuarios que tengan acceso a puertos usb deben llevar las memorias al área de informática para su revisión antes de conectarlas	No se controla todo el software porque puede provenir de diferentes medios como correo, cds, dvds, memorias	Capacitar al personal en manejo de antivirus para minimizar el riesgo de infección	Ing Cesar Sierra Técnico Mario Martínez	T	D	A/ M	Robert Camacho		Definir una política para el uso de antivirus y herramientas de detección de malware y programas similares

Objetivo de Control	Actividad de Control	Priori dad de la Activi dad de Control	Estado Actual de Actividad de Control	Prueba de control	Mejoras a la Actividad de Control	Propieta rio del Control	Frecuencia	Detectivo/ Prevent.	Manual / Auto.	Quien Verifica	Como se Eviden cia	Observación
	Cobertura : Parcial		a los equipos. Se tiene un registro con los equipos que más infecciones se detectan. Se realiza una limpieza profunda de virus en los equipos cuando se le realiza el mantenimien to programado									

En la Tabla 9 se encuentra apartes de los registros del análisis de vulnerabilidades aplicando COBIT (documento completo ver Anexo C), donde es posible determinar:

- **Objetivo de Control:** Código del objetivo analizado.
- **Actividad de Control:** Aquí se relaciona las actividades de control que se han realizado y la cobertura del mismo
- **Prioridad de la Actividad de Control:** Aquí se relaciona la prioridad del control, la escala de medición es cualitativa y va desde el valor bajo, pasando por el medio hasta el alto
- **Estado Actual de la Actividad de Control:** Describe la situación actual de la actividad analizada.
- **Prueba de control:** Describe la actividad que se realiza para verificar su estado.
- **Mejoras a la Actividad de Control:** Propuesta a realizar a la actividad analizada.
- **Propietario del Control:** Usuario a cargo del control.
- **Frecuencia:** Frecuencia en términos de tiempo para la posible aplicación del control el cual se establece en:
    - O: Ocasional
    - D: Diario
    - S: Semanal
    - M: Mensual
    - T: Trimestral

    - A: Anual

- **Detectivo/preventivo:** Indica si el control se aplica de forma preventiva antes que suceda un improvisto, o detectiva cuando se desea buscar alguna anomalía.
- **Manual/Automático:** Indica si la aplicación se realiza automática o manual por un usuario.
- **Quien Verifica:** Indica que usuario realiza la verificación de la aplicación del control.
- **Cómo se evidencia:** mediante documentos o registros detallados de la aplicación del control
- **Observaciones:** Anotaciones adicionales a los controles realizados, según sea el caso.

5.1.8.9 Impacto. El análisis de impacto indica que las consecuencias de las materializaciones de las amenazas son críticas para los activos ver figura 86 SQL SERVER, DINAMICA GERENCIAL Y EL BACKUP

Figura 86. Análisis de Impacto

Fuente: Propia

5.1.8.10 Riesgos. Los riesgos se muestran con la siguiente escala de colores según su valor:

{5} o más: Crítico (Rojo)

{4}: Muy alto (Rosado)

{3}: Alto (Amarillo)

{2}: Medio (Azul)

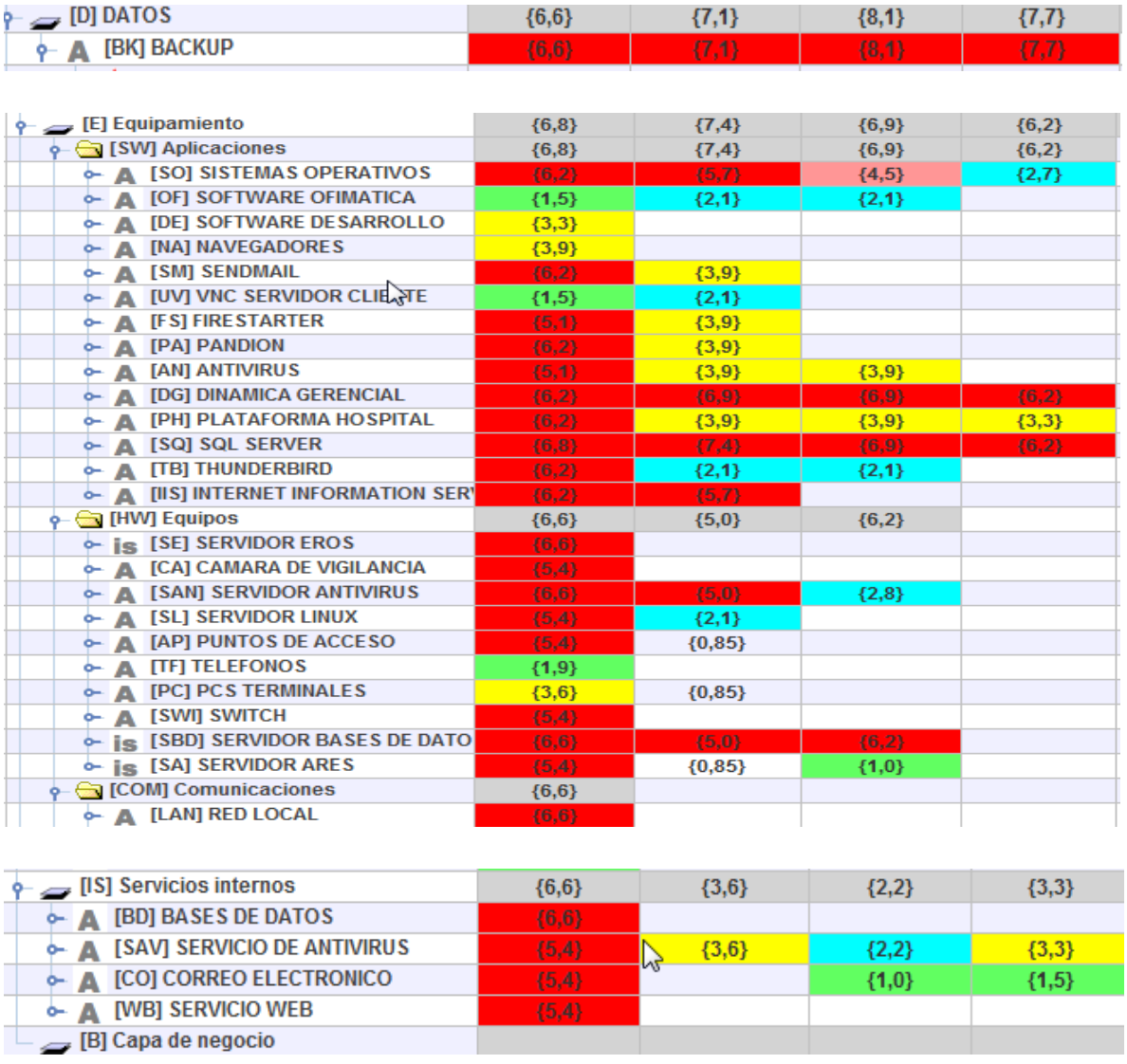
{1}: Bajo (Verde)

{0}: Despreciable

{OFF}: Este activo, o uno del que depende, está marcado como “/indisponible”.

En la Figura 87, se puede observar que los riesgos son más críticos para los activos de backup, los activos relacionados con la base de datos y el software de Dinámica Gerencial.

Figura 87. Identificación de Activos



[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: Propia

En la tabla de riesgo acumulado se muestra la valoración de los activos que presentan el mayor riesgo. Para esto se tienen en cuenta los siguientes parámetros:

- **ACTIVO:** Como su nombre lo indica, es el activo a ser valorado.
- **AMENAZA:** Las amenazas disponibles vienen definidas en la Biblioteca que esté utilizando. Para facilitar el trabajo con las amenazas, se han agrupado según su origen. Cada grupo de amenazas tiene un código asociado, y cada amenaza tiene un código asociado consistente en el identificador del grupo de amenazas y un número de amenaza. Los códigos asociados se muestran entre corchetes (24).
- **DIMENSION:** Muestra las dimensiones que haya definido previamente. Las más para el presente ejercicio se utilizó las más habituales:
    - [D]: Muestra la valoración de la Disponibilidad.
    - [I]: Muestra la valoración de la Integridad.
    - [C]: Muestra la valoración de la Confidencialidad.
    - [A]: Autenticidad de los usuarios y la información
    - [T]: Trazabilidad del servicio y de los datos

- **V (Valor):** El valor del activo. Aparece en la captura de pantalla con el indicador.
- **VA (Valor acumulado):** El valor acumulado del activo (la suma del valor del propio activo más el valor de los activos que dependen de él.

- **D (Degradación):** La degradación que le provoca la amenaza al activo.
- **I (Impacto):** El impacto que le provoca la materialización de la amenaza al activo.
- **Frecuencia:** La estimación con la que se puede materializar una amenaza.

La Tabla 10 de riesgo acumulado comprueba que los activos más críticos son los que tienen alguna relación directa con la base de datos o los aplicativos para gestionarlos.

Tabla 10. 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}

Tabla 10. (Continuación)

Activo	Amenaza	Dimensión	V	VA	D	I	F	Riesgo
[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 ANTIVIRUS	[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: Propia

Para la obtención de los datos se utilizó la herramienta pilar como se mencionó anteriormente, en el anexo D, se puede ver una descripción detallada y paso a paso de la forma que se obtuvo los resultados

5.2 HACER – IMPLEMENTAR Y UTILIZAR EL SGSI

5.2.1 Salvaguardas y Controles. Para reducir el riesgo se necesita la mejora de Salvaguardas existentes o la incorporación de otras nuevas. Se define la función o servicio de salvaguarda como la acción que reduce el riesgo; el mecanismo de salvaguarda como dispositivo, físico o lógico, capaz de reducir el riesgo y opera bien de forma preventiva sobre la vulnerabilidad, “neutralizando” la materialización de la amenaza, antes de que actúe ésta, o bien de forma curativa sobre el impacto, modificando el estado de seguridad del Activo agredido y reduciendo el resultado de la agresión, o sea después de ésta.

Se realizó la evaluación de las salvaguardas en el programa Pilar y se describieron cuáles aplican para el sistema de información del hospital, esta ponderación puede ser vista en el archivo de pilar entregado en el anexo. Para este análisis el programa Pilar presenta los resultados teniendo en cuenta varias categorías como son:

Aspecto cuyos valores son:

- G: Gestión.
- T: Técnico.
- P: Personal.
- F: Seguridad física.

Estrategia: Indica la estrategia que adopta la salvaguarda ante los incidentes para mitigar las amenazas, los valores posibles son:

CR (Corrección, Correction): Se parte que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.
Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes, etc.

EL (Eliminación, Elimination): Se dice que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, en general todo lo que tenga que ver con la fortificación o bastionado, cifrado de la información, armarios ignífugos, etc.

PR (Prevención, Prevention): Se dice que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos.

Ejemplos: autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, metodología segura de desarrollo de software, pruebas en pre-producción, segregación de tareas.

IM (Minimización / limitación del impacto, Impact minimization): Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente.

Ejemplos: desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente, etc.

DR (Disuasión, Deterrence): Se dice que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva.

Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente, etc.

DT (Detección, Detection): Se dice que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños.

Ejemplos: anti-virus, IDS, detectores de incendio, etc.

RC (Recuperación, Recovery): Se dice que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.

Ejemplos: copias de seguridad (back-up), etc.

MN (Monitorización, Monitoring): Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, es posible reaccionar atendiendo el incidente para limitar el impacto; si se detectan

cosas a posterior, con esto se puede aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro.

Ejemplos: registros de actividad, registro de descargas de web, etc.

AW (Concienciación, Awareness): Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación.

Ejemplos: cursos de concienciación, cursos de formación, etc.

AD (Administración, Administrative): Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que haya puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo.

Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad.

STD (Normativa, Standard): Se refiere a las salvaguardas basadas en normas.
Ejemplo: Normativas.

PROC (Procedimiento de seguridad, Procedure): Se refiere a las salvaguardas basadas en procedimientos.

Ejemplo: Procedimientos.

CERT (Producto certificado/acreditado, Certified): Se refiere a las salvaguardas basadas en productos certificados.

Ejemplo: Firewall que ha sido certificado, dispositivo biométrico que ha sido certificado, etc.

Se trata de un valor informativo (no se puede editar).

Salvaguarda: Muestra la salvaguarda o grupo de salvaguardas. Si no puede ver en forma de paraguas y un subíndice. Los colores y valores subíndice de los paraguas informan de la importancia relativa de la salvaguarda, que puede ser:

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

En el archivo de pilar se encuentra el análisis hecho de las salvaguardas y dicha evidencia se muestra en la Figura 88.

Figura 88. Análisis de las salvaguardas

Editar Exportar Importar Estadísticas

[base] Base

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: Propia

El análisis general informa que se deben aplicar salvaguardas para Protecciones Generales, Protección de la información ya que contiene datos confidenciales, Protección de las comunicaciones para garantizar conectividad y también evitar la captura de datos atreves de las redes de comunicaciones. La gestión de claves criptográficas para dar mayor seguridad al acceso a los recursos de información ya que se debe tener un mayor control de los funcionarios o personas que ingresan a las aplicaciones o equipos que guardan la información.

5.2.2 Definición del Plan de Tratamiento de Riesgos.

5.2.2.1 Política de Seguridad de la Información.

- Generalidades. La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo. Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la institución, tanto del Hospital Susana López de Valencia Popayán, como de la División de TIC`S, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información de la Institución y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política. Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Establecer las directrices, los procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos computacionales del Hospital Susana López de Valencia.

Alcance

Esta Política se aplica en todo el ámbito de la División de TIC`S del Hospital Susana López de Valencia Popayán, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Las políticas de seguridad se describen en el Anexo A, proporcionan instrucciones específicas sobre cómo mantener más seguros tanto los equipos de la División de TIC, (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias. Para el desarrollo de las políticas, es necesario considerar las diferentes fuentes de información, que permiten el desempeño diario de las funciones de la División.

5.2.2.2 Organización de la Seguridad de la Información.

- **Generalidades.** Es necesario tener bien definido un marco de gestión para efectuar diferentes tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades, para tener una eficiente administración de la seguridad de información. Debe tenerse en cuenta que ciertas actividades del Hospital

Susana López de Valencia Popayán pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información.

En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

- Administrar la seguridad de la información dentro del Hospital Susana López de Valencia y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.
- Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Institución.

En este control es necesario definir un Comité de Seguridad que entre sus funciones deberá:

- Revisar y proponer a la máxima autoridad del Hospital Susana López de Valencia Popayán para su aprobación, la Política y las funciones generales en materia de seguridad de la información
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro del Hospital Susana López de Valencia Popayán, específicamente en la división de TIC.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información de la Institución frente a interrupciones imprevistas.

Una vez integrado el Comité, es necesario se definan las funciones de los miembros del mismo para poder que este pueda desempeñar sus actividades y mejorar la seguridad en la institución. En la implementación están especificados los miembros del Comité.

El Comité de Seguridad de la Información debe proponer a la administración para su aprobación la definición y asignación de las responsabilidades que surjan de sus funciones.

Es necesario definir el proceso para la autorización de nuevos recursos para el procesamiento de información así como los requerimientos de Seguridad en contratos con Terceros, los principales puntos que se deben considerar lo siguiente:

a) Cumplimiento de la Política de seguridad de la información de la institución.

b) Protección de los activos de la institución, incluyendo:

- Procedimientos para proteger los bienes de la institución, abarcando los activos físicos, la información y el software.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.

d) Nivel de servicio esperado y niveles de servicio aceptables.

e) Permiso para la transferencia de personal cuando sea necesario.

f) Obligaciones de las partes del acuerdo y responsabilidades legales.

g) Definiciones relacionadas con la protección de datos.

h) Acuerdos de control de accesos que contemplen:

- Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
- Proceso de autorización de accesos y privilegios de usuarios.
- Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

i) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

j) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

k) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

l) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

m) Proceso claro y detallado de administración de cambios.

n) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

o) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

p) Controles que garanticen la protección contra software malicioso.

q) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

5.2.2.3 Gestión de los Activos de la Red.

- **Generalidades.** El Hospital Susana López de Valencia Popayán, en su División de TIC debe tener conocimiento sobre los activos que posee como parte importante de la administración de riesgos.

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección. Clasificar la información para señalar su sensibilidad y criticidad. Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

5.2.2.4 Responsabilidad sobre los activos. Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información

contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la Política.

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios, para luego elaborar un inventario con dicha información. El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 4 meses. El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de la Unidad Organizativa.

En la implementación del manual, se debe especificar el inventario realizado así como los responsables de cada activo. Una vez realizado el inventario, se debe clasificar el activo, en base a tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad, esta clasificación se muestra a continuación en la tabla 11, 12 y 13.

Tabla 11. Estándares de Confidencialidad

Activos de información (Confidencialidad)	Clase	Descripción
1	Pública	Puede ser revelado y proporcionado al público en general. Si el contenido fuera revelado, no se consideraran efectos para las operaciones de la Institución o de la División de TIC
2	Uso interno	Puede solo ser revelada y proporcionado en la División de TIC (no disponible a terceras partes). Si el contenido fuera revelado, no hubiera mucho efecto en las operaciones de la División de TIC y sus Servicios u operaciones.
3	Secreto	Puede ser solo revelado y proporcionado a partes específicas y departamentos. Si el contenido fuera revelado, hubiera un gran efecto en las operaciones de la División de TIC y sus servicios y/o operaciones.
4	Alta confidencialidad	Puede ser solo revelado y proporcionado a partes específicas. Si el contenido fuera revelado, hubiera un efecto irrecuperable en las operaciones de la División de TIC, incluyendo sus servicios y/o operaciones.

Fuente: Propia

Tabla 12. Estándares de Integridad

Activos de información (Integridad)	Clase	Descripción
1	No Necesaria	Usado solo para consulta. No tiene posibles problemas
2	Necesaria	Si el contenido fuera falsificado, hubiera problemas, pero estos no afectarían mucho las operaciones de la división de TIC, sus servicios y operaciones
3	Importante	Si la integridad se perdiera, hubiera un efecto fatal en las operaciones y servicios que provee la división de TIC

Fuente: Propia

Tabla 13. Estándares de Disponibilidad

Activos de información (Disponibilidad)	Clase	Descripción
1	Bajo	Si el activo no llegara a estar disponible, no hubiera efectos en las operaciones de la división de TIC
2	Medio	Si el activo no llegara a estar disponible, hubiera algún efecto en las operaciones y/o servicios que provee la División de TIC. Sin embargo, métodos alternativos pudieran ser usados para las operaciones, o los procesos podrían ser demorados hasta que la información esté disponible
3	Alto	Si el activo no estuviera disponible cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones y/o servicios de la división de TIC.

Fuente: Propia

Para clasificar los activos se consideró una de las siguientes categorías:

- CRITICIDAD BAJA: ninguno de los valores asignados superan el 2.
- CRITICIDAD MEDIA: alguno de los valores asignados es 2
- CRITICIDAD ALTA: alguno de los valores asignados es igual o mayor a 3

A continuación se muestra una tabla a seguir para realizar el inventario del activo (tabla 14): donde C – Valor de Confidencialidad, I – Valor de Integridad, y D – Valor de Disponibilidad, donde cada valor dependerá de las 3 tablas anteriores.

Tabla 14. Tabla inventario de Activos

Nombre del Activo	Ubicación del Activo	Responsable del Activo	Servicio o actividad que	Características Técnicas	Clasificación			Criticidad
					C	I	D	
								Baja / Media / Alta

Fuente: Propia

Sólo el propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los usuarios conozcan la nueva clasificación

5.2.2.5 Seguridad Física y del Entorno.

- **Generalidades.** La seguridad física y ambiental minimiza los riesgos de daños e interferencias a la información y a las operaciones del Hospital Susana López de Valencia en la División de TIC. Además, trata de evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.

Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la institución.

Previo a la implementación de un control de seguridad física y del entorno, es necesario que se realice un levantamiento de información de la situación actual del Hospital Susana López de Valencia, específicamente del área de TIC, en cuanto a su seguridad física para determinar las vulnerabilidades y posibles soluciones.

En puntos previos de este proyecto (Identificación de Riesgos) ya se realizó la recolección de la información necesaria para implementar los controles.

5.2.2.6 Gestión de Comunicaciones y Operaciones.

- **Generalidades.** Debido a los peligros existentes como software malicioso, virus, troyanos, etc. es importante que se adopten controles para prevenir cualquier tipo de amenazas.

Se debe separar los ambientes de pruebas y de operaciones, establecer procedimientos que garanticen la calidad de los procesos operativos para evitar incidentes producidos por la mala manipulación de información.

Las comunicaciones establecidas permiten el intercambio de información, se deberá establecer controles para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones. Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas.

El administrador de la red debe revisar con el encargado legal de la división de TIC, todos los contratos y acuerdos con terceros, pues es necesario garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

En la siguiente sección se definen las consideraciones que se deben tener para implementar este control.

5.2.2.7 Control de Acceso.

- **Generalidades.** Es necesario establecer controles que impidan el acceso no autorizado a los sistemas de información por parte de personal diferente a los que tienen permisos, para lo cual es necesario se implementen procedimientos para controlar la asignación de privilegios de acceso a los diferentes sistemas y aplicativos de la división de TIC del Hospital Susana López de Valencia . En estos procedimientos se especifican sugerencias

para mejorar el control actual de los accesos de los usuarios a diferentes niveles.

Es importante para la seguridad de la información controlar el acceso a los recursos, y protegerlos contra el acceso no autorizado, modificación o robo. Para el caso de la División de TIC se definirán políticas para el control de acceso así como los procedimientos que deben seguirse para poder implementarlos en los sistemas operativos y aplicativos. En los procedimientos considerados se debe tener en cuenta que los mismos consideren identificación, autenticación y autorización de los usuarios.

Objetivo

Entre los principales puntos que se desean cubrir con este control se tienen:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar de mejor forma la seguridad en conexiones entre la División de TIC y los proveedores externos.
- Mantener un registro de eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Alcance

En el procedimiento para implementar este control, se define una política de control de acceso que se aplica a todos los usuarios internos y externos que tienen diferentes permisos para acceder a los sistemas de información, tanto a la División de TIC o la red de datos del Hospital Susana López de Valencia.

Así mismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Controles de Acceso

- Negar el acceso a sistemas de cuentas anónimas o usuarios no identificados
- Limitar o monitorear el uso de cuentas con privilegios especiales
- Suspender o retardar el acceso a sistemas, aplicaciones después de un número de intentos fallidos.
- Remover cuentas obsoletas de usuarios que han dejado la compañía
- Suspender cuentas inactivas después de 30 o 60 días.
- Reforzar un criterio estricto de acceso
- Deshabilitar las configuraciones por defecto, servicios y puertos no requeridos.
- Reemplazar las configuraciones de contraseñas por defecto en las cuentas
- Limitar y monitorear reglas de acceso globales
- Forzar rotación de la contraseña
- Forzar requerimientos de contraseñas

- Sistemas de auditorías y eventos de usuarios y acciones, así como revisión de reportes periódicos.

Contraseñas

El usuario puede generar su contraseña, pero el sistema operativo fuerza al usuario a que el mismo cumpla con ciertos requerimientos, como por ejemplo que contenga un cierto número de caracteres, que incluya caracteres especiales, que no se relaciones con el nombre del usuario de la máquina.

Además de mantener un registro de las últimas claves ingresadas, la fecha en la que debe cambiarse.

Si una contraseña trata de ser vulnerada también puede configurarse el registro de intentos fallidos de acceso al sistema con lo cual se puede bloquear el acceso al mismo para de esta manera disminuir el riesgo debido a la vulneración de las contraseñas.

Uso de contraseñas

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

c) Seleccionar contraseñas de calidad, de acuerdo a las políticas de seguridad establecidas, en las que básicamente tratan los siguientes puntos:

- Sean fáciles de recordar.
- No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
- No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

Identificación y Autenticación de los usuarios

Todos los usuarios de la División de TIC deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En los casos que se requiere compartir un ID de usuario, tanto el administrador de la red como el responsable de cada área debe autorizar dicha compartición, así como definir el tiempo en el cual se requiere que se comparta el ID, luego del cual se debe eliminar el identificador y los privilegios del mismo.

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, por ejemplo, lectura, escritura, supresión y ejecución.
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, es decir, la modificación directa del dato almacenado.

Protección de los puertos de diagnóstico remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, por lo cual lo primero que se determina es el diagnóstico de que puertos se encuentran abiertos en la red.

5.2.2.8 Adquisición, desarrollo y mantenimiento de sistemas de Información

- **Generalidades.** En este control se deben revisar las aplicaciones como puntos críticos de vulnerabilidades, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta

implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Con este control se pretende cubrir varios puntos de seguridad, entre los principales objetivos se tienen:

- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible

Alcance

Los controles que se detallan a continuación se aplican a los sistemas informáticos, y a los sistemas operativos que integran los ambientes por el organismo de donde residen los mismos.

Para implementar un mayor control a la información confidencial o importante de la división de TIC, se debe entender como información confidencial a toda información que se refiere a planes de negocio, tecnología no anunciada, información financiera no pública; e información personal como contraseñas.

La División de TIC debe tener aprobado un procedimiento de cambios aprobado por la gerencia, y los cambios deben ser documentados y comunicados a los empleados involucrados. En la implementación se especifica el proceso para llevar a cabo un cambio.

Revisión técnica de los cambios en el sistema operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, el administrador de la red debe tener un procedimiento en el cual se incluye:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
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.
c) Asegurar la actualización del Plan de Continuidad de las Actividades del Organismo.

5.2.2.9 Gestión de Incidentes de Seguridad de la Información.

- **Divulgación de eventos y de debilidades de la seguridad de la información**. Es importante que la División de TIC tenga un procedimiento a seguir cuando se presente un incidente de seguridad en la red, pues es necesario que pueda aprender de los errores y evitar que un ataque ocurra. Por lo cual es importante que luego de cada incidente siga un

procedimiento, técnicas, configuraciones necesarias para reforzar lo modificado y mejorar la seguridad.

Es necesario que se tenga un mejor control del uso apropiado de los recursos de la red, en otros términos, todos los recursos de la informática deben usarse de una manera ética y responsable. El uso de recursos de tecnología de información puede categorizarse ampliamente 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.

Administración de incidentes y mejoras de la seguridad de la información

Después que el incidente ha sido resuelto, es necesario realizar una documentación del mismo para poder determinar las experiencias aprendidas del mismo. Como resultado de un análisis posterior al reporte de incidentes, el personal de seguridad puede necesitar emitir alarmas o advertencias a todos los empleados de la División de TIC sobre las acciones a tomar para reducir 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.
- Minimizar el riesgo de modificación desautorizado de archivos electrónicos guardando los datos sensibles en los medios de comunicación trasladables.
- Asegurar que personal apropiado se entrena para proteger los archivos electrónicos sensibles o clasificados.
- Proveer del respaldo y recuperación de archivos para proteger contra la pérdida de información.
- Asegurar que la seguridad de los archivos electrónicos esté incluido en los planes de seguridad de información globales de la institución.

5.2.2.10 Gestión de Continuidad del Negocio.

- **Generalidades.** Un punto importante para toda organización, es administrar de forma ordenada las actividades necesarias para la continuidad del negocio, en este procedimiento se deben involucrar a todos los empleados de la División de TIC.

El plan de continuidad debe mantenerse actualizado y ser una parte integrada en los diversos procesos de la división de TIC.

Objetivo

Este control es importante para cubrir los puntos críticos de la CMS en caso de algún desastre, a continuación se detallan los principales objetivos:

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
- Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

  a) Detección y determinación del daño y la activación del plan.

  b) Restauración temporal de las operaciones y recuperación del daño producido al sistema original.

  c) Restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

- Asignar funciones para cada actividad definida

Alcance

Estos controles se aplican a los servicios y operaciones críticas de la División de TIC

Proceso de gestión de la 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
- 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.

Desarrollo e implantación de planes de contingencia

Al desarrollar el plan se debe tener bien definido y especificado las responsabilidades a asignarse a cada persona responsable de un proceso determinado, para el caso de la División de TIC de la Universidad del Cauca se debe considerar los siguientes responsables:

- 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.

5.2.2.11 Implementación del Plan de Tratamiento de Riesgos. El objetivo de esta etapa es tomar la acción más apropiada de tratamiento para cada uno de los riesgos identificados, en base a las secciones 5.1.6 Identificación de amenazas y 5.1.7 Identificación de vulnerabilidades, en la presente sección se muestra la tabla No. 15 con el Plan de Tratamiento de Riesgos para cada amenaza y/o vulnerabilidad.

PTR: Plan de Tratamiento de Riesgos.

Tabla 15. Plan de Tratamiento de Riesgos

Activos	Amenazas	Vulnerabilidades	PTR
Servicio Web	Errores de los Usuarios	Falta de políticas de seguridad Insuficiente entrenamiento de empleados Falta de Monitoreo	**Reducir**
	Errores del Administrador del sistema / de Seguridad	Falta de políticas de seguridad Falta de Monitoreo	**Reducir**
	Alteración de la Información	Falta de políticas de seguridad Falta de Monitoreo	**Reducir**
	Destrucción de la Información	Falta de procedimientos para cambio	**Reducir**
	Caída del Sistema por agotamiento de recursos	Falta de planes de continuidad del Negocio Falta de recursos necesario	**Asumir**
	Abuso de Privilegios	Falta de políticas de seguridad	**Reducir**
	Uso no Previsto	Falta de política	**Reducir**

	Modificación de la Información	Falta de procedimientos para cambio	**Reducir**
Servicio DNS	Errores de los Usuarios	Falta de políticas de seguridad Falta de Monitoreo	**Reducir**
	Errores del Administrador del sistema / de Seguridad	Falta de políticas de seguridad Insuficiente entrenamiento de empleados Falta de Monitoreo	**Reducir**
	Alteración de la Información	Falta de políticas de seguridad Falta de Monitoreo Almacenamiento no protegido	**Reducir**
	Destrucción de la Información	Falta de procedimientos para cambio	**Reducir**
	Caída del Sistema por agotamiento de recursos	Falta de planes de continuidad del Negocio Falta de recursos necesario	**Reducir**
	Suplantación de la identidad de usuario	Falta de control de Acceso	**Reducir**
Servicios de Directorios	Errores de los Usuarios	Falta de políticas de seguridad Insuficiente entrenamiento de empleados Falta de Monitoreo	**Reducir**
	Errores del Administrador	Falta de políticas de	**Reducir**

	del sistema / de Seguridad	seguridad Falta de Monitoreo	
	Alteración de la Información	Falta de políticas de seguridad Falta de Monitoreo Almacenamiento no protegido	**Reducir**
	Destrucción de la Información	Falta de procedimientos para Cambio Almacenamiento no protegido	**Reducir**
	Fugas de Información	Falta de políticas Falta de control de acceso	**Reducir**
	Caída del Sistema por agotamiento de recursos	Falta de planes de continuidad del Negocio Falta de recursos necesario	**Reducir**
	Suplantación de la identidad de usuario	Falta de control de Acceso	**Reducir**
	Abuso de Privilegios	Falta de políticas de seguridad	**Reducir**
	Uso no Previsto	Falta de política	**Reducir**
	Acceso no autorizado	Falta de control de Acceso	**Reducir**
	Modificación de la Información	Falta de procedimientos para cambio	**Reducir**
	Destrucción de la Información	Falta de procedimientos para Cambio Falta de control de Acceso	**Reducir**
	Revelación de la	Falta de políticas de	**Reducir**

	Información	seguridad	
Equipo de Comunicaciones [Servidores1] – Switch de Servidores	Fuego	Falta de protección contra fuego	**Reducir**
	Desastres Industriales	Falta de protección física adecuada	**Asumir**
	Avería de origen físico o lógico	Falta de mantenimiento adecuado	**Reducir**
	Errores del Administrador del sistema / de Seguridad	Falta de conocimiento del administrado	**Reducir**
	Errores de Mantenimiento / Actualizaciones de Equipos	Falta de conocimiento del administrado	**Reducir**
	Caída del Sistema por agotamiento de recursos	Falta de planes de continuidad del Negocio Falta de recursos necesario	**Reducir**
	Abuso de Privilegios de Acceso	Falta de políticas de seguridad	**Reducir**
	Uso no Previsto	Falta de política	**Reducir**
	Acceso no Autorizado	Falta de políticas Falta de protección física Falta de control de Acceso	**Reducir**
	Manipulación de Hardware	Falta de control de Acceso	**Reducir**

Fuente: Propia

5.2.2.12 Implementación de los controles seleccionados.

- **Documento de política de seguridad de la información.** A continuación se nombran las políticas de seguridad de la información recomendadas para la División de Tecnologías de la Información y las Comunicaciones del Hospital Susana López de Valencia, de acuerdo a las recomendaciones hechas en cada uno de los dominios de la norma ISO-270002 e ISO 17799

1. Política de Seguridad de La Información
2. Política de Administración de Cambios.
3. Política de Buen Uso de os Recursos de la Empresa
4. Política de Administración de Cuentas
5. Política de Administración de Contraseñas
6. Política de Respaldo y Recuperación de Información
7. Política de uso de Internet
8. Política de Licenciamiento de Software
9. Política de uso del Correo Electrónico
10. Política de Adquisición o Renovación de Recursos de Tecnología
11. Política de acceso Físico a Los Recursos
12. Política de Detección de Virus
13. Política de Acceso a Proveedores
14. Política de Acceso Especial A Recursos
15. Política de administración de Incidentes
16. Política de Entrenamiento y capacitación en Seguridad
17. Política de Monitoreo a la Seguridad

Nota: La definición y establecimiento de cada política se presenta en el Anexo A.

En la implementación se debe desarrollar en un periodo de tiempo de un año por lo cual las primeras decisiones tomadas por el Ingeniero responsable de la seguridad de la información fue solicitar al jefe del área de informática un equipo

para ser utilizado como servidor de monitoreo de seguridad e instalar la aplicación OSSIM

OSSIM en una consola de seguridad central, que permite gestionar y saber el nivel de seguridad (métrica) que tiene una empresa. Se trata de un proyecto Open Source, con lo que todo el mundo puede disfrutar de él sin ningún coste, además de poder colaborar en su código para formar parte de su evolución.

OSSIM engloba más de 22 herramientas de seguridad, entre ellas: IDS (Snort), detector de vulnerabilidades (Nessus), firewall (Iptables), detector de sistema operativo (Pof), monitorización en tiempo real y estadísticas (Ntop), detector de anomalías (Rrd), escaneadores (Nmap), y otros.

Este requerimiento fue aprobado y se instaló la consola como se muestra en la figura que se utilizará como servidor de monitoreo de seguridad de la red, además la institución adquirió un firewall hardware que complementara los niveles de seguridad dela información.

Como resultado de las recomendaciones hechas en la primera visita se tomaron algunas medidas correctivas en los centros de cableados como quitar elementos de madera, cajas y otros artículos que fueron traslados a áreas de almacenamiento o desechadas

5.3 VERIFICAR

En esta etapa se determinará la efectividad de la solución planteada y diseñada para el área de información y tecnología del Hospital Susana López de Valencia y para ello se requiere medir los resultados en fusión del desempeño con respecto a los proceso antes de realizar la aplicación del mismo. Para el caso propuesto no

se llegará a esta etapa dado que la implementación y verificación de los cambios pueden llevar un tiempo estimado entre 6 meses a un año, con continuo seguimiento, en consecuencia se puede inferir que la aplicación redundará en mejores prácticas y uso responsable de la información.

5.4 ACTUAR

Esta etapa al igual que la etapa de verificar, se requiere que se haya verificado y normalizado todo el proceso, con lo que se permitirá documentar todos los aspectos o de las operaciones que permitirán estandarizar cada uno de los procesos y procedimientos, así mismo como se iniciar la capacitación al personal involucrado.

Para esta etapa es importante obtener un grado de rendimiento superior al anterior, para poder verificar se alcanzó lo planificado de acuerdo a los cambios sistematizados y documentados.

En caso de no haber logrado los objetivos esperados, se analizarán las causas, generando las acciones que permitan la corrección o erradicación por completo de las mimas.

6. CONCLUSIONES

Al término del proyecto se cumplió con todos los objetivos propuestos, ayudando a sentar las bases para la mejora de la seguridad de la información en el Hospital Susana López de Valencia E.S.E.

Al aplicar la norma ISO 27001, en procesos críticos que se manejan en el HSLV se pueden sentar las bases para garantizar la seguridad y disponibilidad los servicios que presta la Institución.

Las políticas de seguridad de la información permitirán tener un mayor control sobre todos los activos que maneja el HSLV.

La información es el principal activo que tiene el HSLV, es por ello que se debe tener mucho cuidado al momento de almacenar y trasladar los dispositivos de respaldos.

El análisis del riesgo determina la probabilidad, ocurrencia de las amenazas y determinar el impacto potencial en la Institución.

El riesgo informático es todo factor que pueda generar una disminución en la confidencialidad, integridad y disponibilidad en la Institución.

7. RECOMENDACIONES

Se recomienda que la cúpula de Directivos considere como prioridad principal el cumplimiento de las sugerencias dadas por los integrantes del grupo a cargo de este proyecto.

El proyecto puede continuar con el fin de realizar las fases faltantes de la norma como son las de actualización y Chequeo de las políticas, recomendaciones y de las observaciones entregadas por el grupo a cargo del proyecto.

Otra recomendación es que el personal involucrado en la aplicación, ejecución y control de las políticas debe sujetarse al cumplimiento de la norma y deberán estar en constante actualización y revisión.

También se recomienda realizar una evaluación de las políticas de seguridad de la información semestralmente, para que sigan manteniéndose acorde a las necesidades de la empresa, esto se puede lograr mediante la aplicación de auditorías internas.

Igualmente se debe realizar un control del acceso de las personas que ingresan al centro de cómputo a través de dispositivos de seguridad electrónicos, para impedir futuros desmanes en el mismo.

De acuerdo al análisis de vulnerabilidades desarrollado, se recomienda realizar las actualizaciones de los sistemas operativos de los servidores y servicios instalados (hardening).

Para permitir el acceso remoto hacia los servidores se recomienda el uso de herramientas de conexión seguras, como SSH, o escritorio remoto, y evitar el uso de aplicaciones no seguras como el VNC.

BIBLIOGRAFÍA

1. **ECBTI.** Lineas de Investigación. [En línea] 3 de Marzo de 2011. http://estudios.unad.edu.co/ecbti/investigacion. .

2. **Minsalud.** Minsalud. [En línea] 25 de Febrero de 2013. http://www.minsalud.gov.co/Normatividad/Resoluci%C3%B3n%200509%20de%202013.pdf.

3. **Alfonso, Nicole.** Apuntes de investigación. [En línea] 3 de Septiembre de 2012. http://apuntesdeinvestigacion.upbbga.edu.co/wp-content/uploads/ESI-Nicole-juliet-Alfonso-Nieto.pdf.

4. **HOSPITAL UNIVERSITARIO SAN JOSÉ DE POPAYÁN .E.S.E.** Hospital San Jose. [En línea] 10 de febrero de 2014. http://www.hospitalsanjose.gov.co/gestionNoticias/verNoticia.php?idn=2&id=261.

5. **Areitio, javier.** *Seguridad de la información. Redes, informática y sistemas .* madrid : Paraninfo, 2008.

6. **Catamarca.** Dirección Provinsial de informatica . [En línea] 1 de Julio de 2011. http://www.informatica.catamarca.gov.ar/multimedia/archivos/norma_seguridad_informatica_reducido.pdf.

7. **El portal de ISO 27001.** ISO 27000.es. [En línea] 4 de Febrero de 2012. http://www.iso27000.es/sgsi.html.

8. **Cotecna.** cotecna. [En línea] 2012. [Citado el: 10 de Agosto de 2013.] http://www.cotecna.com.ec/Services/~/media/Countries/Ecuador/Documents/Brochure-iso-27001-cotecna-ecuador-FINAL.ashx.

9. **AEC.** AEC. [En línea] 2012. [Citado el: 4 de Agosto de 2013.] http://www.aec.es/web/guest/centro-conocimiento/norma-une-isoiec-27001.

10. **iso27000.** El portal de ISO. [En línea] 2012. [Citado el: 4 de Agosto de 2013.] http://www.iso27000.es/iso27000.html.

11. **Solarte, Francisco.** Datateca unda. [En línea] 20 de Frerero de 2012. datateca.unad.edu.co/.../leccin_17_aspectos_jurdicos_de_la_norma_iso_.

12. **Sigea.** Sigea. [En línea] 24 de Junio de 2013. [Citado el: 3 de Septiembre de 2013.] http://www.sigea.es/estandares-para-evaluar-riesgos-de-seguridad-de-la-informacion/.

13. **Ministerio de justicia Gobierno de España.** sisej. [En línea] 3 de Julio de 2013. http://www.sisej.com/documentos/doc_view/1407-politica-de-calidad-y-seguridad-en-las-nuevas-tecnologias.

14. **Seguridad Inforatica.** Seguridad . [En línea] 13 de Mayo de 2012. [Citado el: 13 de Agosto de 2013.] https://seguridadinformaticaufps.wikispaces.com/page/history/PILAR+-+Herramienta+para+An%C3%A1lisis+y+Gesti%C3%B3n+de+Riesgos.

15. **Tools, Pilar.** TITULO LIBRO,PAIS, EDITORIAL, [En línea] 22 de Octubre de 2012. PAGINA INTERNET|

16. **COBIT.** *Cobit, Sumario Ejecutivo.* Buenos Aires : Systems Auditand Control, 1998.

17. **IT Governance Institute.** redyseguridad. [En línea] 4 de Diceimbre de 2013. http://redyseguridad.fi-p.unam.mx/proyectos/cobit/seccion_informativa/pdfscobit/resumen_ejecutivo.pdf.

18. **Reyes, Alejandro.** Unam_Cert. [En línea] 22 de Octubre de 2010. [Citado el: 30 de Agosto de 2013.] http://www.seguridad.unam.mx/descarga.dsc?arch=2776.

19. **Metasploit.** Ciscmetasploit. [En línea] Septiembre de 2011. [Citado el: 15 de Agosto de 2013.] http://ciscmetasploit.wordpress.com/about/.

20. **Diario Oficial.** Diario Oficial. [En línea] 5 de Enero de 2009. http://www.ccit.org.co/files/Leyes/Ley_1273_de_2009.pdf.

21. **MinTics.** Gobierno en linea. [En línea] 21 de Diciembre de 2012. http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/decreto-2693-de-2012.pdf.

22. **Equipo Gestión de la calidad - Hospital San Blas.** Politicas de seguridad informatica . [En línea] 19 de Abril de 2011. http://www.hospitalsanblas.gov.co/documentos/politicas/informaticas.pdf.

23. **Magerit Libro I - Método.** Administración electronica. [En línea] 4 de Octubre de 2012. http://www.seap.minhap.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/Monografias0/parrafo/Magerit_2012/Magerit_v3_libro1_metodo.pdf.

24. **Mendez Barco, Andrés.** *GUÍA DE SEGURIDAD DE LAS TIC.* Madrid : Ministerio de Defensa, 2008.

25. **Hospital, Susana Lopez.** Hospital Susana Lopez. [En línea] 14 de Febrero de 2013. http://www.hosusana.gov.co/resena.

26. **Oficina de Estadistica e Informatica - Arequipa.** Oficina de Estadistica e Informatica. [En línea] 30 de Julio de 2012. http://redperifericaaqp.gob.pe/sites/default/files/Directivas/GESTION%20DE%20SEGURIDAD%20DE%20INFORMACION%20_OEI.pdf.

27. **Hospital Centro Oriente.** esecentro oriente. [En línea] 4 de Abril de 2013. http://www.esecentrooriente.gov.co/hco/images/stories/planeacion/gestioncalidad/implementacion%20del%20sig.pdf.

28. **ITGI Y la OGC.** ISACA. [En línea] 4 de Agosto de 2008. http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf.

ANEXOS

Los anexos del presente proyecto se encuentran almacenados en la carpeta “ANEXOS” que acompaña este documento.