DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA IPS ASSALUD DE COROZAL SUCRE, MEDIANTE LA IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT (V3.0) Y LA NORMA ISO 27001:2013

LUIS CARLOS DIAZ RICARDO

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION EN SEGUIDAD INFORMATICA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
COROZAL
2017

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA IPS ASSALUD DE COROZAL SUCRE, MEDIANTE LA IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT (V3.0) Y LA NORMA ISO 27001:2013

LUIS CARLOS DIAZ RICARDO

Propuesta de grado para optar por el título de Especialista en Seguridad Informática

Asesor de Proyecto
Ing. YINA ALEXANDRA GONZALEZ SANABRIA

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION EN SEGUIDAD INFORMATICA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
COROZAL
2017

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma Jurado

_____

Firma Jurado

Corozal, 18 de Noviembre de 2017

DEDICATORIA

Primero que todo quiero dedicar a nuestro padre superior Dios, que fue quien me guio en todo momento con su sabiduría y divinidad en el andar de esta experiencia.

De igual forma a mis padres, hermanos, esposa e hijo que sin ellos no habría sido posible empezar y culminar esta etapa tan importante de la vida, como lo es formarnos profesionalmente y con sentido social apoyados por los valores inculcados en mi hogar puestos a prueba en la universidad.

Por último a todas aquellas personas, amigos que de alguna u otro manera estuvieron involucradas en el desarrollo de este proyecto agradecemos toda su colaboración y paciencia.

AGRADECIMIENTOS

Doy infinitas gracias a Dios por ser la fuerza que me impulsa diariamente y me permitió seguir adelante durante el tiempo recorrido; mis familiares por su apoyo incondicional y estar siempre a mi lado siendo los pilares fundamentales en mi vida.

A la Universidad, por brindarme la oportunidad de adquirir conocimientos y experiencias que contribuyeron a mi crecimiento como persona y profesional.

A todas y cada unas de las personas que contribuyeron a que esta meta llegara a su final.

CONTENIDO

Pág.

LISTADO DE GRAFICAS

Pág.

LISTADO DE IMÁGENES

Pág.

LISTADO DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCIÓN

Un sistema de gestión de la seguridad de la información (SGSI), es aquel que permite a una empresa tener su información de manera segura, teniendo en cuenta que se entiende por información todo dato que la empresa considere valioso, y el cual se pueda transmitir por los distintos medios de comunicación sean audiovisuales, escritos, por señas, etc.

Los SGSI están fundamentados en la norma ISO 27001, la cual establece lineamientos para proteger la confidencialidad, integridad y disponibilidad, de la información de una empresa, con el fin de garantizar que todos los datos de la empresa se encuentren debidamente protegidos y son accedidos de la mejor forma posible.

Para poder llevar a cabo el diseño de un SGSI, es necesario tener pleno conocimiento de los bienes que posee una empresa y los riesgos a los cuales están expuestos, para llevar a cabo este proceso es necesario la implementación de una metodología que establezca las pautas para tal fin, en este caso será utilizada Magerit, la cual se centra en tres fases, la planeación, el análisis de riesgo y el tratamiento del riesgo, con ello se logra obtener una idea clara de los riesgos y además se definen salvaguardas para ser utilizados en caso de presentarse uno de ellos.

La IPS ASSALUD, es una entidad encargada de brindar servicios en salud, se encarga del manejo y atención de pacientes, lo que convierte la información que en ella se maneja en un bien de gran valor y el cual actualmente se encuentra en gran riesgo debido a que no se cuenta con ningún tipo de controles de seguridad ni políticas que fijen con claridad el manejo de toda la información dentro de la IPS.

1. TITULO

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA IPS ASSALUD DE COROZAL SUCRE, MEDIANTE LA IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT (V3.0) Y LA NORMA ISO 27001:2013

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES

Dentro de las aplicaciones de un SGSI se destacan ciertas aplicaciones dentro del ámbito nacional e internacional me permito citarlos a continuación como un marco referencial para el desarrollo de este proyecto.

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

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

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

El fin de este proyecto es proponer un SGSI que le permita a la IPS ASSALUD mantener su sistema de información funcionando y alejado de los riesgos, se utilizara la metodología MAGERIT con el fin de mantener un estándar durante el análisis de riesgo y este sea lo más coherente posible.

2.2 DESCRIPCIÓN DEL PROBLEMA

En la Institución Prestadoras de Servicios en Salud ASSALUD, no se le da la importancia necesaria a la seguridad informática, se puede decir que no tiene un buen diseño y estructura en su Sistema de Información, igualmente se observa que no tienen implementadas metodologías, técnicas o normas de seguridad estandarizadas que les permita garantizar la integridad del Sistema.

Actualmente en la IPS ASSALUD no se cuenta con ningún tipo de políticas de seguridad lo que incrementa los daños en los activos y peor aún dificultades para llevar a fin termino el desarrollo de su actividad principal, la cual consiste en atender a pacientes tanto en medicina general como especializada, manteniendo de esos pacientes su historial clínico y evoluciones por tratamientos.

Siendo esta la situación de la empresa y considerando que la información es un bien vital, se presenta una escenario critico el cual es la violación de la confidencialidad de la información ya que no se cuenta con perfiles designados para cada rol, todo usuario puede visualizar la información y además modificarla, lo que causa una gran falla en lo pertinente a la disponibilidad, confidencialidad e integridad de la información, si se mira desde la perspectiva de la metodología MAGERIT se encontrara una gran falencia en esas dimensiones de valoración de activo.

Además de lo antes mencionado se presenta perdida de las historias clínicas lo que genera grabes daños al sistema de información y repercusiones legales debido a que los pacientes exigen este valioso dato y en la IPS no se puede entregar por que ha desaparecido, y como si fuera poco las copias de seguridad del sistema que almacena el historial se lleva en un disco extraíble y este es de uso general, es decir todo el personal lo puede utilizar para trasladar información entre los equipos de cómputo.

Al mirar el sistema de forma general los activos no cuentan con ninguna protección y se encuentran completamente expuestos a cualquier amenaza, las cuales cobran una gran frecuencia debido a las debilidades obvias que posee la IPS ASSALUD.

2.3 FORMULACIÓN DEL PROBLEMA

¿El diseño de un sistema de gestión de la seguridad de la información podrá minimizar las vulnerabilidades, amenazas y riesgos asociados al uso del sistema de información de la IPS ASSALUD?

3. JUSTIFICACIÓN

La seguridad informática es el proceso por medio del cual se protegen los activos informáticos. Se debe tener en cuenta que en la actualidad, la información juega un papel muy importante y es considerado el activo más valioso en todas las organizaciones, lo cual ha generado que se le dé mayor atención a la disponibilidad, confidencialidad e integridad de los sistemas informáticos para así garantizar una fluidez de información segura y sistemas protegidos.

Actualmente la IPS ASSALUD, no cumple con los mínimos estándares para el manejo de la información, se reportan perdidas de historias clínicas, virus en el sistema, daños de la base de datos, violación en accesos, uso desmedido de los recursos para fines personales, demandas por parte de los pacientes pertinentes a su historial clínico, todas estas situaciones reducen el impacto positivo de la IPS y la llevan a tener una mala imagen corporativa y todo ello debido a que no cuentan con un SGSI que les permita tener control sobre el activo más grande que tiene cualquier empresa su información.

Por esta razón se pretende diseñas del SGSI basado en la norma ISO 27001, utilizando como base la metodología de análisis de riesgo MAGERIT, con el fin último de fortificar el sistema de información, brindando las herramientas necesarias para contrarrestar todos los percances y evitar que la empresa llegue a momento más caótico que el presentado en la actualidad, con la implementación del SGSI se lograra mejorar la imagen corporativa de la IPS, evitando que pacientes se quejen o decidan retirase de nuestro servicio, lo que al presentarse generaría la cancelación de los contratos con las aseguradoras, viéndose esto reflejado en la disminución de los recursos económicos que tiene la IPS.

Si no se lleva a cabo el diseño del SGSI, en poco tiempo la IPS mas que poder brindar un servicio, se enfrascara en responder por asuntos legales y denuncias de sus pacientes a los cuales en muchas veces le es violado el derecho de confidencialidad Paciente – Medico, lo que en Colombia es un asunto supremamente legal y que en este caso no recaería sobre el médico sino directamente sobre la IPS ya que no cuenta con un sistema de información seguro que garantice este derecho.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de la Seguridad de la Información adecuado para la corrección de los problemas de seguridad de la información de la IPS ASSALUD de Corozal-Sucre, mediante la implementación de la metodología MAGERIT y la norma ISO 27001:2013.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar, clasificar y valorar los activos con los que cuenta el sistema de información de la IPS ASSALUD aplicando la metodología MAGERIT.

- Identificar y valorar las amenazas presentes en los activos del sistema de información de la IPS ASSALUD aplicando la metodología MAGERIT.

- Gestionar los riegos y especificar salvaguardas, que permitan controlar los riesgos posibles en la IPS ASSALUD, según lo dispuesto en la metodología MAGERIT.

- Crear un Sistema de Políticas de Seguridad que permita optimizar el sistema de seguridad de información manejado actualmente en la IPS ASSALUD.

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO

Los conceptos que se utilizan para elaborar este proyecto son los siguientes:

✓ **Seguridad de la Información:**

Este término enmarca la seguridad que tiene un activo de información, no solo siendo este información sino también todo el conglomerado de elementos que respaldan la información, ya sean estos servidores, bases de datos en la nube, redes LAN, y elementos de backup, para poder establecer una buena seguridad informática es necesario cumplir ciertos requisitos que trascienden desde normas internacionales, leyes, hasta simples condiciones expuestas o exigidas por una empresa.

De este término se deriva el concepto de seguridad informática la cual según Aguilera López "Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información segura y confiable."(Aguilera López, Purificación, 2010).

✓ **Activo de la Información:**

Según Alexander (2007, 44). Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, los activos necesitan tener protección para asegurar una correcta operación del negocio y una continuidad de las operaciones. Para cualquier tipo de empresa es de vital importancia la gestión y la responsabilidad de los activos.

En este punto es importante clasificar que es un activo de información. Según el ISO 17799:2005 (Código de práctica para la gestión de seguridad informática), un activo de información es algo a lo que la organización directamente le asigna un valor, por lo tanto, la organización debe proteger. Los activos de información se pueden dividir en las siguientes categorías:

- Activos de información: (datos, manuales de usuarios, etc.)
- Documentos papel: (contratos).
- Activos de Software: (aplicaciones, software de sistemas. etc.)

- Activos de Hardware: (computadores, impresoras, Servidores, medios magnéticos)
- Personal: (clientes, empleados).
- Servicios: (comunicaciones, etc.)

✓ **Políticas de la Seguridad Informática:**

Las Políticas de Seguridad son ITEM que permiten la comunicación sencilla del buen uso de las herramientas de la información que la organización posee. Dando a conocer las buenas prácticas del manejo de la información, resaltando siempre la integridad de los sistemas, ratificando que la información es el eje fundamental de la organización. Se debe tener en cuenta algunos elementos importantes para la elaboración de las políticas:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Responsabilidades de los usuarios con respecto a la información a la que él o ella tiene acceso.

Las políticas deben surgir a partir del análisis y administración del riesgo, deben ser claras y especificas quien es la autoridad que asuma las medidas disciplinarias y evaluación de la situación, estas deben ser promovidas y dadas a conocer a todos los empleados de la organización.

✓ **ISO/ IEC 27001.**

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.[1]

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

✓ **Sistema de Gestión de Seguridad de la Información (SGSI).**

El ***SGSI*** es la abreviatura usada para referirse al ***Sistema de Gestión de la Seguridad de la Información*** e ISMS son las siglas equivalentes en ingles a Information Security Management System.[2]
El Sistema de Gestión de Seguridad de la Información, según *ISO 27001* consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización.

✓ **Fundamentos:**

Para garantizar que el ***Sistema de Gestión de Seguridad de la Información*** gestionado de forma correcta se tiene que identificar el ***ciclo de vida*** y los aspectos relevantes adoptados para garantizar su:

- Confidencialidad: la información no se pone a disposición de nadie, ni se revela a individuos o entidades no autorizados.

- Integridad: mantener de forma completa y exacta la información y los métodos de proceso.

- Disponibilidad: acceder y utilizar la información y los sistemas de tratamiento de la misma parte de los individuos, entidades o proceso autorizados cuando lo requieran.
  Según el conocimiento que se tiene del ciclo de vida de la información relevante se puede adoptar la utilización de un proceso sistemático, documentado y conocido por toda la empresa, desde un enfoque de riesgos empresarial. El proceso es el que constituye un ***SGSI***.

[1] tomado de https://advisera.com/27001academy/es/que-es-iso-27001/
[2] tomado de http://www.pmg-ssi.com/2015/07/que-es-sgsi/

✓ **Identificación de Amenazas y Vulnerabilidades**.

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado que puede generar daño a la organización y a sus activos.

Podemos entender por información todo el conjunto de datos que se organizan en una organización y otorgan valor añadido para ésta, de forma independiente de la forma en la que se guarde o transmita, el origen que tenga o la fecha de elaboración.

Las Amenazas. "Una amenaza es la identificación de un potencial evento no deseado". En esta definición, los actores se refieren a una situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural. En su libro Information Segurity Risk Analysis (Welter, 2001). Thomas Welter plantea que una amenaza puede significar muchas cosas, dependiendo el texto donde se ubique.

Clasificación de las amenazas. Cuando la empresa inicia la identificación de amenazas que pudiesen afectar sus activos, conviene clasificarlas por su naturaleza, para así facilitar su ubicación. En consecuencia, también difieren los métodos para estimar su posibilidad de ocurrencia:

- Amenazas Naturales
- Amenazas a Instalaciones
- Amenazas Humanas
- Amenazas Tecnológicas
- Amenazas Operacionales
- Amenazas Sociales

Las Vulnerabilidades, son debilidades de seguridad asociadas con los activos de información de una organización. Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daños. Simplemente son condiciones que pueden ser una amenaza que afecte a un activo. Las vulnerabilidades se pueden clasificar como:

- Seguridad de los Recursos Humanos

- Control de Acceso
- Seguridad Física y Ambiental
- Mantenimiento, desarrollo y adquisición de sistemas de información.
- Gestión de operaciones y comunicación

Una vez clasificadas las vulnerabilidades, por cada una de ellas, se deberá evaluar la posibilidad de que sean explotadas por la amenaza. Es bueno entender que las vulnerabilidades y las amenazas deben presentarse juntas, para causar incidentes que pueden dañar los activos.

✓ **Análisis de Riesgo y su Evaluación.**

El objetivo de análisis de riesgo es identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan multiplicando la probabilidad por el impacto, el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la probabilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

✓ **Metodología MAGERIT.**

Una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma ***implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados***. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.[3]

[3] Portal administración electrónica. MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los sistemas de información. [En línea]. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pe_Mage rit.html#.VCmVZhZRVJQ

Puntualmente ***MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad,*** buscando ***identificar las amenazas*** que pueden llegar a afectar la compañía ***y las vulnerabilidades*** que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiada.

Magerit está compuesta por tres libros, el libro I, describe el método a seguir para la ejecución del análisis de riesgos. El libro II; catálogo de elementos discriminados en: activos, amenazas, vulnerabilidades, impacto, riesgo y salvaguardas. Y el libro III, es la guía de técnicas para realizar el análisis final y gestión de riesgos, se puede aplicar técnicas cualitativas o cuantitativas.[4]

5.2 MARCO CONCEPTUAL

- ✓ **Integridad:** Protección de la información respecto a modificaciones no autorizadas, tanto a la almacenada en los elementos computarizados de la organización como la usada como soporte. Estas modificaciones pueden llevarse a cabo de manera accidental, intencional, o por errores de hardware-software.

- ✓ **Autenticidad:** Garantía que el usuario autorizado tiene para usar un recurso y que no sea suplantado por otro usuario.

- ✓ **Control de Acceso:** Posibilidad de controlar los permisos a cualquier usuario para acceder a servicios o datos de la organización.

- ✓ **Disponibilidad de los recursos y de la información**: Protección de los elementos que poseen la información de manera que en cualquier momento, cualquier usuario autorizado pueda acceder a ella, sin importar el problema que ocurra.

- ✓ **Consistencia:** Capacidad del sistema de actuar de manera constante y consistente, sin variaciones que alteren el acceso a la información.

[4] DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I: Método Libro II: Catálogo de Elementos, Libro III: Guía de Técnicas. 2012

- ✓ **Auditoría:** Capacidad para determinar todos los movimientos del sistema, como accesos, transferencias, modificaciones, etc., en el momento en que fueron llevados a cabo (fecha y hora).

- ✓ **Amenaza:** Será cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. De esta manera, el punto más débil.

- ✓ **Vulnerabilidad:** Consiste en cualquier debilidad que puede explotarse para causar pérdida o daño del sistema. De esta manera, el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.

- ✓ **Seguridad de la información:** Es un término que hace referencia a la seguridad de activos de forma general, incluyendo la seguridad informática, la seguridad TIC y la seguridad de los datos.

- ✓ **Seguridad informática:** "Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información segura y confiable."(Aguilera López, Purificación, 2010).

- ✓ **Mecanismos de seguridad:** Todo aquello de naturaleza hardware como software que se utiliza para crear, reforzar y mantener la seguridad informática.

5.3 MARCO LEGAL

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. La cual habla sobre:

De los atentados contra la disponibilidad, confidencialidad e integridad de los datos y sistemas informáticos.

- **Artículo 269A:** Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y

ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- **Artículo 269B:** Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- **Artículo 269C:** Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- **Artículo 269D:** Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- **Artículo 269E:** Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- **Artículo 269F:** Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269G:** Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute,

programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

- **Artículo 269H:** Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  De los atentados informáticos y otras infracciones.

- **Artículo 269I:** Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

- **Artículo 269J:** Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

  Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

5.4 MARCO CONTEXTUAL

Se demarca claramente el entorno donde se desarrollara el proyecto, los entes vinculados y la distribución actual de las instalaciones pertenecientes a ASSALUD, quien es la IPS a la cual se le aplicara todos los conceptos manejados en este proyecto

5.4.1 Quienes Somos Es una Asociación de Prestadores de Servicios y Suministros de Salud: ASSALUD, constituida como entidad sin ánimo de lucro el 27 de agosto del 2001.

Tiene como Objetivo Social en la prestación de servicios de salud en todos los componentes y factores, tales como la educación, fomento, prevención, tratamiento y rehabilitación de la salud y el suministro de medicamentos.

En ASSALUD, cuenta con el mejor equipo de trabajo, compuesto por personal idóneo, enfocado en el crecimiento continuo, y en la excelencia del servicio, teniendo en cuenta que el bienestar y la seguridad de los usuarios es nuestro principal objetivo. [1]

5.4.2 Ubicación y Cobertura ASSALUD IPS dentro de sus zonas de operación, cuenta con puntos de atención en 14 Departamentos del país, ubicados así:

- Hace presencia en tres (3) regiones del país.
- Cuenta con Puntos de Atención en catorce (14) departamentos.
- Presta servicio en 173 Puntos de Atención Farmacéutica y cuenta con once (10) IPS, distribuidas en IPS BÁSICAS y CENTROS DE REFERENCIA DIAGNÓSTICA C.R.D.

[1] tomado de http://www.assalud.com/

Imagen: Cobertura de Zonas de Operaciones

Fuente: Registro fotográfico página web

5.4.3 Descripción De La Empresa

Imagen: Foto IPS Assalud Corozal

Fuente: Registro fotográfico tomado de la Empresa

Imagen: Foto IPS Assalud Corozal Planta de Trabajo

Fuente: Registro fotográfico tomado de la Empresa

ASSALUD IPS COROZAL, es una institución nacional que presta servicios de salud de I y II nivel de complejidad en las áreas de consulta externa ambulatoria y servicios de promoción y prevención en salud, creada para la atención integral en salud de sus afiliados.

Se encuentra certificada por el Departamento Administrativo de Seguridad Social en Salud Sucre (DASSALUD) por cumplir con los requisitos esenciales para servicios de salud de II nivel, bajo el código prestador numero 7021501191-01.

Inscrita en el sistema de Vigilancia en Salud Pública del Municipio de Sincelejo como unidad notificadora, identificada en la DIAN con el NIT No. 804011768-1.

Sus instalaciones están ubicadas en el municipio de Corozal en la calle 30 Nº 23-18 Barrio San Miguel, teléfonos: 2857233 / 3212042403, correo electrónico assalud.corozal@gmail.com.

Cuenta con una infraestructura física amplia y confortable para sus usuarios y empleados; equipos médicos, odontológicos y de procedimientos básicos adecuados para la prestación de sus servicios; equipo de profesionales de la salud idóneos, altamente calificados, con valores éticos y morales dispuestos a servir a la comunidad, bajo los principios de sentido social, calidad, actualización y planeación.[2]

[2] tomado de Portafolio de Servicios de Salud IPS Assalud

ASSALUD IPS COROZAL, tiene la finalidad de prestar servicios de salud en todos sus componentes y factores tales como educación, asistencia, fomento, prevención, tratamiento y rehabilitación de la salud, y el suministro de medicamentos genéricos de primer nivel y de alto costo, apoyados en el talento humano, infraestructura física y financiera, como soporte para lograr la atención de las necesidades de nuestros clientes institucionales y el de nuestros colaboradores internos.

5.4.4 Servicios Ofertados

Servicios De Atención En Salud Básicos
Ofrece los medios para solucionar los problemas de salud de nuestros usuarios a través de una atención profesional con la más alta calidad científica, abarcando las fases de prevención, diagnóstico, Tratamiento y rehabilitación, así como actividades de educación en salud.

Medicina General

- Consulta externa

Medicina Especializada

- Ginecología
- Pediatría
- Medicina Interna
- Fonoaudiología
- Psicología
- Fisioterapia

Imagen: Foto Instalación de Consultorio Medicina Especializada

Fuente: Registro fotográfico tomado del Portafolio de Servicio

Odontología General

- Operatoria dental.
- Endodoncia y exodoncia.
- Control de placa.
- Aplicación de Sellantes, fluorización y profilaxis.
- Planificación, orientación, ejecución y evaluación de programas de salud oral con base en el Conocimiento de la comunidad.

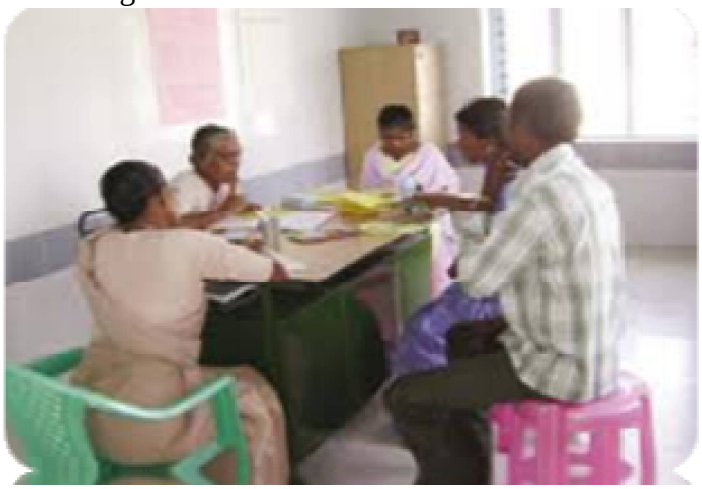
Imagen: Foto Instalación de Consultorio Odontología

Fuente: Registro fotográfico tomado del Portafolio de Servicio

Apoyo Multidisciplinario

- Nutrición
- Psicología
- Fonoaudiología
- Enfermería
- Fisioterapia

Imagen: Foto tomada Consultorio Nutrición



Fuente: Registro fotográfico tomado del Portafolio de Servicio

Apoyo Diagnostico:

Cuenta con la Red de Servicios en Salud como Laboratorio Clínicos Básico y Especializado, Imágenes Diagnosticas como ecografías obstétricas, ecografías especializadas I y II nivel de atención y electrocardiograma.

Imagen: Estudios Ecográficos Obstétricos

Fuente: Registro fotográfico tomado del Portafolio de Servicio

Promoción y Prevención

La IPS Assalud se anticipa a la aparición de enfermedades, es por eso que cuenta con atención preventiva de la Enfermedad como hipertensiva y diabetes, diseñados con base en las normas vigentes y ejecutadas con la intención transparente de generar un impacto positivo en la salud de nuestra población.

- Atención del adulto mayor hipertenso y diabético
- Inserción de implantes subdérmicos. (implanon)
- Programa de alto riesgo obstétrico

Imagen: Actividades de Promoción y Prevención “Control Prenatal”

Fuente: Registro fotográfico tomado del Portafolio de Servicio

Programa De Control De Enfermedades De Riesgo Cardiovascular

Ofrece una atención integral a los pacientes con Hipertensión Arterial y Diabetes Mellitus abarcando las fases de tamizaje, diagnóstico, tratamiento y seguimiento estricto por un equipo multidisciplinario conformado por personal altamente calificado en las áreas de Medicina General, Psicología, Enfermería, Médico Internista, Laboratorio Clínico, Nutrición y Dietética, Cultura Física y Rehabilitación Cardiovascular, buscando reducir las complicaciones, secuelas y mortalidad evitable en este grupo de pacientes mejorando además su calidad de vida.

Actualmente cuenta con un Programa de hipertensos y diabéticos dirigido a la población adulto mayor para la realización de actividad física y recreación.

Imagen: Foto Actividades Física para el control de enfermedades.

Fuente: Registro fotográfico tomado del Portafolio de Servicio

Programa De Rehabilitación Integral

Valoraciones Interdisciplinarias: realizadas por profesionales en el área de psicología, fisioterapia, fonoaudiología y terapia ocupacional los cuales se realizan de manera integral y diaria.

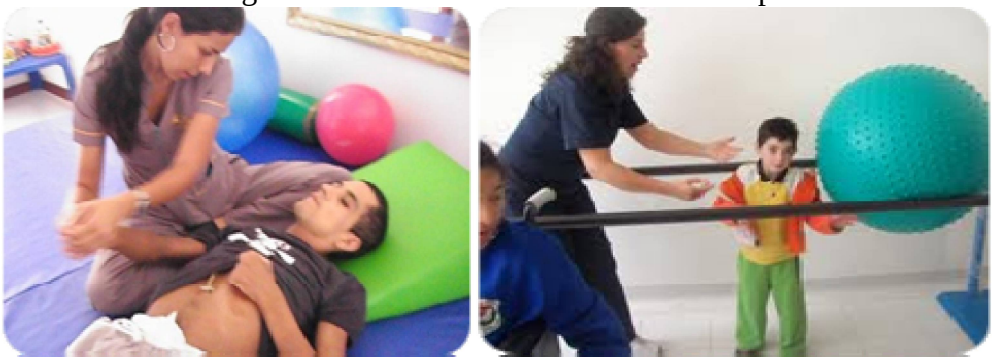
Tratamiento En El Área De Psicología: esta área interviene en las conductas, emociones, pensamientos disfuncionales trabajando en el proceso básico de aprendizaje y funciones ejecutivas de cada individuo.

Imagen: Programa de Rehabilitación Integral

Fuente: Registro fotográfico tomado del Portafolio de Servicio

Tratamiento En El Área De Fisioterapia: realizado por un profesional en el área el se base en el desarrollo de la kinecia y funcionalidad del cuerpo humano con capacitación y entrenamiento en ABA.

Imagen: Tratamiento en el Área de Fisioterapia



Fuente: Registro fotográfico tomado del Portafolio de Servicio

Tratamiento En El Área De Fonoaudiología: El profesional realiza terapias del lenguaje, habla y audición para la recuperación y prevención de trastornos en la comunicación con capacitación en análisis de comportamiento aplicado. [3]

[3] tomado de Portafolio de Servicios de Salud IPS Assalud

Imagen: Tratamiento en el Área de Fonoaudiología

Fuente: Registro fotográfico tomado del Portafolio de Servicio

Laboratorio Clínico: Brinda cumplimiento a la realización de laboratorios clínico de I y II nivel de atención además de procesamiento de tomas muestras de ambos niveles ofreciendo una entrega oportuna al paciente y demostrando la satisfacción del mismo .

Esta Sede cuenta 26 empleados de nomina y de contratos de los cuales 8 son Personal Administrativos y 18 Personal Asistencial ubicado en las siguientes dependencias:

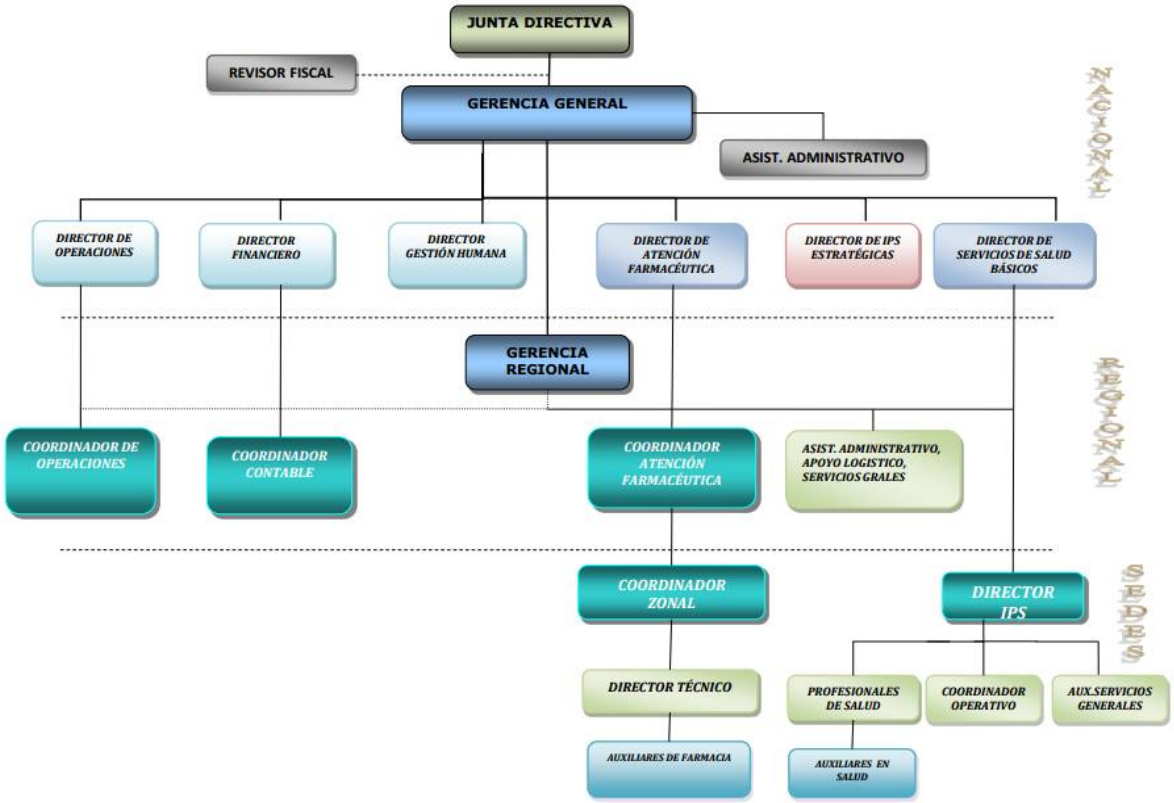
Tabla 1: Dependencias y Consultorio/Oficinas

Dependencias	Consultorios / Oficinas
Personal Asistencial	Medicina Especializada
	Medicina General
	Bacteriología
	Odontología
	Fisioterapia
	Fonoaudiología
	Psicología
	Auxiliares
Personal Administrativos	Coordinación Medica
	Ingeniero de Sistemas
	Facturación
	SIAU
	Auxiliares
	Recepción
	Contabilidad

Fuente: Información entregada en la entidad.

5.4.5 Organigrama

5.4.5.1 Organigrama General de la Empresa



Fuente: Información entregada en la entidad.

5.4.6 Plataforma Estratégica

Misión

Contribuye al bienestar social brindando servicios de alta calidad que aportan a la conservación y restablecimiento de la salud de nuestros usuarios, apoyados en personal calificado, seguridad y transparencia administrativa como pilar fundamental de la organización.

Responsabilidad, credibilidad y confianza, encausan nuestro esfuerzo hacia el desarrollo integral de nuestros colaboradores y la participación en acciones que generen bienestar social y mejoramiento de la calidad de vida de la población.[4]

Visión

Lograr el posicionamiento como líder nacional en el sector farmacéutico y de prestación de servicios de salud; a través de la incursión en nuevos mercados, capacitación permanente de nuestros colaboradores, la mejora continua de procesos administrativos y el soporte para la prestación de servicios de alta calidad a nuestros usuarios.[5]

Valores

- Compromiso: Se comprometen a mejorar continuamente nuestras aptitudes y actitudes.
- Servicio: Viven el servicio como una actitud, en la que dan todo para brindar lo mejor a los demás.
- Honestidad: Actúan de acuerdo a los valores morales y éticos de la sociedad.
- Sensibilidad: Entiende las vivencias y problemáticas de sus usuarios, esto los impulsa a ofrecer la mejor atención.
- Responsabilidad: Actúan responsablemente frente a los procesos, cumpliendo así las exigencias de nuestros usuarios.
- Pertenencia: Nos sentimos parte importante de la organización y en el éxito de sus objetivos.
- Trabajo en equipo: Juntos constituyen un todo en el que cada uno es importante en el crecimiento de la organización.[6]

Políticas De La Empresa

Política de Calidad.

Tienen como compromiso de prestar servicios de atención farmacéutica y de salud de altos estándares de calidad, que cumplan con especificaciones de oportunidad, confiabilidad y agilidad a costos razonables, para lograr la satisfacción y confianza de nuestros clientes internos y externos.

Para tal fin trabajan integralmente con el apoyo de personas de amplia capacidad humana y técnica, así como diversos recursos que orientan nuestros procesos hacia el mejoramiento

continuo, a partir de la retroalimentación de la información interna y la percepción del cliente sobre el servicio prestado.[7]

Política de Seguridad y Salud en el Trabajo.

ASSALUD es una empresa dedicada a la prestación de servicios de salud cuya misión está orientada a Contribuir al bienestar social brindando servicios de alta calidad que aportan a la conservación y restablecimiento de la salud de nuestros usuarios, apoyados en personal calificado, seguridad y transparencia administrativa como pilar fundamental de la organización.

ASSALUD cumple con los requisitos legales y aplicables, está comprometida con la promoción de la salud de sus colaboradores, contratistas y visitantes en general, para mantener su integridad física y mental mediante el control de los peligros, el mejoramiento de las prácticas laborales y su sensibilización en mantener un ambiente sano, seguro y un medio ambiente protegido, integramos a las partes interesadas y destinamos los recursos necesarios para el logro de los objetivos del sistema de seguridad y salud en el trabajo.

Los programas desarrollados en ASSALUD están orientados a fomentar una cultura preventiva y de auto cuidado, a la intervención de las condiciones de trabajo que puedan causar accidentes o enfermedades laborales, al control del ausentismo y a la prevención, atención y manejo de emergencias.

Todos los empleados, contratistas y visitantes tienen la responsabilidad de cumplir con las normas y procedimientos de seguridad, con el fin de realizar un trabajo seguro y productivo. Igualmente son responsables de notificar oportunamente todas aquellas condiciones que puedan generar consecuencias y contingencias para los colaboradores y visitantes de la empresa en general.[8]

[4, 5, 6, 7,8] tomado de http://www.assalud.com/

6 DISEÑO METODOLÓGICO

6.1 TIPO DE INVESTIGACIÓN

La línea de investigación contemplada en esta Monografía, se enmarcan en el diseño de un sistema de gestión de seguridad de la información, para la IPS ASSALUD de Corozal – Sucre, según los objetivos definidos y las necesidades presentadas por la IPS, utilizando como guía la Metodología MAGERIT y la Norma ISO 27001.

La metodología de investigación a utilizar será de campo, la cual permitirá corroborar el estado actual del sistema de información con el que cuenta la IPS ASSALUD, partiendo de la identificación de sus activos y verificando que amenazas son propensas y como deberán ser manejadas en caso de materializarse.

6.2 LÍNEA DE INVESTIGACIÓN

Tomando como referencia la metodología MAGERIT y la norma ISO 27001:2013, la línea de investigación de este proyecto se enmarcara en:

- Análisis y Gestión de Riesgos en los Activos.

6.3 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Para el desarrollo de esta monografía se planea usar las fuentes bibliográficas relacionas con el tema de este estudio. Tomando como bases, servicios de internet, manuales, tesis y todos los elementos documentales existentes tanto físicos como electrónicos, que ayuden a investigar y conocer los antecedentes relacionados con este contenido.

De igual manera, se utilizara la observación directa y entrevistas con el personal del área tecnológica, permitiendo conocer más a fondo el área tecnológica.

6.4 POBLACIÓN

Esta Monografía se realizara en las instalaciones de la IPS ASSALUD, ubicada en la ciudad de Corozal - Sucre.

6.5 MUESTRA

Actualmente existen en 26 empleados, de los cuales 18 son Personal Asistencial “Médicos, Enfermera, Bacterióloga, Auxiliares de enfermería, Odontóloga, Higienista Ora y Auxiliares de Laboratorio Clínico” y 8 Personal Administrativos “Coordinador Médico, Secretaria, Coordinador SIAU, Ingeniero de Sistemas, Auxiliar de Sistemas, Facturador y Auxiliar Contable”, estos estarán involucrado en el desarrollo de la investigación propuesta.

7 METODOLOGÍA DE DESARROLLO

Para el desarrollo de los objetivos del proyecto es necesario abordar 4 fases específicas con acciones que ayudaron a dar una solución al problema plantado las cuales se definirán a continuación.

Fase 1: Identificar, clasificar y valorar los activos con los que cuenta el sistema de información de la IPS ASSALUD aplicando la metodología MAGERIT

En esta fase se desarrolló un diagnostico general que permite identificar claramente todos los activos de información con los cuales cuenta la empresa, además el estado en el cual se encuentra cada activo, tanto físico como funcional como su relevancia para mantener el sistema de información en funcionamiento, los elementos que se desarrollaron en esta fase son:

- Aplicar encuesta para conocer el estado actual del sistema de información y los conocimientos que se tiene sobre la seguridad informática.

- Realizar recorrido en toda la IPS ASSALUD, e inventariar de sistemas informáticos, haciendo énfasis en los activos relevantes para el sistema de información.

- Clasificar los activos encontrados en la IPS ASSALUD, y enmarcarlos en los grupos definidos por la Metodología Magerit v3.

- Con los datos obtenidos en las entrevistas y durante el recorrido, se procederá hacer la valoración de todos los activos clasificados según su relevancia para el sistema de información.

- Registrar toda la información obtenida en la herramienta PILAR

Fase 2: Identificar y valorar las amenazas presentes en los activos del sistema de información de la IPS ASSALUD aplicando la metodología MAGERIT.

En esta fase del proyecto se identificaron claramente las amenazas presentes a cada uno de los activos, y a su vez se realizaron una valoración del impacto producido en caso de que

esa amenaza sea materializada, todo esta fase se realizara mediante la herramienta PILAR, y los procesos ejecutados para consolidarla son los siguientes:

- Una vez registrada la información en la herramienta PILAR, se procede a identificar las amenazas que recaen sobre cada activo, para llevar a cabo este proceso se utilizara la herramienta PILAR, la cual arrojara de forma automática según la clasificación y valoración que se le dio a cada activo una serie de amenazas, las cuales según las circunstancias y el conocimiento que se tiene sobre el sistema de información, deberán ser ampliadas o reducida por cada activo según sea el caso.

- Luego de identificadas las amenazas se procede a realizar su valoración directamente sobre cada activo en la herramienta PILAR

Fase 3: Gestionar los riegos y especificar salvaguardas, que permitan controlar los riesgos posibles en la IPS ASSALUD, según lo dispuesto en la metodología MAGERIT.

Esta fase es la última de la aplicación de la metodología de Magerit, en ella se consolido todo el trabajo desarrollado en las fases anteriores y como resultado arroja, en primera instancia un riesgo residual, el cual marca la minimización de las amenazas que pudieron ser gestionadas, y en segunda instancia un listado de salvaguardas que se deberán aplicar en caso de materialización de una amenaza.

- Este proceso se realizara automáticamente mediante el algoritmo que posee la herramienta PILAR y arrojara un listado de salvaguardas que permiten mitigar las amenazas en caso de materialización, además nos ofrece un esquema valorativo de los riesgos residuales presentes luego de la gestión del riesgo y definición de las salvaguardas.

Fases 4: Crear un Sistema de Políticas de Seguridad que permita optimizar el sistema de seguridad de información manejado actualmente en la IPS ASSALUD.

La fase final del desarrollo de este proyecto se enmarca en la creación de políticas de seguridad que se alcanzaron luego de aplicar completamente la metodología Magerit, lo que mantendrá un sistema de información más seguro y confiable, y evitara posibles amenazas a los activos con los que cuenta la empresa. Dentro de los procesos a desarrollar para obtener las políticas de seguridad necesarias se enmarcan:

- Definir políticas de seguridad que permitan mantener el sistema de seguridad a salvo, basado en las amenazas presentes en el sistema de información.

- Definir los alcances de las políticas de seguridad a implementar y los responsables de su monitoreo, como también las personas que se verán afectadas con su implementación.

- Crear el listado de políticas de seguridad factibles para la IPS ASSALUD.

- Socializar en toda la IPS el Sistema de Políticas de Seguridad Informática definido para mantener el sistema de seguridad a salvo de posibles amenazas.

8 DESARROLLO FASE 1

8.1 VULNERABILIDADES EN EL SISTEMA INFORMÁTICA DE LA IPS ASSALUD.

Con base en las consultas hechas es necesario identificar las diferentes partes críticas en las cuales se puede vulnerar la seguridad de un sistema: como los puntos de red, las redes inalámbricas, el Servidor de Aplicaciones, las estaciones de trabajo, otros sistemas y el personal de trabajo, como estos activos se pueden establecer los principales pasos para definir un SGSI.

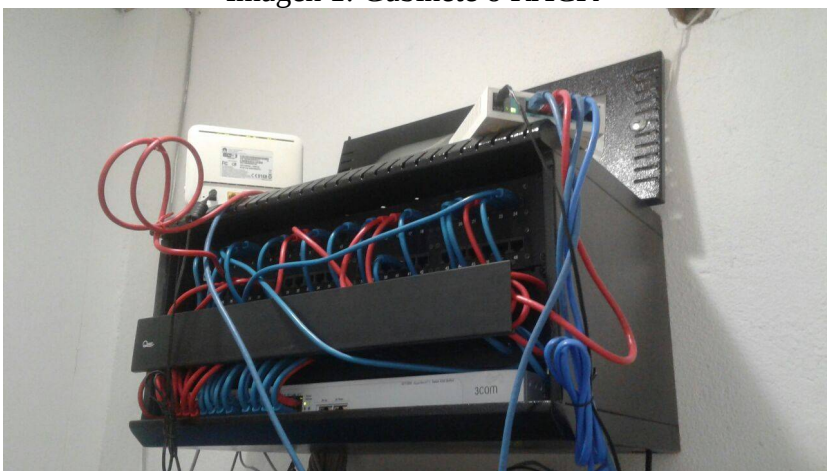
Las amenazas que se pueden surgir y las vulnerabilidades que se den por el descuido de lo anterior, abren paso a que los atacantes las exploten ya que es sabido que no hay un sistema 100% efectivo, por lo cual es indispensable tener estos puntos críticos controlados por la inmensa cantidad de incidencias del exterior y del interior de IPS Assalud.

Partes Críticas del Sistemas:

- Debilidad en el diseño de protocolos utilizados en las redes: No existe un Router que ayude administrar la seguridad del tráfico de datos en la red a través de protocolos de enrutamientos.

  En la siguiente imagen se observa que la red de datos solo se encuentra conectado dos dispositivos entre si un Swich y un Modem del proveedor de servicios de internet, lo cual indica que no hay una un control de seguridad en el trafico de los datos que circulan en la red que brinde una garantía de seguridad.

Imagen 1: Gabinete o RACK

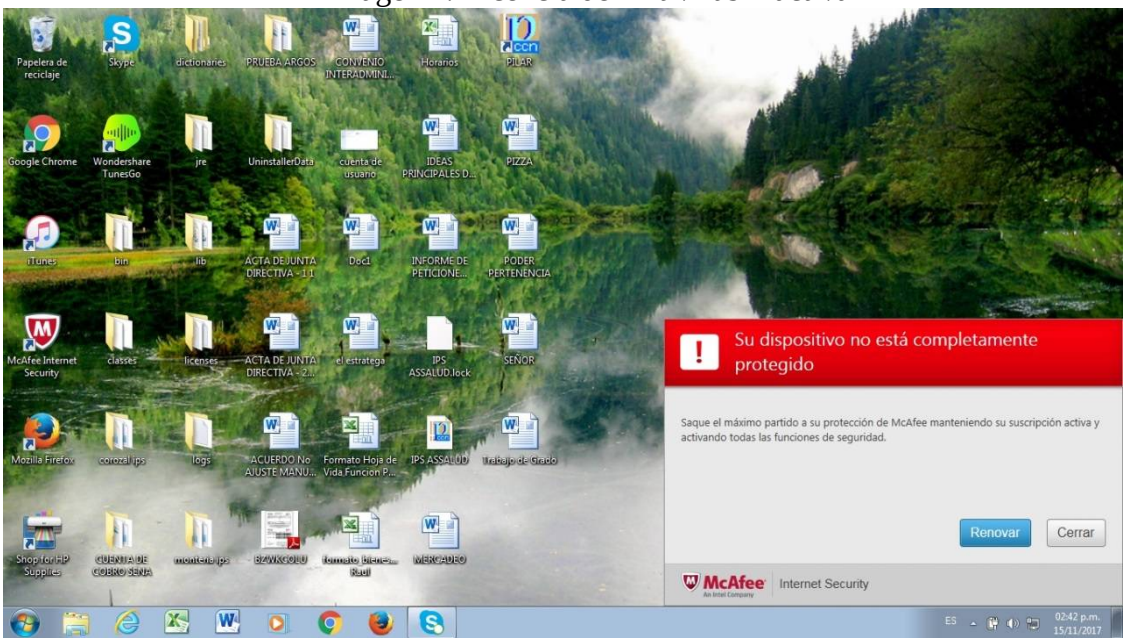


Fuente: Registro fotográfico tomado del Cuarto de Comunicaciones

- Mala configuración de los sistemas informáticos en seguridad. Los PC Mantienen instalado antivirus sin ningún tipo de licencia activa, lo cual hace que el PC no se encuentre completamente protegido ante algún tipo de ataque por virus.

  En la siguiente imagen se observa como los PC no mantiene una protección activa de cualquier ataque, la licencias se encuentran caducada.

Imagen 2: Licencia de Antivirus Inactiva

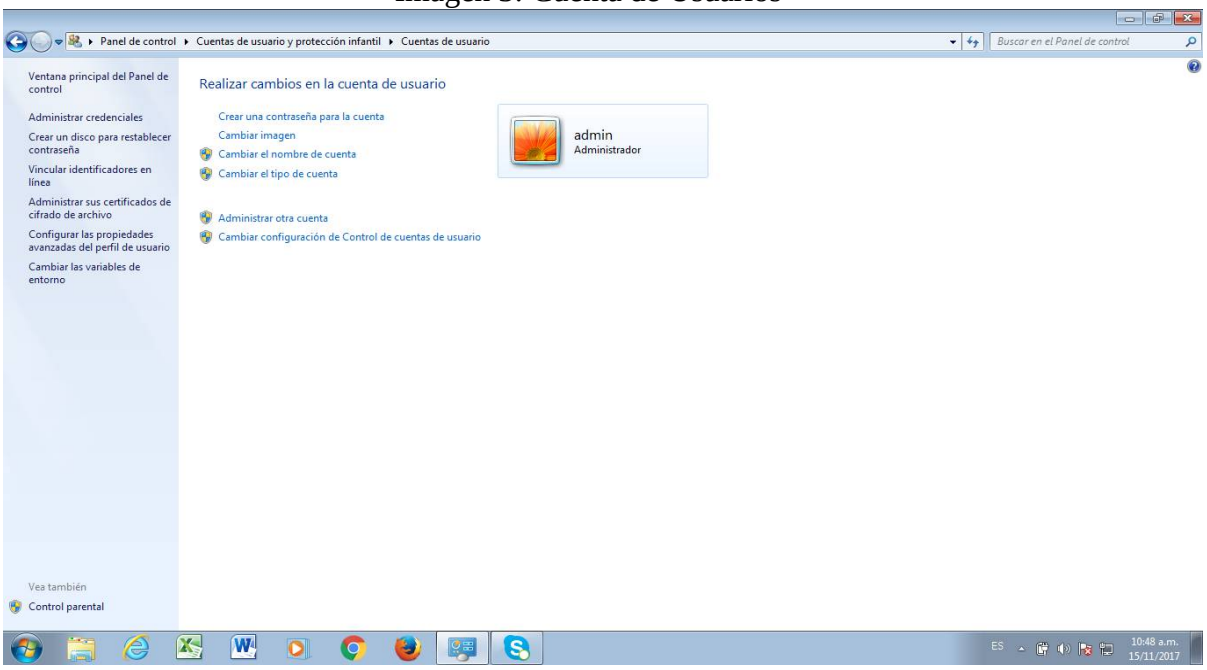


Fuente: Registro fotográfico tomado de PC de Oficina

- Debilidad en el control de acceso a los PC: No existen cuentas de usuarios definidas para los empleados, cualquier persona de la empresa puede tener el control de algunos de los PC de la empresa fácilmente.

  En la siguiente imagen se observan que todos los PC de la IPS no tienen creado un usuario y contraseña de acceso todos pueden ingresar con el perfil de administrador.

Imagen 3: Cuenta de Usuarios



Fuente: Registro fotográfico tomado de PC de Oficina

- Inseguridad en el Cuarto de Comulaciones: Este sitio no brinda las mejores medidas de seguridad para los dispositivos de la Red, la puerta de acceso al Cuarto de comunicaciones es insegura no tiene una cerradura que garantice su protección, en este cuarto también es utilizado para guardar insumos de la IPS y no cumple con los requerimientos de la norma de cableado estructurado en cuento a la organización del cableado red y eléctrico.

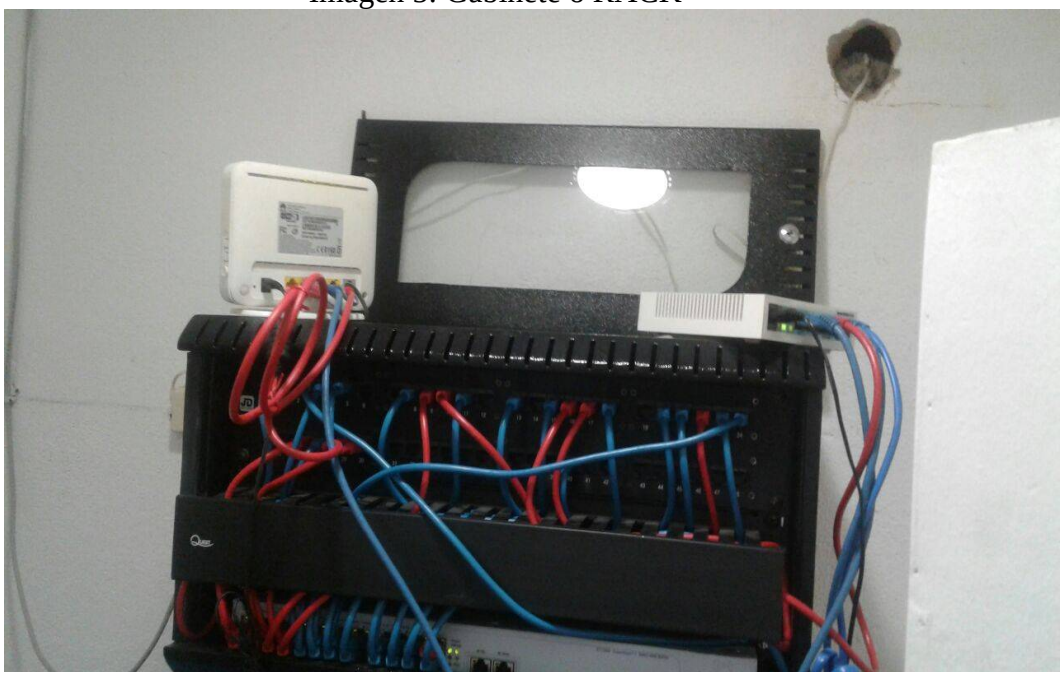
  En la siguiente imagen de observa como el Servidor de Aplicaciones se encuentra ubicado en el piso no hay una mesa o soporte para mantenerlo protegido de cualquier evento que se presente en este sitio.

Imagen 4: Servidor de Aplicaciones

Fuente: Registro fotográfico tomado de Cuarto de Comunicaciones

En la siguiente imagen se observa, el desorden que hay en la RACK hay muchos cables de red sueltos y dispositivos de red sin protección.

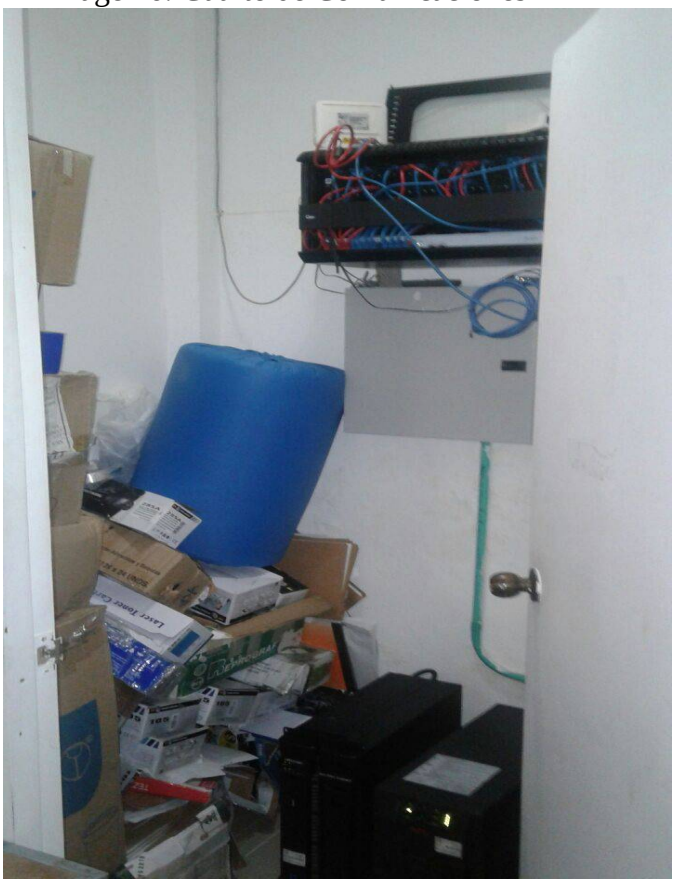
Imagen 5: Gabinete o RACK



Fuente: Registro fotográfico tomado de Cuarto de Comunicaciones

En la siguiente imagen se observa, que el cuarto de comunicaciones no solo está destinado para dispositivos de red, también es utilizado para guardar insumos de la IPS.

Imagen 6: Cuarto de Comunicaciones



Fuente: Registro fotográfico tomado de Cuarto de Comunicaciones

- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.

- La denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

- Políticas de seguridad deficiente e inexistente.

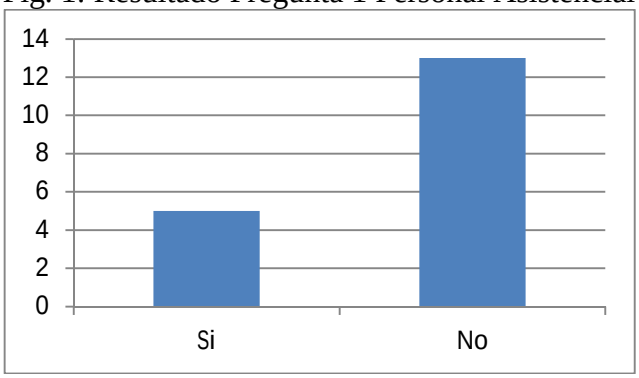
Una vez de haber identificado las partes críticas de la IPS Assalud, se realizo un sondeo a través de unas encuestas las cuales indicaron claramente en un gran porcentaje tanto el personal Asistencial como el personal Administrativo los cuales si consideran de alta importancia la seguridad informática, pero no saben sobre el tema, al igual que la información que se maneja dentro de las red de dato no es exclusivamente de la IPS, si de carácter personal. Así como las actividades desarrolladas suelen ser diferentes de los temas de su labor, por ejemplo Redes Sociales, Descargas de información (Música, juegos entre otros) lo que claramente incrementan los riesgos y posibles amenazas ya estudiadas con anterioridad.

Esto nos indica algo que se confirma durante el estudio, la Empresa en general no conoce siquiera si hay políticas de seguridad informática implementadas, si hay reglas claras que se deben cumplir cuando se está en la red o se utilizan los recursos de la IPS Assalud por lo que cualitativamente los encuestados respondieron en general que "No nos sentimos seguros", es decir no conocen las pautas claras que deben haber y se sienten en riesgo al navegar sobre los sistemas de la IPS, los resultados fueron prácticamente los mismos en toda las dependencia de la IPS, objeto de estudio.

Se va a mencionar los resultados de las preguntas más relevantes para el proyecto del Personal Asistencial:

1. ¿Conoce o ha escuchado sobre Seguridad Informática?

Fig. 1: Resultado Pregunta 1 Personal Asistencial

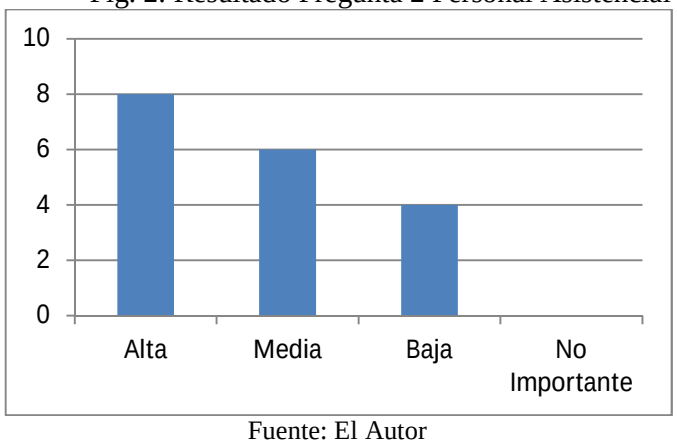


Fuente: El Autor

Se puede apreciar que el 80% del Personal Asistencial no conoce el tema de seguridad informática. Por tal razón no saben dar solución a un problema informático que se presente el su labor diaria.

2. ¿Qué tan importante le parece la seguridad informática?

Fig. 2: Resultado Pregunta 2 Personal Asistencial

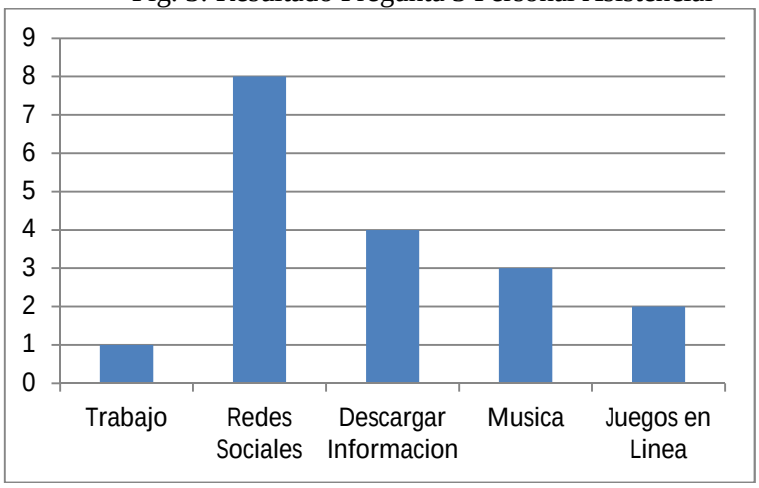


Fuente: El Autor

Un 22% del personal asistencial no les paceré muy importe este tema ya que solo se limitan a realizar su labor diaria en la IPS, el otro 78 % de personal si consideran importante este tema debe ser prioritario, pero piensan que no se está aplicando cuando trabajan en un computador.

3. ¿En su tiempo libre qué actividades realiza con los recursos informáticos de la IPS Assalud?

Fig. 3: Resultado Pregunta 3 Personal Asistencial

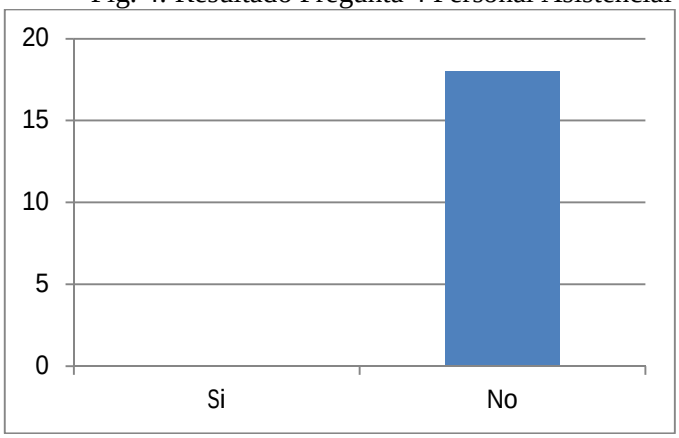


Fuente: El Autor

Se puede observar que no solo dentro de la IPS Assalud se utilizan los Recursos informáticos para su labor diaria, también para otras actividades que pueden acrecentar los peligros de ataques informáticos al Sistema de Información.

4. ¿Conoces las Políticas de Seguridad Informáticas implementadas en la IPS Assalud?

Fig. 4: Resultado Pregunta 4 Personal Asistencial



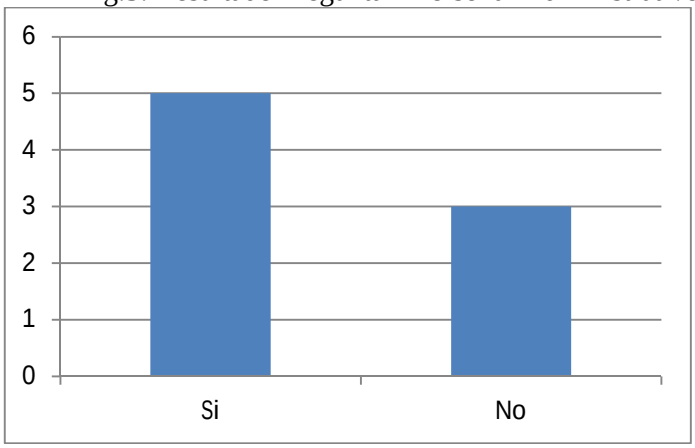
Fuente: El Autor

Ninguno de los Médicos, Bacteriólogo, Odontólogo, Auxiliares encuestados no saben si hay políticas por parte de la institución, lo que demuestra que si las hay, no se están difundiendo adecuadamente al personal Asistencial de la IPS Assalud.

Resultados de las preguntas más relevantes para el proyecto al Personal Administrativo:

1. ¿Conoce o ha escuchado sobre Seguridad Informática?

Fig.5: Resultado Pregunta 1 Personal Administrativo

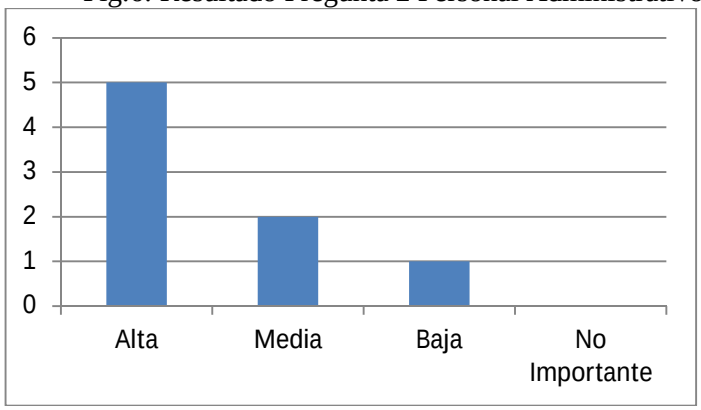


Fuente: El Autor

En este punto los empleados de la IPS Assalud han escuchado un poco más sobre el tema, ya que ellos son un poco cuidadosos con la información que procesan.

2. ¿Qué tan importante le parece la seguridad informática?

Fig.6: Resultado Pregunta 2 Personal Administrativo

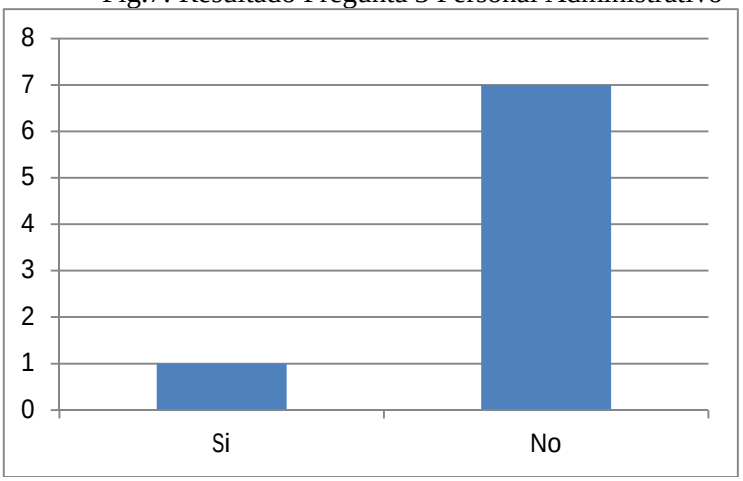


Fuente: El Autor

El personal Administrativo tienden a darle un poco importancia a este tema, ya que algunos de ellos tienden a darle prioridad a la información evitando pérdida o daño en la misma.

3. ¿Conoces las Políticas de Seguridad Informáticas implementadas en la IPS Assalud?

Fig.7: Resultado Pregunta 3 Personal Administrativo



Fuente: El Autor

Con relación a las políticas de Seguridad de la información en la empresa, el personal del área administrativa no ha recibido las indicaciones o parámetros a seguir para mantener la información segura y saber enfrentar un problema que se presente.

A lo anterior cabe aclarar que la información recolectada es de manera confidencial concertada con las personas entrevistadas por lo que no se dará a conocer los resultados explícitos, pero si se pueden sacar algunas conclusiones:

- Las políticas son desarrolladas por el área de sistemas, no se han contratado personas o empresas expertas en el tema para implementarlas.
- En la IPS Assalud sí consideran importante la seguridad informática, pero no se está implementando un esquema de seguridad de información.
- En la IPS Assalud ya han ocurrido incidentes como pérdida de información por los altos riesgos a los que se exponen.

En resumen del trabajo de campo:

Tabla 2: Población Encuestada

Empresa	Encuestas Personal Asistencial	Encuestas Personal Administrativos
Assalud IPS	18	8

Fuente: El Autor

8.2 IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT

Dentro del análisis de riesgo se utilizó la Metodología Magerit, mediante la herramienta ear/pilar en su versión 6.2, la cual ayuda a minimizar los riesgos que tiene un Sistema de Información, tiene una serie de etapas que se detallan a continuación:

8.3 IDENTIFICACIÓN DE ACTIVOS

La IPS ASSALUD cuenta con cierto grupo de activos informáticos los cuales se detallan a continuación:

Tabla 3. Inventario de activos de la IPS ASSALUD

TIPO DE ACTIVO	ACTIVO	SERVICIO	SISTEMA OPERATIVO	CANTIDAD
Tangible	Switch 4200 26-Port 3COM	Intercomunicación de la red LAN		1
Tangible	MikroTik	Administración del trafico datos y servicio en la Red.		1
Tangible	Modem huawei	Brinda el Servicio de Internet. "Proveedor UNE"		1
Tangible	Red telefónica ADSL	Intercomunicación entre extensiones		1
Tangible	Red de cableado estructurado	Interconectividad de red		1
Tangible	Servidor Hp Proliant ML110 G7. PROCESADOR: 1 x Intel Xeon E3-1220 / 4.2 GHz (Quad-Core) RAM: 8 GB ALMACENAMIENTO: 1 Tera HDD (Disco Duro) GRAFICA: Matrox G200 UNIDAD OPTICA: Ninguna CONECTIVIDAD/PUERTOS: 8 x USB - 4 PIN USB tipo A (4 frontales, 4 traseras) CONTROLADORA RAID: Smart Array B110i NIVEL RAID: RAID 0, RAID 1, RAID 10	Servidor de Teléfonos IP	Linux Ubuntu	1
Tangible	Ups APC 3KVA	Sistema de alimentación ininterrumpida		2
Tangible	Computadores de escritorio Hp Compaq Pro 4300 PROCESADOR: Intel® Core™ i3-3220 Processor (3M Cache, 3.20 GHz) MEMORIA: 4 GB (1x 4GB) 1600 MHz DDR3 SDRAM 2 SODIMM DICO DURO: 500 GB		Windows 7 de 64 Bits Office 2007 Antivirus Kaspersky	14
Tangible	Computador portátil dell Inspiron 14z PROCESADOR: Intel Core i5		Windows 7 de 64 Bits Office 2007	2

	3317U (1700 MHz - 2600 MHz) MEMORIA: RAM: 6GB DDR3 (1333 MHz) DISCO DURO: HDD 500GB (5400rpm) mSATA 32GB.		Antivirus Kaspersky	
Tangible	Impresora de Red Kyocera Multifincional	Brinda servicio de impresión escaneo y copiado de documentos, se encuentra conectada en la Red de Datos.		1
Tangible	Impresora de Red Kyocera	Brinda servicio de impresión de documentos, se encuentra conectada en la Red de Datos.		1
Tangible	Impresara HP Laserjet P1606dn	Impresa conectada a tres equipos en el Área Farmacia		1
Tangible	Impresaro HP Laserjet 1100w	Impresa conectada a un solo equipo en el Área de Laboratorio Clínico.		1
Tangible	Teléfonos IP	Comunicación con el exterior e intercomunicación		9
Intangible	Servicio de internet	Navegación en internet		1
Intangible	Servicio WEB	Sistema de Información ProgSalud. Historias Clínicas, Asignación de Citas Médicas, Informes Estadísticos, Laboratorio Clínico	Instalado sobre plataforma Windows Server. Este Servidor se encuentra Instalación en la Nube con una licencia de Windows Server	1
Intangible	Bases de datos SQL Server Native Client	Registro de consultas, pacientes, citas médicas, resultado	Instalado sobre plataforma Windows	1

		de laboratorio clínico, entre otras	Server	
Intangible	Software Facturación	Generación de Facturas, Generación de RIPS, Planos Contables.	Instalado sobre plataforma Windows 7	1

Fuente: El Autor

Identificación de Activos según la Metodología MAGERIT, para el desarrollo de este proceso se utilizó el libro 2 de la metodología denominado catálogo de elementos (ver ANEXO A: libros metodología MAGERIT)

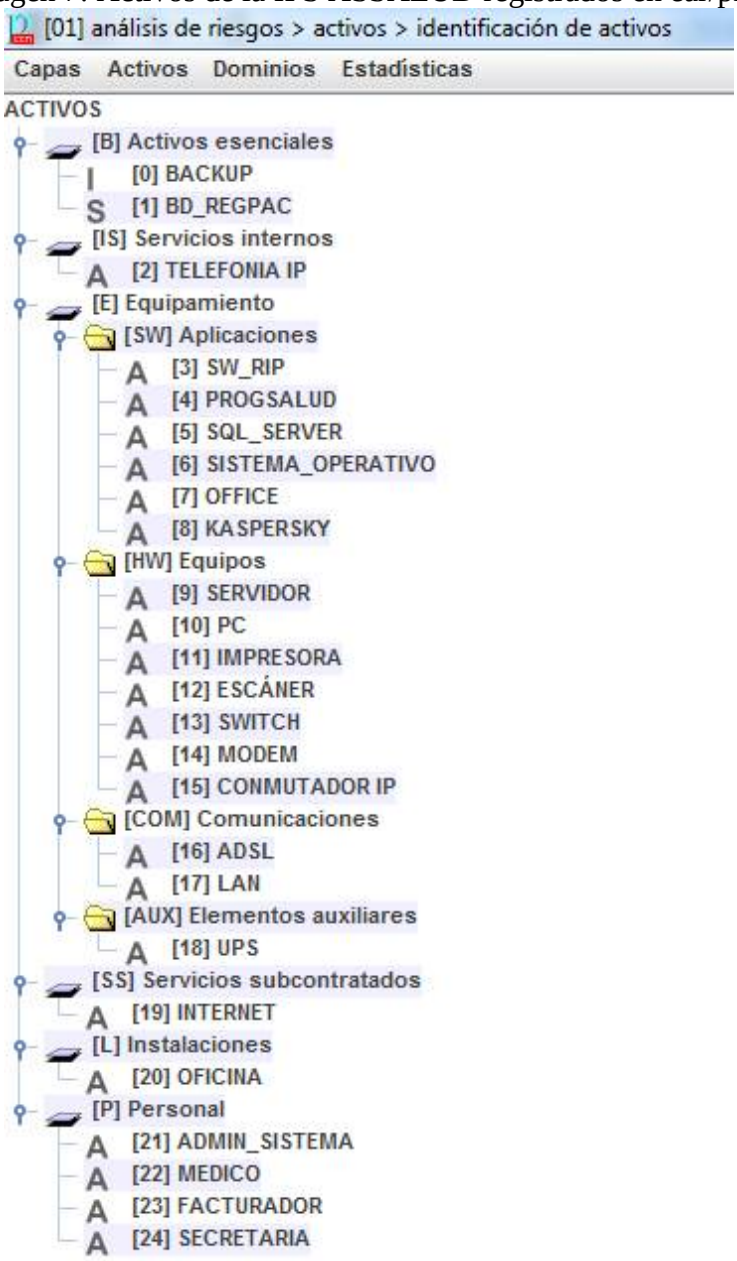
Tabla 4. Activos

TIPO	NOMBRE DEL ACTIVO
DATOS / INFORMACIÓN	0. [BACKUP] Copias de seguridad servidor y estaciones de trabajo
	1. [BD_REGPAC] registro de pacientes y facturación
SERVICIOS	2. [INTERNET] Conexión a internet
	3. [TELEFONIA IP] VOZ IP
APLICACIONES	4. [SW_RIP] registros contables y generador de facturas (RIP)
	5. [PROGSALUD] Plataforma administración de pacientes (citas médicas e historias clínicas, laboratorio)
	6. [SQL_SERVER] sistema de gestión de bases de datos relacionales
	7. [SISTEMA_OPERATIVO] Sistema Operativo Windows
	8. [OFFICE] office 2007
	9. [KASPERSKY] Anti virus
EQUIPAMIENTO INFORMÁTICO	10. [SERVIDOR] servidor principal registro contable
	11. [PC] Computadora de puestos de trabajo y consultorios
	12. [IMPRESORA] medios de impresión en red
	13. [ESCÁNER] escáner en red
	14. [SWITCH] Intercomunicación de la red LAN
	15. [MODEM] módems de acceso a internet brindado por UNE
	16. [CONMUTADOR IP] conmutador interno y externo telefónico
REDES DE COMUNICACIONES	17. [ADSL] Conexión a internet para telefonía IP
	18. [LAN] red local

EQUIPAMIENTO AUXILIAR	19. [UPS] sistemas de alimentación ininterrumpida de 3 KVA en el servidor de bases de datos
INSTALACIONES	20. [OFICINA] IPS ASSALUD COROZAL SAN MIGUEL-CENTRO
PERSONAL	21. [ADMIN_SISTEMA] ingeniero de sistemas a cargo
	22. [MEDICOS] personal médicos en general
	23. [FACTURADOR] Encargado de la generación de RIP
	24. [SECRETARIA] asignación de citas medicas

Fuente: El Autor

Imagen 7: Activos de la IPS ASSALUD registrados en ear/pilar



Fuente: El Autor

8.4 VALORACIÓN DE ACTIVOS

Para la valoración de los activos conviene tomar a consideración, La dimensiones en que el activo es relevante y la estimación de valoración de cada dimensión, para llevar a cabo este

proceso es necesario recurrir al libro 2 de la Metología de Magerit donde nos estipulan las 5 dimensiones en las que un activo debe ser valorado estas dimensiones son:

1. [D] **Disponibilidad**: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].

2. [I] **Integridad**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].

3. [C] **Confidencialidad**: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007].

4. [A] **Autenticidad** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008].

5. [T] **Trazabilidad**: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

Una vez comprendida las dimensiones se procede a establecer la valoración que MAGERIT nos sugiere teniendo en cuenta que este proceso será realizado en herramienta ear/pilar

Tabla 5. Valoración de las dimensiones según MAGERIT

VALOR		**CRITERIO**
10	EXTREMO	Daño extremadamente grave
9	MUY ALTO	Daño muy grave
6-8	ALTO	Daño grave
3-5	MEDIO	Daño importante.
1-2	BAJO	Daño menor.
0	DESPRECIABLE	Irrelevante a efectos prácticos.

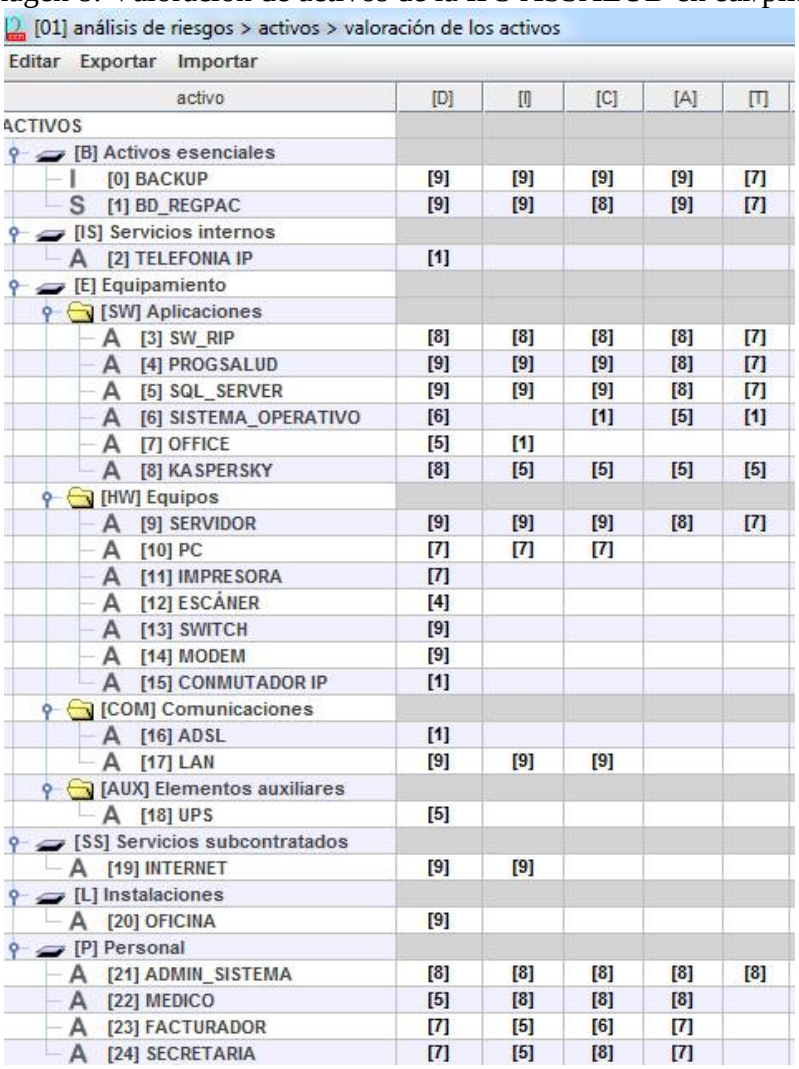
Fuente: El Autor

Tabla 6: Dimensionamiento de Activos

ACTIVOS	DIMENSIONAMIENTO				
DATOS / INFORMACIÓN	**D**	**I**	**C**	**A**	**T**
[BACKUP] Copias de seguridad servidor y estaciones de trabajo	9	9	8	9	7
[BD_REGPAC] registro de pacientes y facturación	9	9	8	9	7
SERVICIOS					
[INTERNET] Conexión a internet	9	9			
[TELEFONÍA IP] VOZ IP	1				
APLICACIONES					
[SW_RIP] registros contables y generador de facturas (RIP)	8	8	8	8	7
[PROGSALUD] Plataforma administración de pacientes (citas médicas e historias clínicas, laboratorio)	9	9	9	8	7
[SQL_SERVER] sistema de gestión de bases de datos relacionales	9	9	9	8	7
[SISTEMA_OPERATIVO] Sistema Operativo Windows	6		1	5	1
[OFFICE] office 2007	5	1			
[KASPERSKY] Anti virus	8	5	5	5	5
EQUIPAMIENTO INFORMÁTICO					
[SERVIDOR] servidor principal registro contable	9	9	9	8	7
[PC] Computadora de puestos de trabajo y consultorios	7	7	7		
[IMPRESORA] medios de impresión en red	7				
[ESCÁNER] escáner en red	4				
[SWITCH] Intercomunicación de la red LAN	9				
[MODEM] módems de acceso a internet brindado por UNE	9				
[CONMUTADOR IP] conmutador interno y externo telefónico	1				
COMUNICACIONES					
[ADSL] Conexión a internet para telefonía IP	1				
[LAN] red local	9	9	9		
Equipos Auxiliares					
[UPS] sistemas de alimentación ininterrumpida de 3 KVA en el servidor de bases de datos	5				
INSTALACIONES					
[OFICINA] IPS ASSALUD Corozal San Miguel-Centro	9				
Personal					
[ADMIN_SISTEMA] ingeniero de sistemas a cargo	8	8	8	8	8
[MEDICOS] personal médicos en general	5	8	8	8	
[FACTURADOR] Encargado de la generación de RIP	7	5	6	7	
[SECRETARIA] asignación de citas medicas	7	5	8	7	

Fuente: El Autor

Imagen 8: Valoración de activos de la IPS ASSALUD en ear/pilar



[01] análisis de riesgos > activos > valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[0] BACKUP	[9]	[9]	[9]	[9]	[7]
[1] BD_REGPAC	[9]	[9]	[8]	[9]	[7]
[IS] Servicios internos					
[2] TELEFONIA IP	[1]				
[E] Equipamiento					
[SW] Aplicaciones					
[3] SW_RIP	[8]	[8]	[8]	[8]	[7]
[4] PROGSALUD	[9]	[9]	[9]	[8]	[7]
[5] SQL_SERVER	[9]	[9]	[9]	[8]	[7]
[6] SISTEMA_OPERATIVO	[6]		[1]	[5]	[1]
[7] OFFICE	[5]	[1]			
[8] KASPERSKY	[8]	[5]	[5]	[5]	[5]
[HW] Equipos					
[9] SERVIDOR	[9]	[9]	[9]	[8]	[7]
[10] PC	[7]	[7]	[7]		
[11] IMPRESORA	[7]				
[12] ESCÁNER	[4]				
[13] SWITCH	[9]				
[14] MODEM	[9]				
[15] CONMUTADOR IP	[1]				
[COM] Comunicaciones					
[16] ADSL	[1]				
[17] LAN	[9]	[9]	[9]		
[AUX] Elementos auxiliares					
[18] UPS	[5]				
[SS] Servicios subcontratados					
[19] INTERNET	[9]	[9]			
[L] Instalaciones					
[20] OFICINA	[9]				
[P] Personal					
[21] ADMIN_SISTEMA	[8]	[8]	[8]	[8]	[8]
[22] MEDICO	[5]	[8]	[8]	[8]	
[23] FACTURADOR	[7]	[5]	[6]	[7]	
[24] SECRETARIA	[7]	[5]	[8]	[7]	

Fuente: El Autor

Los niveles de valoración y dimensiones utilizadas por la herramienta ear/pilar se enmarcan en la siguiente tabla, siendo los niveles 9 y 10, demasiado valioso y extremadamente valioso respectivamente.

Tabla 7: Niveles de Valoración y dimensiones ear/pilar

Nivel	Criterio
10	Nivel 10
9	Nivel 9
8	Alto (+)
7	Alto
6	Alto (-)
5	Medio(+)
4	Medio
3	Medio(-)
2	Bajo (+)
1	Bajo
0	Depreciable

Dimensiones	
D	Disponibilidad
I	Integridad de Datos
C	Confidencialidad
A	Autenticidad
T	Trazabilidad

Fuente: El Autor

9 DESARROLLO FASE 2

9.1 IDENTIFICACIÓN DE AMENAZAS

Para llevar a cabo la identificación de las amenazas y según lo expresado por el libro 2 "catálogo de elementos" de la metodología MAGERIT se deben enmarcar dentro de sus categorías, las cuales son:

- **[N] Desastres naturales**

✓ [N.1] Fuego
✓ [N.2] Daños por agua
✓ [N.*] Desastres naturales

- **[I] De origen industrial**

✓ [I.1] Fuego
✓ [I.2] Daños por agua
✓ [I.*] Desastres industriales
✓ [I.3] Contaminación mecánica
✓ [I.4] Contaminación electromagnética
✓ [I.5] Avería de origen físico o lógico
✓ [I.6] Corte del suministro eléctrico
✓ [I.7] Condiciones inadecuadas de temperatura o humedad
✓ [I.8] Fallo de servicios de comunicaciones
✓ [I.9] Interrupción de otros servicios o suministros esenciales
✓ [I.10] Degradación de los soportes de almacenamiento de la información
✓ [I.11] Emanaciones electromagnéticas

- **[E] Errores y fallos no intencionados**

✓ [E.1] Errores de los usuarios
✓ [E.2] Errores del administrador
✓ [E.3] Errores de monitorización (log)
✓ [E.4] Errores de configuración
✓ [E.7] Deficiencias en la organización
✓ [E.8] Difusión de software dañino
✓ [E.9] Errores de [re-]encaminamiento
✓ [E.10] Errores de secuencia
✓ [E.14] Fugas de información
✓ [E.15] Alteración de la información
✓ [E.16] Introducción de falsa información

- ✓ [E.17] Degradación de la información
- ✓ [E.18] Destrucción de la información
- ✓ [E.19] Divulgación de información
- ✓ [E.20] Vulnerabilidades de los programas (software)
- ✓ [E.21] Errores de mantenimiento / actualización de programas (software)
- ✓ [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- ✓ [E.24] Caída del sistema por agotamiento de recursos
- ✓ [E.25] Pérdida de equipos
- ✓ [E.28] Indisponibilidad del personal

- **[A] Ataques intencionados**
- ✓ [A.4] Manipulación de la configuración
- ✓ [A.5] Suplantación de la identidad del usuario
- ✓ [A.6] Abuso de privilegios de acceso
- ✓ [A.7] Uso no previsto
- ✓ [A.8] Difusión de software dañino
- ✓ [A.9] [Re-]encaminamiento de mensajes
- ✓ [A.10] Alteración de secuencia
- ✓ [A.11] Acceso no autorizado
- ✓ [A.12] Análisis de tráfico
- ✓ [A.13] Repudio
- ✓ [A.14] Interceptación de información (escucha)
- ✓ [A.15] Modificación de información
- ✓ [A.16] Introducción de falsa información
- ✓ [A.17] Corrupción de la información
- ✓ [A.18] Destrucción de la información
- ✓ [A.19] Divulgación de información
- ✓ [A.22] Manipulación de programas
- ✓ [A.24] Denegación de servicio
- ✓ [A.25] Robo de equipos
- ✓ [A.26] Ataque destructivo
- ✓ [A.27] Ocupación enemiga
- ✓ [A.28] Indisponibilidad del personal
- ✓ [A.29] Extorsión
- ✓ [A.30] Ingeniería social (picaresca)

Aplicando estos lineamientos a los activos identificados en la herramienta pilar obtenemos la siguiente identificación de amenazas sobre cada uno de los activos.

Tabla 8: Amenazas en los activos

ACTIVOS	AMENAZAS
[**BACKUP**] Copias de seguridad servidor y estaciones de trabajo	[E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado
[**BD_REGPAC**] registro de pacientes y facturación	[I.5] Avería de origen físico o lógico [E.8] Difusión de software dañino [E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.22] Manipulación de programas
[**INTERNET**] Conexión a internet	[I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.13] Repudio (negación de actuaciones) [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.24] Denegación de servicio
[**TELEFONÍA IP**] VOZ IP	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso

	[A.7] Uso no previsto [A.11] Acceso no autorizado [A.13] Repudio (negación de actuaciones) [A.15] Modificación de la información [A.18] Destrucción de la información [A.24] Denegación de servicio
[**SW_RIP**] registros contables y generador de facturas (RIP)	[I.5] Avería de origen físico o lógico [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas
[**PROGSALUD**] Plataforma administración de pacientes (citas médicas e historias clínicas, laboratorio)	[I.5] Avería de origen físico o lógico [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas
[**SQL_SERVER**] sistema de gestión de bases de datos relacionales	[I.5] Avería de origen físico o lógico [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas
[**SISTEMA_OPERATIVO**] Sistema Operativo Windows	[I.5] Avería de origen físico o lógico [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas
[**OFFICE**] office 2007	[I.5] Avería de origen físico o lógico [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas
[**KASPERSKY**] Anti virus	[I.5] Avería de origen físico o lógico [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas
[**SERVIDOR**] servidor principal registro contable	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales

	[I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.11] Emanaciones electromagnéticas [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo
[**PC**] Computadora de puestos de trabajo y consultorios	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.11] Emanaciones electromagnéticas [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo
[**IMPRESORA**] medios de impresión en red	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.11] Emanaciones electromagnéticas [E.23] Errores de mantenimiento / actualización de equipos (hardware)

	[E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo
[**ESCÁNER**] escáner en red	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.11] Emanaciones electromagnéticas [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo
[**SWITCH**] Intercomunicación de la red LAN	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.11] Emanaciones electromagnéticas [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo

[**MODEM**] módems de acceso a internet brindado por UNE	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.11] Emanaciones electromagnéticas [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo
[**CONMUTADOR IP**] conmutador interno y externo telefónico	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.11] Emanaciones electromagnéticas [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo
[**ADSL**] Conexión a internet para telefonía IP	[I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad

	[A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.24] Denegación de servicio
[**LAN**] red local	[I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.24] Denegación de servicio
[**UPS**] sistemas de alimentación ininterrumpida de 3 KVA en el servidor de bases de datos	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.7] Uso no previsto [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo
[**OFICINA**] IPS ASSALUD Corozal San Miguel-Centro	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto

	[A.26] Ataque destructivo [A.27] Ocupación enemiga
[**ADMIN_SISTEMA**] ingeniero de sistemas a cargo	[E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.28] Indisponibilidad del personal [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca)
[**MEDICOS**] personal médicos en general	[E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.28] Indisponibilidad del personal [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca)
[**FACTURADOR**] Encargado de la generación de RIP	[E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.28] Indisponibilidad del personal [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca)
[**SECRETARIA**] asignación de citas medicas	[E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.28] Indisponibilidad del personal [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca)

Fuente: El autor

9.2 VALORACIÓN DE IMPACTO EN LAS AMENAZAS

Para realizar la valoración de impacto en las amenazas de los activos, es necesario evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo y estimar la degradación que causaría en cada dimensión del activo que define MAGERIT. Para valorar las amenazas de cada activo se ha toma las siguientes tablas:

Tabla 9: Niveles de degradación de las dimensiones de un activo

NIVEL	PORCENTAJE
T - total	100%
MA - muy alta	90%
A – alta	50%
M – media	10%
B – baja	1%

Fuente: herramienta EAR/PILAR

Tabla 10: Probabilidad de materialización de la Amenaza ear/pilar

PROBABILIDAD	FRECUENCIA
CS - casi seguro	100
MA - muy alta	10
P – posible	1
PP - poco probable	0,1
MR -muy rara	0.01

Fuente: herramienta EAR/PILAR

Imagen 9: Valoración de Amenazas del activo BACKUP en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[B] Activos esenciales						
[0] BACKUP		B	M	A	T	
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		
[A.5] Suplantación de la identidad	MA		M	A	T	
[A.6] Abuso de privilegios de acceso	MA	B	M	A		
[A.11] Acceso no autorizado	CS		M	A		

Fuente: El Autor

Imagen 10: Valoración de Amenazas del activo BD_REGPAC en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
S [1] BD_REGPAC		T	T	T	T	
[I.5] Avería de origen físico o lógico	P	A				
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas	P	B	M	M		
[E.21] Errores de mantenimiento / actualiz	MA	B	B			
[A.5] Suplantación de la identidad	MA		M	A	T	
[A.6] Abuso de privilegios de acceso	MA	B	M	A		
[A.8] Difusión de software dañino	P	T	T	T		
[A.11] Acceso no autorizado	CS		M	A		
[A.22] Manipulación de programas	P	A	T	T		

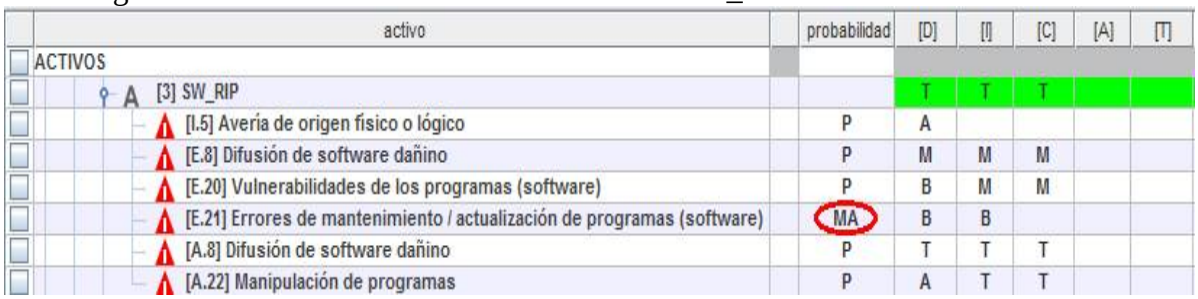
Fuente: El Autor

Imagen 11: Valoración de Amenazas del activo TELEFONIA IP en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
A [2] TELEFONIA IP		A	A	A	T	T
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sisten	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.24] Caída del sistema por agotamiento	MA	A				
[A.5] Suplantación de la identidad	P		A	A	T	
[A.6] Abuso de privilegios de acceso	P	B	M	M	T	
[A.7] Uso no previsto	P	B	M	M		
[A.11] Acceso no autorizado	P		M	A	T	
[A.13] Repudio (negación de actuaciones)	MA					T
[A.15] Modificación de la información	MA		A			
[A.18] Destrucción de la información	P	A				
[A.24] Denegación de servicio	MA	A				

Fuente: El Autor

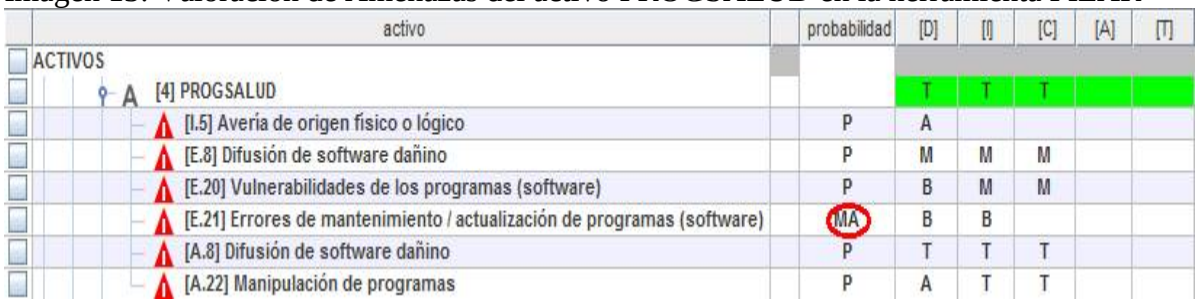
Imagen 12: Valoración de Amenazas del activo SW_RIP en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[3] SW_RIP		T	T	T		
[I.5] Avería de origen físico o lógico	P	A				
[E.8] Difusión de software dañino	P	M	M	M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.8] Difusión de software dañino	P	T	T	T		
[A.22] Manipulación de programas	P	A	T	T		

Fuente: El Autor

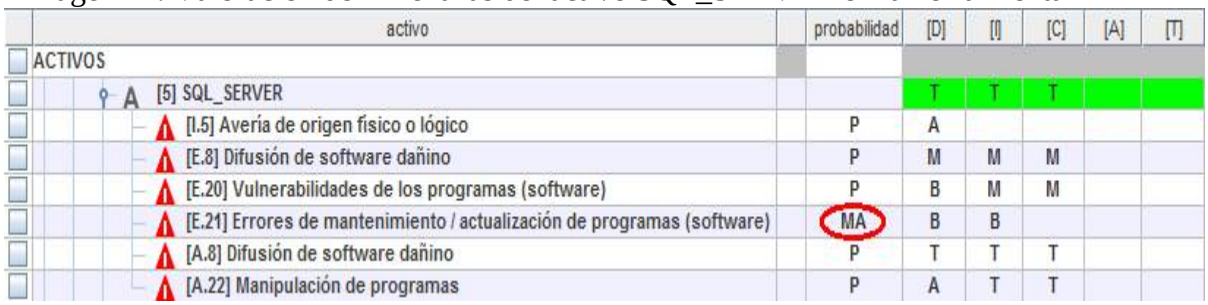
Imagen 13: Valoración de Amenazas del activo PROGSALUD en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[4] PROGSALUD		T	T	T		
[I.5] Avería de origen físico o lógico	P	A				
[E.8] Difusión de software dañino	P	M	M	M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.8] Difusión de software dañino	P	T	T	T		
[A.22] Manipulación de programas	P	A	T	T		

Fuente: El Autor

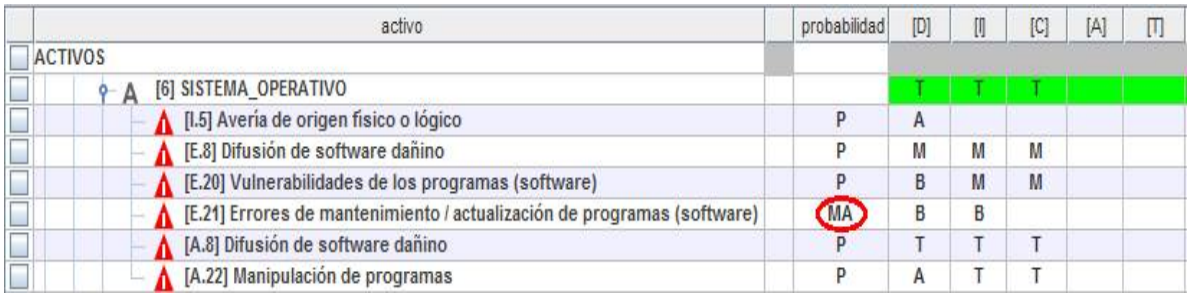
Imagen 14: Valoración de Amenazas del activo SQL_SERVER en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[5] SQL_SERVER		T	T	T		
[I.5] Avería de origen físico o lógico	P	A				
[E.8] Difusión de software dañino	P	M	M	M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.8] Difusión de software dañino	P	T	T	T		
[A.22] Manipulación de programas	P	A	T	T		

Fuente: El Autor

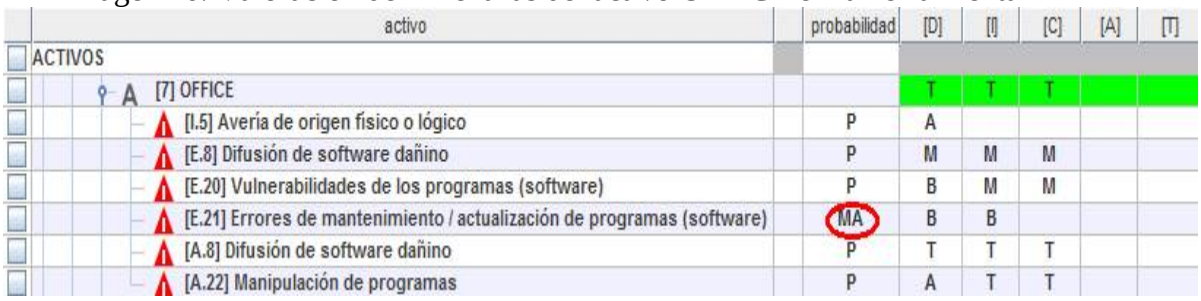
Imagen 15: Valoración de Amenazas del activo SISTEMA_OPERATIVO en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[6] SISTEMA_OPERATIVO		T	T	T		
[I.5] Avería de origen físico o lógico	P	A				
[E.8] Difusión de software dañino	P	M	M	M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.8] Difusión de software dañino	P	T	T	T		
[A.22] Manipulación de programas	P	A	T	T		

Fuente: El Autor

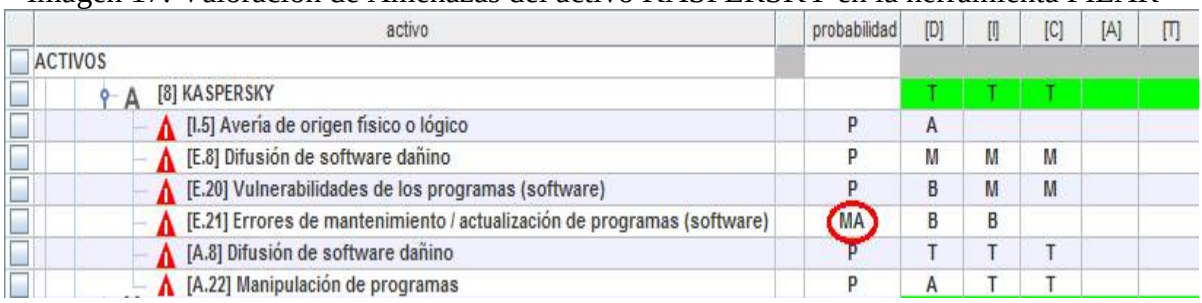
Imagen 16: Valoración de Amenazas del activo OFFICE en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[7] OFFICE		T	T	T		
[I.5] Avería de origen físico o lógico	P	A				
[E.8] Difusión de software dañino	P	M	M	M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.8] Difusión de software dañino	P	T	T	T		
[A.22] Manipulación de programas	P	A	T	T		

Fuente: El Autor

Imagen 17: Valoración de Amenazas del activo KASPERSKY en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[8] KASPERSKY		T	T	T		
[I.5] Avería de origen físico o lógico	P	A				
[E.8] Difusión de software dañino	P	M	M	M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.8] Difusión de software dañino	P	T	T	T		
[A.22] Manipulación de programas	P	A	T	T		

Fuente: El Autor

Imagen 18: Valoración de Amenazas del activo SERVIDOR en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
A [9] SERVIDOR		T	M	T		
[N.1] Fuego	PP	T				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	T				
[I.1] Fuego	P	T				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	T				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte del suministro eléctrico	P	T				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	T				
[I.11] Emanaciones electromagnéticas	P			B		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	T		T		
[A.7] Uso no previsto	P	B	B	M		
[A.11] Acceso no autorizado	P	M	M	A		
[A.23] Manipulación del hardware	P	A		A		
[A.24] Denegación de servicio	P	T				
[A.25] Robo de equipos	P	T		T		
[A.26] Ataque destructivo	P	T				

Fuente: El Autor

Imagen 19: Valoración de Amenazas del activo PC en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
A [10] PC		T	M	A		
[N.1] Fuego	PP	T				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	T				
[I.1] Fuego	P	T				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	T				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte del suministro eléctrico	P	T				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	T				
[I.11] Emanaciones electromagnéticas	P			B		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	MA	M		M		
[A.7] Uso no previsto	P	M	B	M		
[A.11] Acceso no autorizado	P	M	M	A		
[A.23] Manipulación del hardware	P	A		A		
[A.24] Denegación de servicio	P	T				
[A.25] Robo de equipos	MA	M		M		
[A.26] Ataque destructivo	P	T				

Fuente: El Autor

Imagen 20: Valoración de Amenazas del activo IMPRESORA en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
A [11] IMPRESORA		T	M	A		
[N.1] Fuego	PP	T				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	T				
[I.1] Fuego	P	T				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	T				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte del suministro eléctrico	P	T				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	T				
[I.11] Emanaciones electromagnéticas	P			B		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	T		A		
[A.11] Acceso no autorizado	P	M	M	A		
[A.23] Manipulación del hardware	P	A		A		
[A.24] Denegación de servicio	P	T				
[A.25] Robo de equipos	P	T		A		
[A.26] Ataque destructivo	P	T				

Fuente: El Autor

Imagen 21: Valoración de Amenazas del activo ESCANER en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
A [12] ESCÁNER		T	M	A		
[N.1] Fuego	PP	T				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	T				
[I.1] Fuego	P	T				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	T				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte del suministro eléctrico	P	T				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	T				
[I.11] Emanaciones electromagnéticas	P			B		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	T		A		
[A.11] Acceso no autorizado	P	M	M	A		
[A.23] Manipulación del hardware	P	A		A		
[A.24] Denegación de servicio	P	T				
[A.25] Robo de equipos	P	T		A		
[A.26] Ataque destructivo	P	T				

Fuente: El Autor

Imagen 22: Valoración de Amenazas del activo SWITCH en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
A [13] SWITCH		T	M	A		
[N.1] Fuego	PP	T				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	T				
[I.1] Fuego	P	T				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	T				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte del suministro eléctrico	P	T				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	T				
[I.11] Emanaciones electromagnéticas	P			B		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	M		A		
[A.7] Uso no previsto	P	M		M		
[A.11] Acceso no autorizado	P	M	M	A		
[A.23] Manipulación del hardware	P	T		A		
[A.24] Denegación de servicio	P	T				
[A.25] Robo de equipos	P	M		A		
[A.26] Ataque destructivo	P	T				

Fuente: El Autor

Imagen 23: Valoración de Amenazas del activo MODEM en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
A [14] MODEM		T	M	A		
[N.1] Fuego	PP	T				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	T				
[I.1] Fuego	P	T				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	T				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte del suministro eléctrico	P	T				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	T				
[I.11] Emanaciones electromagnéticas	P			B		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	M		A		
[A.7] Uso no previsto	P	M		M		
[A.11] Acceso no autorizado	P	M	M	A		
[A.23] Manipulación del hardware	P	T		A		
[A.24] Denegación de servicio	P	T				
[A.25] Robo de equipos	P	M		A		
[A.26] Ataque destructivo	P	T				

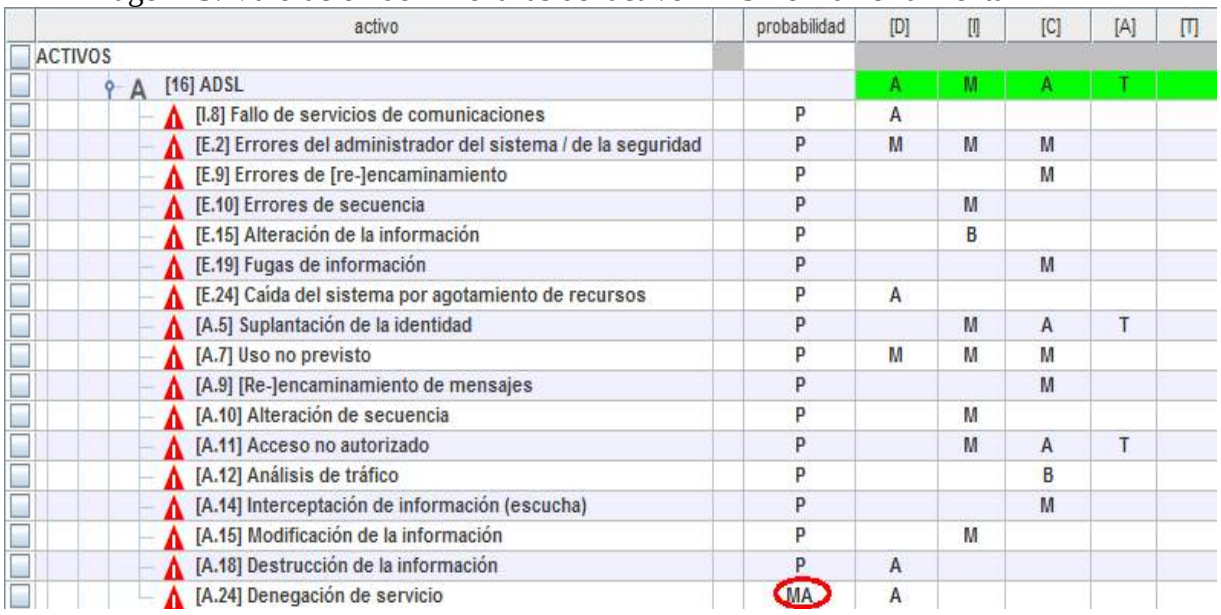
Fuente: El Autor

Imagen 24: Valoración de Amenazas del activo CONMUTADOR IP en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
A [15] CONMUTADOR IP		T	M	A		
[N.1] Fuego	PP	T				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	T				
[I.1] Fuego	P	T				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	T				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte del suministro eléctrico	P	T				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	T				
[I.11] Emanaciones electromagnéticas	P			B		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	T		A		
[A.11] Acceso no autorizado	P	M	M	A		
[A.23] Manipulación del hardware	P	A		A		
[A.24] Denegación de servicio	P	T				
[A.25] Robo de equipos	P	T		A		
[A.26] Ataque destructivo	P	T				

Fuente: El Autor

Imagen 25: Valoración de Amenazas del activo ADSL en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
A [16] ADSL		A	M	A	T	
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			M		
[E.10] Errores de secuencia	P		M			
[E.15] Alteración de la información	P		B			
[E.19] Fugas de información	P			M		
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[A.5] Suplantación de la identidad	P		M	A	T	
[A.7] Uso no previsto	P	M	M	M		
[A.9] [Re-]encaminamiento de mensajes	P			M		
[A.10] Alteración de secuencia	P		M			
[A.11] Acceso no autorizado	P		M	A	T	
[A.12] Análisis de tráfico	P			B		
[A.14] Interceptación de información (escucha)	P			M		
[A.15] Modificación de la información	P		M			
[A.18] Destrucción de la información	P	A				
[A.24] Denegación de servicio	MA	A				

Fuente: El Autor

Imagen 26: Valoración de Amenazas del activo LAN en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]
ACTIVOS					
A [17] LAN		A	M	A	T
[I.8] Fallo de servicios de comunicaciones	P	A			
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M	
[E.9] Errores de [re-]encaminamiento	P			M	
[E.10] Errores de secuencia	P		M		
[E.15] Alteración de la información	P		B		
[E.19] Fugas de información	P			M	
[E.24] Caída del sistema por agotamiento de recursos	P	A			
[A.5] Suplantación de la identidad	P		M	A	T
[A.7] Uso no previsto	P	M	M	M	
[A.9] [Re-]encaminamiento de mensajes	P			M	
[A.10] Alteración de secuencia	P		M		
[A.11] Acceso no autorizado	P		M	A	T
[A.12] Análisis de tráfico	P			B	
[A.14] Interceptación de información (escucha)	P			B	
[A.15] Modificación de la información	P		M		
[A.18] Destrucción de la información	P	A			
[A.24] Denegación de servicio	MA	A			

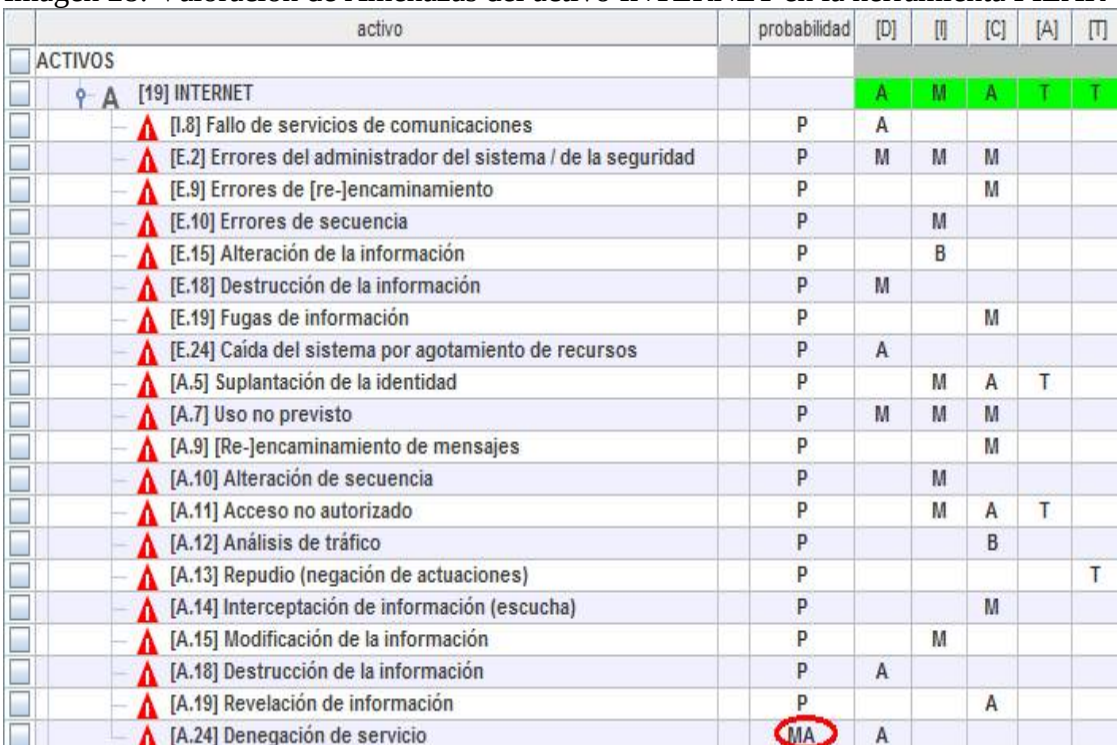
Fuente: El Autor

Imagen 27: Valoración de Amenazas del activo BACKUP en la herramienta PILAR

activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
A [18] UPS		B				
[N.1] Fuego	PP	B				
[N.2] Daños por agua	PP	B				
[N.*] Desastres naturales	PP	B				
[I.1] Fuego	P	B				
[I.2] Daños por agua	P	B				
[I.*] Desastres industriales	P	B				
[I.3] Contaminación medioambiental	PP	B				
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B				
[A.7] Uso no previsto	P	B				
[A.23] Manipulación del hardware	P	B				
[A.25] Robo de equipos	P	B				
[A.26] Ataque destructivo	P	B				

Fuente: El Autor

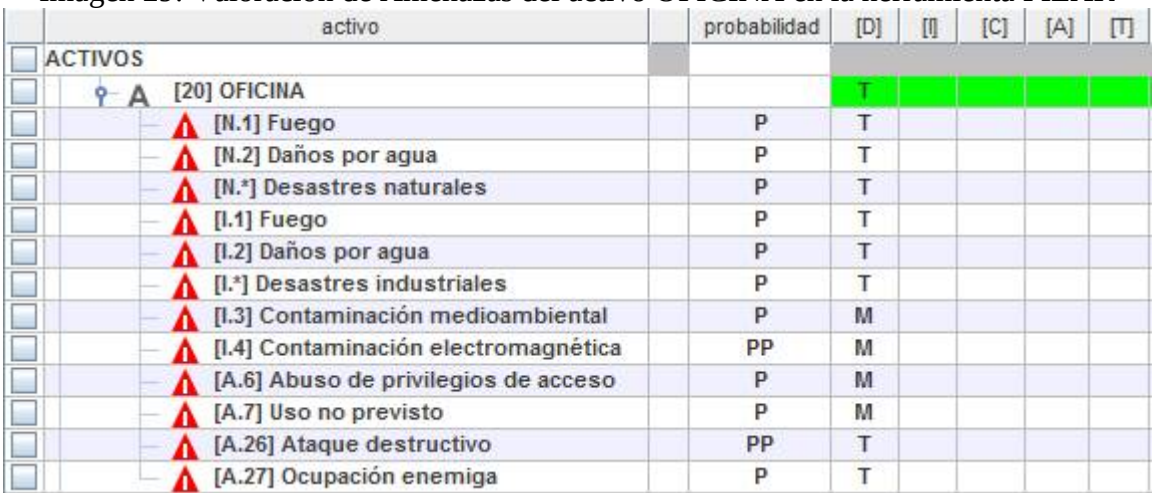
Imagen 28: Valoración de Amenazas del activo INTERNET en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[19] INTERNET		A	M	A	T	T
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			M		
[E.10] Errores de secuencia	P		M			
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[A.5] Suplantación de la identidad	P		M	A	T	
[A.7] Uso no previsto	P	M	M	M		
[A.9] [Re-]encaminamiento de mensajes	P			M		
[A.10] Alteración de secuencia	P		M			
[A.11] Acceso no autorizado	P		M	A	T	
[A.12] Análisis de tráfico	P			B		
[A.13] Repudio (negación de actuaciones)	P					T
[A.14] Interceptación de información (escucha)	P			M		
[A.15] Modificación de la información	P		M			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.24] Denegación de servicio	MA	A				

Fuente: El Autor

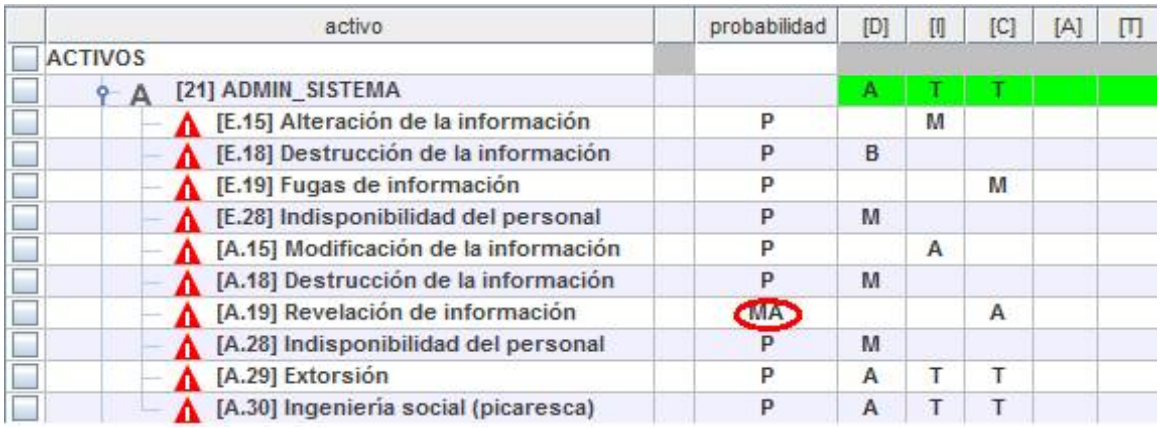
Imagen 29: Valoración de Amenazas del activo OFICINA en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[20] OFICINA		T				
[N.1] Fuego	P	T				
[N.2] Daños por agua	P	T				
[N.*] Desastres naturales	P	T				
[I.1] Fuego	P	T				
[I.2] Daños por agua	P	T				
[I.*] Desastres industriales	P	T				
[I.3] Contaminación medioambiental	P	M				
[I.4] Contaminación electromagnética	PP	M				
[A.6] Abuso de privilegios de acceso	P	M				
[A.7] Uso no previsto	P	M				
[A.26] Ataque destructivo	PP	T				
[A.27] Ocupación enemiga	P	T				

Fuente: El Autor

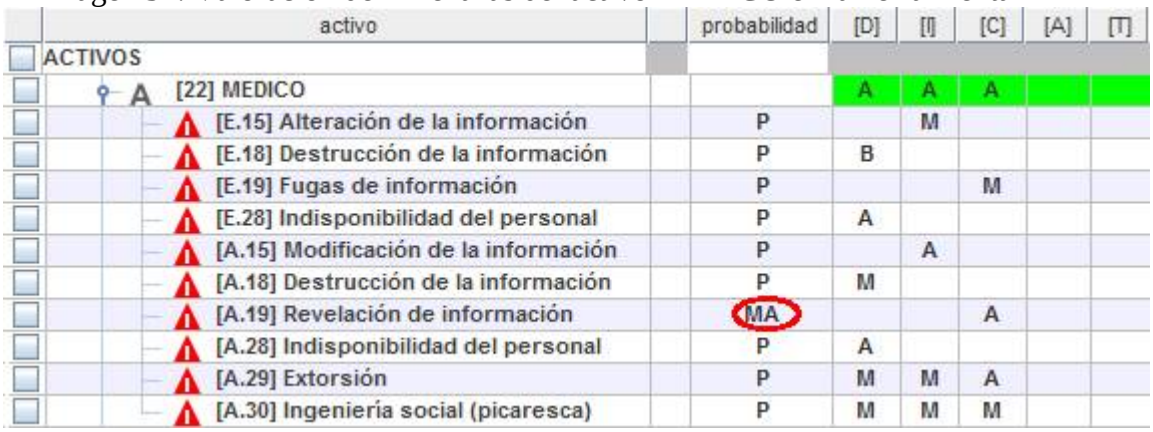
Imagen 30: Valoración de Amenazas del activo ADMIN_SISTEMA en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[21] ADMIN_SISTEMA		A	T	T		
[E.15] Alteración de la información	P		M			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		
[E.28] Indisponibilidad del personal	P	M				
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	M				
[A.19] Revelación de información	MA			A		
[A.28] Indisponibilidad del personal	P	M				
[A.29] Extorsión	P	A	T	T		
[A.30] Ingeniería social (picaresca)	P	A	T	T		

Fuente: El Autor

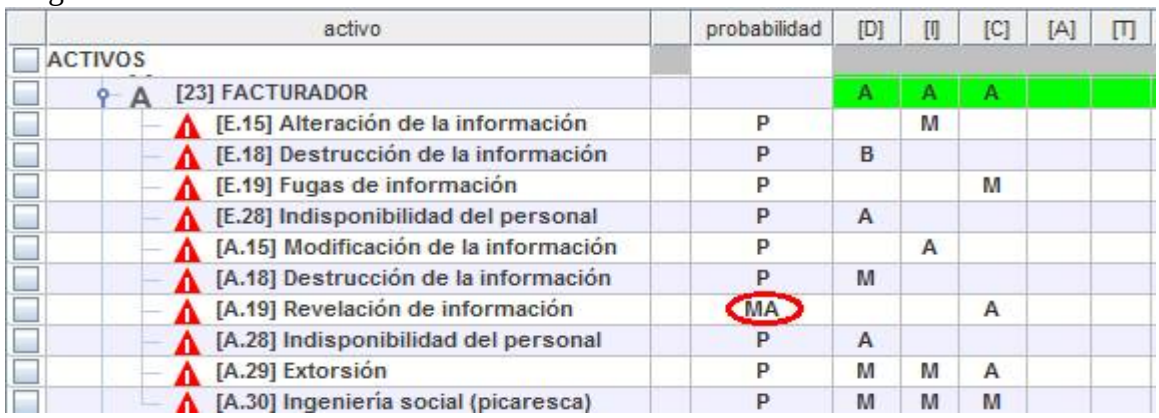
Imagen 31: Valoración de Amenazas del activo MEDICO en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[22] MEDICO		A	A	A		
[E.15] Alteración de la información	P		M			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		
[E.28] Indisponibilidad del personal	P	A				
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	M				
[A.19] Revelación de información	MA			A		
[A.28] Indisponibilidad del personal	P	A				
[A.29] Extorsión	P	M	M	A		
[A.30] Ingeniería social (picaresca)	P	M	M	M		

Fuente: El Autor

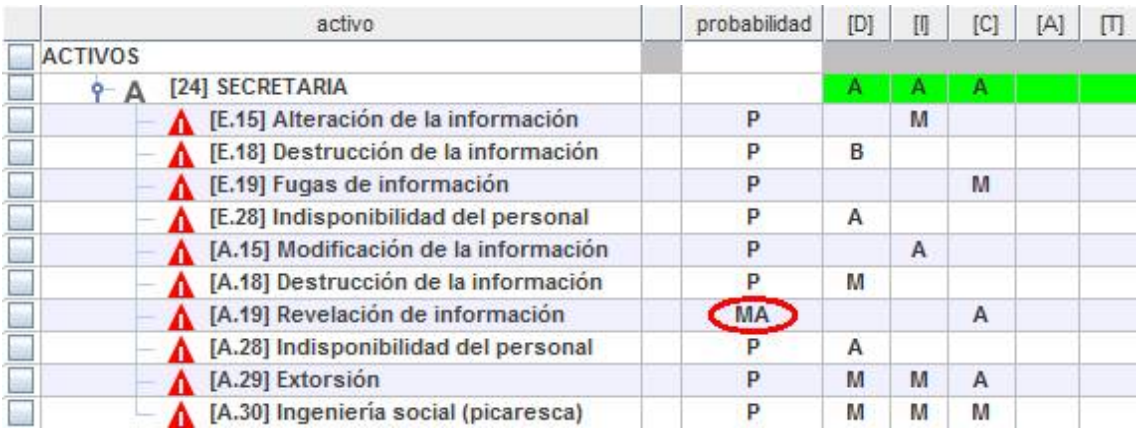
Imagen 32: Valoración de Amenazas del activo FACTURADOR en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[23] FACTURADOR		A	A	A		
[E.15] Alteración de la información	P		M			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		
[E.28] Indisponibilidad del personal	P	A				
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	M				
[A.19] Revelación de información	MA			A		
[A.28] Indisponibilidad del personal	P	A				
[A.29] Extorsión	P	M	M	A		
[A.30] Ingeniería social (picaresca)	P	M	M	M		

Fuente: El Autor

Imagen 33: Valoración de Amenazas del activo SECRETARIA en la herramienta PILAR



activo	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[24] SECRETARIA		A	A	A		
[E.15] Alteración de la información	P		M			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		
[E.28] Indisponibilidad del personal	P	A				
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	M				
[A.19] Revelación de información	MA			A		
[A.28] Indisponibilidad del personal	P	A				
[A.29] Extorsión	P	M	M	A		
[A.30] Ingeniería social (picaresca)	P	M	M	M		

Fuente: El Autor

Resumiendo la información obtenida desde la valoración de las amenazas es coherente decir que:

- En los activos BACKUP y BD_REG, las probabilidades de materialización de las amenazas pertinentes a la suplantación de identidad y abuso de privilegios son muy altas y al presentarse ocasionarían daños las cuatro dimensiones fundamentales, siendo la disponibilidad la menos golpeada y la confidencialidad la de mayor impacto, además en BD_REG, es casi probable que se presenten amenazas de tipo acceso no autorizado lo que generaría problemas altos en su dimensión de confidencialidad y la integridad puede verse moderadamente afectada pues no se tiene claridad con que fin el intruso entro a la base de datos.

- El activo TELEFONIA IP, se ve amenazado en gran parte por la denegación del servicio y aunque es un servicio que brindamos internamente depende de un proveedor externo para su ejecución plena entre todas las sedes con las que cuenta la IPS.

- Los activos ubicados en la capa de software (SW_RIP, PROGSALUD, SQL_SERVER, SISTEMA_OPERATIVO, OFFICE, KASPERSKY), es notorio que una amenaza de tipo Errores de mantenimiento / actualización de programas (software), se encuentra en un nivel muy alto de materialización y esto se debe en principio a no contar con políticas que estructuren un proceso seguro de realización de este proceso, aunque su materialización produciría un impacto bajo sobre la disponibilidad y la integridad no debe ser descuidado, además de esta amenaza está presente una de mucho cuidado la cual es la Manipulación de

programas la cual al materializarse genera degradación total del activo en la dimensión de integridad y confidencialidad sin dejar a un lado la disponibilidad la cual tendría una alta degradación, por tal motivo es necesario aplicar correctivos para evitar daños a esta capa de activos.

- La capa hardware la cual cuenta con los activos, SERVIDOR, PC, IMPRESORA, ESCANER, SWITCH, MODEM Y COMUTADOR IP, presenta un muy alto índice de materialización de la amenaza "Caída del sistema por agotamiento de recursos", la cual genera un alto impacto en la disponibilidad de cada uno de los activos, esta amenaza se presenta debido a la baja organización y estructuración de la red, de los perfiles de acceso a la información, y sobre todo a los pocos conocimientos que posee el personal sobre el manejo adecuado de los recursos de información y más aún en lo pertinente a la seguridad informática, además de la anterior hay una amenaza circundante que afecta a más de una dimensión de forma considerable esta es el acceso no autorizado, esta amenaza se debe a que no se cuenta con manuales de funciones y estipulación clara de zonas restringidas, accesos no permitidos y condiciones precisas sobre el manejo y responsabilidades de la seguridad de la información que se debe tener en la IPS.

- En cuanto a los activos ADSL, LAN e INTERNET, la amenaza más presentada y la cual ocasiona degradación alta en la dimensión de disponibilidad es la denegación de servicio, la cual acarrea una caída completa del sistema debido a que este funciona con la interconexión de la red local y además la conexión con internet para la plataforma utilizadas para administrar el historial clínico, esa amenaza está muy presente debido a que los planes de mantenimiento y correcto uso de la red y el servicio de internet, son inexistentes lo que ha traído muchos problemas e inconvenientes para el desarrollo eficiente del objeto principal de la IPS

- En cuanto al bien OFICINA es claro afirmar que dentro de sus mayores amenazas es el Abuso de privilegios de acceso, lo que no solo registra problemas grabes de seguridad al sistema de información sino también a nivel del recurso humano que muchas veces se ve afectado por la intromisión de personal no autorizado para el acceso que llega a la empresa con fines de agredir a funcionarios o con intenciones de extraer elementos de la IPS, como también ocurre con el personal interno que no tiene claro los lugares donde están los sistemas y que son de acceso altamente restringido.

- Dentro del pernal que interactúa con el sistema de información en términos general se ve afectado principalmente por tres amenazas, la Revelación de

información, que es una amenaza grande que afecta la confidencialidad y por la cual al tratarse de información de historias clínicas tiene afectaciones legales sobre la mala utilización de esta información, esta amenaza tiene mucha fuerza y poco control debido a que los empleados no tienen en su contrato una cláusula de confidencialidad donde se exprese que la información a la cual acceden en la IPS es de carácter confidencial y no debe ser revelada sin una justa causa y previa autorización de la IPS, además la amenaza de Modificación de la información y Destrucción de la información, están presentes y afectan directamente la disponibilidad e integridad del sistema de información, esta amenaza es muy propensa al no contar con perfiles de acceso bien definido con restricciones y accesos completamente puntuales logrando con ello evitar que personal no capacitado o no autorizado pueda realizar cambios a la información y/o eliminar la misma.

10 DESARROLLO FASE 3

10.1 DETERMINACIÓN DEL IMPACTO POTENCIAL ACUMULADO

El libro 1 del manual de MAGERIT "método", define como impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

Tabla 11: Escala Nivel del Impacto MAGERIT

VALOR		**CRITERIO**
10	EXTREMO	Daño extremadamente grave
9	MUY ALTO	Daño muy grave
8-6	ALTO (+)	Daño grave
	ALTO	
	ALTO (-)	
5-3	MEDIO (+)	Daño importante.
	MEDIO	
	MEDIO (-)	
2-1	BAJO (+)	Daño menor.
	BAJO	
0	DESPRECIABLE	Irrelevante a efectos prácticos.

Fuente: El Autor

Imagen 34: Impacto potencial acumulado en la herramienta PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[9]	[9]	[9]	[9]	[7]
[B] Activos esenciales	[9]	[9]	[9]	[9]	
[0] BACKUP	[3]	[6]	[8]	[9]	
[1] BD_REGPAC	[9]	[9]	[9]	[9]	
[IS] Servicios internos	[8]	[8]	[8]	[9]	[7]
[2] TELEFONIA IP	[8]	[8]	[8]	[9]	[7]
[E] Equipamiento	[9]	[9]	[9]	[9]	
[SW] Aplicaciones	[9]	[9]	[9]		
[3] SW_RIP	[9]	[9]	[9]		
[4] PROGSALUD	[9]	[9]	[9]		
[5] SQL_SERVER	[9]	[9]	[9]		
[6] SISTEMA_OPERATIVO	[9]	[9]	[9]		
[7] OFFICE	[9]	[9]	[9]		
[8] KASPERSKY	[9]	[9]	[9]		
[HW] Equipos	[9]	[6]	[9]		
[9] SERVIDOR	[9]	[6]	[9]		
[10] PC	[9]	[6]	[8]		
[11] IMPRESORA	[9]	[6]	[8]		
[12] ESCÁNER	[9]	[6]	[8]		
[13] SWITCH	[9]	[6]	[8]		
[14] MODEM	[9]	[6]	[8]		
[15] CONMUTADOR IP	[9]	[6]	[8]		
[COM] Comunicaciones	[8]	[7]	[8]	[9]	
[16] ADSL	[8]	[7]	[8]	[9]	
[17] LAN	[8]	[7]	[8]	[9]	
[AUX] Elementos auxiliares	[3]				
[18] UPS	[3]				
[SS] Servicios subcontratados	[8]	[7]	[8]	[9]	[7]
[19] INTERNET	[8]	[7]	[8]	[9]	[7]
[L] Instalaciones	[9]				
[20] OFICINA	[9]				
[P] Personal	[8]	[9]	[9]		
[21] ADMIN_SISTEMA	[8]	[9]	[9]		
[22] MEDICO	[8]	[8]	[8]		
[23] FACTURADOR	[8]	[8]	[8]		
[24] SECRETARIA	[8]	[8]	[8]		

Fuente: El Autor

10.2DETERMINACIÓN DEL RIESGO POTENCIAL ACUMULADO

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

La herramienta PILAR nos ofrece una cierta gama de niveles con los cuales el valora la criticidad del riesgo a continuación se presenta.

Imagen 35. Niveles de criticidad del riesgo en la herramienta PILAR

Fuente: El Autor

Imagen 36: Riesgo Potencial Acumulado

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{6,6}	{6,6}	{7,5}	{7,1}	{5,7}
[B] Activos esenciales	{6,2}	{6,2}	{7,5}	{7,1}	
[0] BACKUP	{3,6}	{6,2}	{7,5}	{7,1}	
[1] BD_REGPAC	{6,2}	{6,2}	{7,5}	{7,1}	
[IS] Servicios internos	{6,6}	{6,6}	{5,7}	{6,2}	{5,7}
[2] TELEFONIA IP	{6,6}	{6,6}	{5,7}	{6,2}	{5,7}
[E] Equipamiento	{6,6}	{6,2}	{6,2}	{6,2}	
[SW] Aplicaciones	{6,2}	{6,2}	{6,2}		
[3] SW_RIP	{6,2}	{6,2}	{6,2}		
[4] PROGSALUD	{6,2}	{6,2}	{6,2}		
[5] SQL_SERVER	{6,2}	{6,2}	{6,2}		
[6] SISTEMA_OPERATIVO	{6,2}	{6,2}	{6,2}		
[7] OFFICE	{6,2}	{6,2}	{6,2}		
[8] KASPERSKY	{6,2}	{6,2}	{6,2}		
[HW] Equipos	{6,6}	{4,5}	{6,2}		
[9] SERVIDOR	{6,6}	{4,5}	{6,2}		
[10] PC	{6,6}	{4,5}	{5,7}		
[11] IMPRESORA	{6,6}	{4,5}	{5,7}		
[12] ESCÁNER	{6,6}	{4,5}	{5,7}		
[13] SWITCH	{6,6}	{4,5}	{5,7}		
[14] MODEM	{6,6}	{4,5}	{5,7}		
[15] CONMUTADOR IP	{6,6}	{4,5}	{5,7}		
[COM] Comunicaciones	{6,6}	{5,0}	{5,7}	{6,2}	
[16] ADSL	{6,6}	{5,0}	{5,7}	{6,2}	
[17] LAN	{6,6}	{5,0}	{5,7}	{6,2}	
[AUX] Elementos auxiliares	{2,7}				
[18] UPS	{2,7}				
[SS] Servicios subcontratados	{6,6}	{5,0}	{5,7}	{6,2}	{5,1}
[19] INTERNET	{6,6}	{5,0}	{5,7}	{6,2}	{5,1}
[L] Instalaciones	{6,2}				
[20] OFICINA	{6,2}				
[P] Personal	{5,7}	{6,2}	{6,6}		
[21] ADMIN_SISTEMA	{5,7}	{6,2}	{6,6}		
[22] MEDICO	{5,4}	{5,7}	{6,6}		
[23] FACTURADOR	{5,4}	{5,7}	{6,6}		
[24] SECRETARIA	{5,4}	{5,7}	{6,6}		

Fuente: El Autor

Para la obtención de los valores vistos en la imagen anterior PILAR utiliza una tabla mediante la que realiza los cálculos del riesgo, esta tabla se encuentra en el ANEXO 2

(tabla de valoración del riesgo e impacto potencial), y para comprender los valores hay representados a continuación se presenta a detalle el concepto de cada columna:

Activo – el activo
Amenaza – la amenaza
Dimensión – la dimensión de seguridad

Tabla 12: Detalles de columnas presentes en el anexo 2

V	El valor propio del activo en esa dimensión, si lo tiene
VA	El valor acumulado del activo en esa dimensión
D	La degradación causada por la amenaza
I	El impacto
N	La probabilidad
R	El riesgo

Fuente: el Autor

10.3 IDENTIFICACIÓN DE SALVAGUARDAS

Según el libro 1 de la metodología MAGERIT "método", Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal.

La herramienta pilar nos ofrece una serie de salvaguardas según su análisis del riesgo presente.

Imagen 37: Salvaguardas ofrecidos por la herramienta PILAR

aspecto	tdp	salvaguarda	dudas	fuente	comentario	recomendación
		SALVAGUARDAS				
G	EL	[IA] Identificación y autenticación				8
T	EL	[AC] Control de acceso lógico				7
G	PR	[D] Protección de la Información				6
G	EL	[K] Protección de claves criptográficas				
G	PR	[S] Protección de los Servicios				6
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7
G	PR	[HW] Protección de los Equipos Informáticos (HW)				7
G	PR	[COM] Protección de las Comunicaciones				8
G	PR	[IP] Sistema de protección de frontera lógica				
G	PR	[MP] Protección de los Soportes de Información				
G	PR	[AUX] Elementos Auxiliares				6
F	PR	[L] Protección de las Instalaciones				7
F	EL	[PPS] Protección del perímetro físico				
P	PR	[PS] Gestión del Personal				6
G	PR	[PDS] Servicios potencialmente peligrosos				
G	CR	[IR] Gestión de incidentes				6
T	PR	[tools] Herramientas de seguridad				8
G	CR	[V] Gestión de vulnerabilidades				6
T	MN	[A] Registro y auditoría				5
G	RC	[BC] Continuidad del negocio				5
G	AD	[G] Organización				5
G	AD	[E] Relaciones Externas				6
G	AD	[NEW] Adquisición / desarrollo				5

Fuente: el autor

Como se puede inferir de la imagen los salvaguardas más recomendados son identificación y autentificación, protección de las comunicaciones y herramientas de seguridad, aunque seguidos de otros muy relevantes a continuación se relacionan a detalle los salvaguardas a utilizar en la gestión del riesgo no solo centrado en los ofrecidos por la herramienta PILAR sino también por lo sugeridos por el método Magerit en su libro 2 “catálogo de elementos” y la norma ISO 27002

Salvaguardas de tipo Protecciones generales u horizontales:

H Protecciones Generales: implementar red eléctrica regulada y con soporte ininterrumpido (ups), sistema contra incendios (extintores), vigilancia para impedir acceso de personas no autorizadas, registro de operaciones ejecutadas en los equipos de cómputo.

H.IA Identificación y autenticación: crear políticas de perfiles de acceso protegido por contraseña, contraseñas que contengan mínimo 8 caracteres, dentro de los cuales debe incluir letras, números y mínimo un signo, estas contraseñas tendrán caducidad de 30 días.

Salvaguardas de tipo Protección de los datos / información:

D.A Copias de seguridad de los datos (backup): actualización de la política de backup esta debe realizarse al finalizar la semana laboral y debe contener la copia de seguridad del servidor y de todos los equipos de cómputo en los cuales se genera producción de información, esta debe ser almacenada en dos medios, un disco duro extraíble y en un disco óptico DVD, el cual debe ser rotulado con la fecha de creación de la copia de seguridad, de ser posible crear una tercera copia y almacenarla en un servidor web contratado por la IPS.

D.I Aseguramiento de la integridad: establecer políticas para la manipulación de la información, establecer restricciones para la modificación de información, si es necesario modificarla, se debe presentar una solicitud al administrador del sistema, esté previa validación del motivo por el cual se modificara dejara un registro detallado del cambio y quien lo efectúa.

Salvaguardas de tipo Protección de los servicios:

S.SC Se aplican perfiles de seguridad: asignación de perfiles de acuerdo al rol del usuario en el sistema, este perfil debe contener las restricciones y accesos que sean estrictamente necesarios para llevar a cabo las funciones establecidas para él, en este momento se proponen 4 perfiles, administrador, médicos, facturación y secretaria.

S.CM Gestión de cambios (mejoras y sustituciones): implementar políticas de mantenimiento de equipo de cómputo de tipo preventivo y correctivo, además a todo el sistema de red LAN y eléctrico, sin dejar a un lado el de sistemas de refrigeración, los mantenimientos preventivos deberán ser realizados cada 6 meses, en cuanto a los correctivos deben ser realizados al percibir cualquier anomalía y si incluye el remplazo de un dispositivo debe ser llevado a cabo en la brevedad Salvaguardas de tipo Protección de las aplicaciones (software)

SW.CM Cambios (actualizaciones y mantenimiento): definir políticas de instalación de actualizaciones estas solo podrán ser realizadas por el administrador del sistema, previamente el deberá hacer pruebas sobre la nueva versión y validar que sea funcional para no generar caos en el sistema, además de ello dentro del proceso de mantenimiento se debe incluir el de la base de datos del servidor con el fin de garantizar que este siempre se encuentre en óptimas condiciones este proceso debe ejecutarse cada 3 meses y como resultado debe dejar una copia de seguridad antes y después del proceso de mantenimiento.

Salvaguardas de tipo Protección de las comunicaciones:

COM.internet Internet: uso de acceso a: crear política de acceso al servicio de internet este debe estar limitado y brindar soporte exclusivo al desarrollo de actividades laborales deben bloquearse redes sociales, motores de búsqueda, correos electrónicos distintos al institucional, páginas dedicadas a la reproducción de multimedia denomínese este audio y/o video.

Salvaguardas de tipo Seguridad física – Protección de las instalaciones:

L.AC Control de los accesos físicos: establecer políticas de acceso a lugares restringidos dentro del edificio, para el ingreso al centro de cómputo establecer sistema de entrada biométrico o en su defecto acceso mediante clave numérica.

Salvaguardas de tipo Salvaguardas relativas al personal:

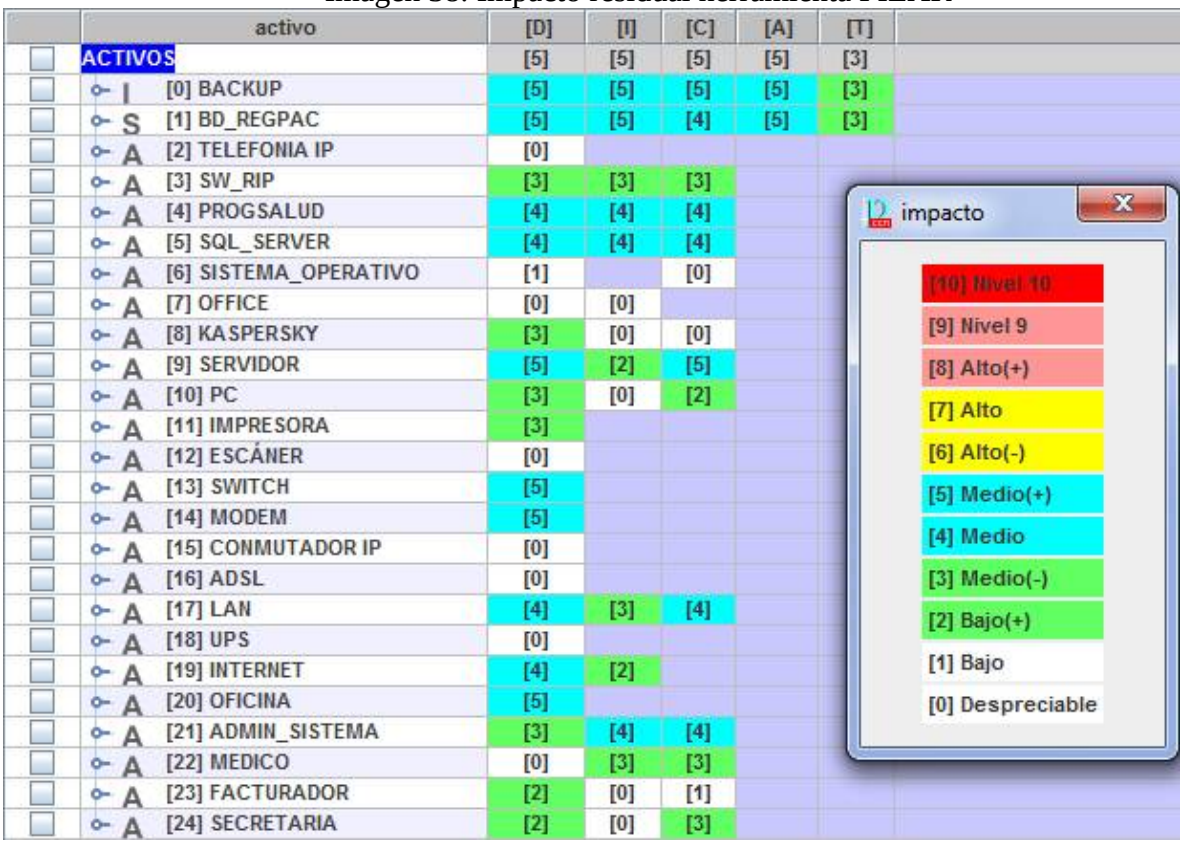
PS Gestión del Personal: mantener la carga laboral sobre niveles aceptables, si la carga laboral se extrema se deben contratar personal temporal para adelantar las labores.

PS.AT Formación y concienciación: fundamental creación de planes de capacitación de funciones y manejo seguro de la informacion, creación de manual de inducción y re inducción, en el crear apartado para la seguridad informática, implementar cronograma capacitaciones al personal en general, en lo pertinente al administrador del sistema crear plan de capacitaciones en específico que le permita conocer los nuevos riesgos y protocolos para incrementar la seguridad y eficiencia del sistema.

10.4 IMPACTO RESIDUAL

La herramienta PILAR nos arroja el cálculo del impacto residual después de la aplicación de las salvaguardas sugeridas por su algoritmo interno, aunque el impacto ha disminuido notoriamente aún se siguen presentado impactos esto se debe que actualmente no existe un sistema que sea cien por ciento impermeable a impactos producidos por amenazas.

Imagen 38. Impacto residual herramienta PILAR



	activo	[D]	[I]	[C]	[A]	[T]
	ACTIVOS	[5]	[5]	[5]	[5]	[3]
	I [0] BACKUP	[5]	[5]	[5]	[5]	[3]
	S [1] BD_REGPAC	[5]	[5]	[4]	[5]	[3]
	A [2] TELEFONIA IP	[0]				
	A [3] SW_RIP	[3]	[3]	[3]		
	A [4] PROGSALUD	[4]	[4]	[4]		
	A [5] SQL_SERVER	[4]	[4]	[4]		
	A [6] SISTEMA_OPERATIVO	[1]		[0]		
	A [7] OFFICE	[0]	[0]			
	A [8] KASPERSKY	[3]	[0]	[0]		
	A [9] SERVIDOR	[5]	[2]	[5]		
	A [10] PC	[3]	[0]	[2]		
	A [11] IMPRESORA	[3]				
	A [12] ESCÁNER	[0]				
	A [13] SWITCH	[5]				
	A [14] MODEM	[5]				
	A [15] CONMUTADOR IP	[0]				
	A [16] ADSL	[0]				
	A [17] LAN	[4]	[3]	[4]		
	A [18] UPS	[0]				
	A [19] INTERNET	[4]	[2]			
	A [20] OFICINA	[5]				
	A [21] ADMIN_SISTEMA	[3]	[4]	[4]		
	A [22] MEDICO	[0]	[3]	[3]		
	A [23] FACTURADOR	[2]	[0]	[1]		
	A [24] SECRETARIA	[2]	[0]	[3]		

Fuente: el autor

10.5 RIESGO RESIDUAL

La herramienta PILAR nos arroja el cálculo del riesgo residual después de la aplicación de las salvaguardas sugeridas por su algoritmo interno, aunque el riesgo ha disminuido notoriamente aún se siguen presentado riesgo esto se debe que actualmente no existe un sistema que sea cien por ciento impermeable a riesgo producidos por amenazas.

Imagen 39. Riesgo residual herramienta PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{3,0}	{2,6}	{3,6}	{3,3}	{1,8}
I [0] BACKUP	{3,0}	{2,6}	{3,6}	{3,3}	{1,8}
S [1] BD_REGPAC	{3,0}	{2,6}	{3,1}	{3,3}	{1,8}
A [2] TELEFONIA IP	{0,40}				
A [3] SW_RIP	{1,5}	{1,6}	{1,6}		
A [4] PROGSALUD	{2,1}	{2,2}	{2,2}		
A [5] SQL_SERVER	{2,1}	{2,2}	{2,2}		
A [6] SISTEMA_OPERATIVO	{0,87}		{0,29}		
A [7] OFFICE	{0,75}	{0,29}			
A [8] KASPERSKY	{1,5}	{0,76}	{0,76}		
A [9] SERVIDOR	{2,9}	{0,92}	{2,6}		
A [10] PC	{1,7}	{0,69}	{0,93}		
A [11] IMPRESORA	{1,7}				
A [12] ESCÁNER	{0,79}				
A [13] SWITCH	{2,9}				
A [14] MODEM	{2,9}				
A [15] CONMUTADOR IP	{0,44}				
A [16] ADSL	{0,45}				
A [17] LAN	{2,9}	{1,2}	{2,0}		
A [18] UPS	{0,17}				
A [19] INTERNET	{2,7}	{0,99}			
A [20] OFICINA	{2,8}				
A [21] ADMIN_SISTEMA	{1,5}	{2,0}	{2,5}		
A [22] MEDICO	{0,72}	{1,6}	{2,5}		
A [23] FACTURADOR	{0,95}	{0,76}	{1,3}		
A [24] SECRETARIA	{0,95}	{0,76}	{2,5}		

Fuente: el autor

11 RESULTADO Y DISCUSIÓN

11.1 DISEÑO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

11.2 POLÍTICAS DE SEGURIDAD

Una política de seguridad es la herramienta que brinda las pautas necesarias para comprender que se permite y que está prohibido, si nos referimos a un sistema de información hará énfasis en que está permitido hacer con la información y que no se puede hacer con ella, y no solo eso también estipulara el proceso correcto para el manejo de la información tal cual lo demande el manual de funciones o el rol que juegue una persona dentro de una empresa, en este caso en particular se definirán políticas para el manejo de los activos de tipo información y además los protocolos que se deben mantener para garantizar la seguridad de tales activos, a continuación iniciamos con las políticas planteadas luego de realizado el análisis de riesgos a los cuales está expuesto el sistemas de información de la IPS ASSALUD, todo ello basado en lo sugerido por la norma ISO/IEC 27001/2013 .

11.2.1 Política de Administración de Activos de Información.

- **Objetivo**: definir las pautas a seguir para garantizar la seguridad de los activos de información.

- **Aplicabilidad**: aplicadas a todo el personal vinculado a la IPS ASSALUD denomínese estos administrativos y asistenciales, en resumidas palabras aplican a toda persona que manipule o utilice la información de la IPS (planta de personal).

- **Directrices**:

  - ✓ Inventario de activos de información: la IPS ASSALUD garantiza tener un registro detallado y actualizado de todos los activos de información con los que cuenta, este registro contendrá datos detallados del activo e información del responsable de su manejo, este registro estará a cargo del administrador del sistema de información.

  - ✓ Propietario de los activos de información: la IPS ASSALUD es la única propietaria de la los activos de información, el personal que interactúa con este activo se denomina usuario y se encontraran catalogados por el rol que juegan a partir de nivel de acceso que tengan sobre la información, teniendo en cuenta que este acceso

los hace responsables del uso dado al activo y de las consecuencias por su manipulación indebida.

11.2.2 Política para el Uso de Activos de Información.

- **Objetivo**: garantizar la seguridad de los activos de información asignando la responsabilidad de su manejo a la persona designada para tal fin teniendo en cuenta el perfil o rol que tiene dentro del sistema de información.

- **Aplicabilidad**: aplicadas a todo el personal vinculado a la IPS ASSALUD denomínese estos administrativos y asistenciales, en resumidas palabras aplican a toda persona que manipule o utilice la información de la IPS (planta de personal).

- **Directrices**:

  - ✓ Propietario y uso: la IPS ASSALUD es la única propietaria de la los activos de información denomínese estos equipos y datos, los archivos creados en cumplimiento del objeto laboral serán propiedad de ASSALUD y el uso a este activo será exclusivamente laboral.

  - ✓ Estaciones y lugar de trabajo: los usuarios deben realizar sus labores en el equipo y lugar asignados por el administrador del sistema de información.

  - ✓ Copia de activos de información: los usuarios están limitados a realizar copia de sus archivos personales, en caso de requerir realizar copia de la información relacionada con el objeto laboral deberá solicitar autorización al administrador del sistema de información, el uso no autorizado (copia, eliminación o divulgación) será objeto de sanciones de acuerdo a las leyes establecidas para el uso de la información y derechos de autor.

  - ✓ Instalación y/o desinstalación de aplicativos: se prohíbe la instalación de cualquier tipo de aplicativo, como también la descarga de información no pertinente al objeto laboral, sin la previa autorización del administrador del sistema de información, se realizaran revisiones periódicas a todos los equipos contenidos en el sistema de información, en caso de encontrarse irregularidades de este tipo, el responsable será sancionado de acuerdo a lo estipulado en las normas de la IPS ASSALUD.

  - ✓ Acceso a internet: los usuarios no podrán utilizar la conexión a internet para ninguna actividad personal, el uso de este activo está limitado al ámbito laboral, su uso para fines personales será sancionado por la gerencia.

- ✓ Manipulación de los activos: se prohíbe modificar, actualizar, desinstalar, desconectar, conectar cualquier hardware o software perteneciente a ASSALUD

11.2.3 Política de Control de Acceso al Sistema de Información.

- **Objetivo**: establecer el protocolo para el acceso controlado de carácter físico y lógico del sistema de información de ASSALUD.

- **Aplicabilidad**: aplicadas a todo el personal vinculado a la IPS ASSALUD denomínese estos administrativos y asistenciales, en resumidas palabras aplican a toda persona que manipule o utilice la información de la IPS (planta de personal).

- **Directrices**:

  - ✓ Conexión al sistema de información: la IPS ASSALUD suministra todos los recursos físicos y lógicos a nivel tecnológico para garantizar el desarrollo del objeto contractual de todos los usuarios, por tanto se prohíbe la conexión de cualquier elemento a las redes de comunicación, ya sean estos portátiles, Tablet, celulares, y cualquier otro tipo de elementos que entre en conexión directa o indirecta con el sistema de información, todo ello sin la previa autorización del administrador del sistema de información.

  - ✓ Asignación de claves de acceso al sistema de información: la IPS ASSALUD asignara claves a cada uno de los usuarios del sistema de información (plataforma, aplicativos, equipos), el uso de las claves es personal e intransferible y la responsabilidad del acceso recae sobre el usuario, por lo tanto este debe garantizar su manejo.

  - ✓ Perímetros de Seguridad: La política debe definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales el personal de trabajo, tienen acceso y a cuales no, la política debe definir los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.

11.2.4 Política de establecimiento de claves de acceso.

- **Objetivo**: establecer parámetros para la configuración y uso de las claves de acceso al sistema de información de ASSALUD.

- **Aplicabilidad**: aplicadas a todo el personal vinculado a la IPS ASSALUD denomínese estos administrativos y asistenciales, en resumidas palabras aplican a toda persona que manipule o utilice la información de la IPS (planta de personal).

- **Directrices**:

✓ Complejidad de la contraseña: la IPS ASSALUD suministra una contraseña provisional a todo usuario para su primer ingreso al sistema, luego de ello el usuario deberá cambiar esta contraseña, la cual debe contener como mínimo 8 caracteres, dentro de ellos debe incluir letras(mayúsculas y minúsculas), números y como mínimo un signo.

✓ Caducidad de la contraseña: la contraseña tendrá una caducidad de máximo 30 días, para garantizar el acceso el usuario deberá realizar el cambio de esta contraseña, se impedirá la reutilización de una contraseña antes asignada o establecida.

✓ Manejo de contraseña: la contraseña no debe ser escrita en ninguna superficie o almacenada de forma descifrable en ningún dispositivo.

11.2.5 Política de Backus y restablecimiento de información.

- **Objetivo**: definir elementos para realización de copias de seguridad y restauración de la información.

- **Aplicabilidad**: aplicadas al administrador del sistema de información y/o a todo el personal delegado por la gerencia para realizar administración sobre el sistema de información la IPS ASSALUD.

- **Directrices**:

✓ Elementos utilizados para realizar copias de seguridad: los elementos autorizados para realizar Backus son los discos duros extraíbles y lis medios ópticos DVD.

✓ Copias de seguridad: las copias de seguridad se deben efectuar sobre todos los equipos de cómputo que hagan parte del sistema de información de ASSALUD, y deben contener todos los archivos generados en cumplimiento del objeto laboral.

✓ Frecuencia de realización de las copias de seguridad: las copias de seguridad en estaciones de trabajo se realizaran semanalmente y las de los equipos servidor se realizaran una vez al mes.

- ✓ Lugar de almacenamiento de los Backus: los dispositivos que contienen las copias de seguridad deberán reposar en la caja fuerte y/o en la bodega de respaldo contratada por ASSALUD.

- ✓ Uso de los Backus: las copias de seguridad serán utilizadas para la restauración de la información en el caso de una calamidad, ya sea daño en el disco duro de la estación de trabajo, virus que eliminaran información, materialización de una amenaza natural o industrial, por disposición de gerencia y en coordinación del administrador del sistema de información.

11.2.6 Política para el administrador del sistema de información.

- **Objetivo**: garantizar la seguridad de los sistemas de información por parte del administrador del sistema o personal designado para el manejo de la información en ASSALUD.

- **Aplicabilidad**: aplicadas al administrador del sistema de información y/o a todo el personal delegado por la gerencia para realizar administración sobre el sistema de información la IPS ASSALUD.

- **Directrices**:

  - ✓ Manejo de contraseñas: el manejo de la contraseña es de carácter personal e intransferible, no se debe escribir en ninguna superficie, ni almacenada en medios donde sea fácilmente descifrada, esta clave debe tener un alto grado de complejidad, de mínimo 10 caracteres en los cuales se asigne 2 letras en mayúsculas, 2 números, 3 signos, y 3 letras en minúscula, además esta deberá ser cambiada mensualmente, y no se permitirá la reutilización de contraseñas.

  - ✓ Custodia de elementos informáticos: le es asignada la responsabilidad de custodia de seriales, contraseñas de administración de plataforma, correos, aplicativos y equipos de cómputo, se debe garantizar la seguridad de estos elementos.

  - ✓ Manipulación de la información: para llevar a cabo el proceso de eliminación y/o modificación se debe dejar registro detallado del proceso y las causas que lo justifican, siendo el administrador el encargado de facilitar la autorización para la modificación de la información registrada en las bases de datos debe mantener la integridad y la confidencialidad que se demanda.

  - ✓ Asignación de accesos al sistema: no asignar privilegios de acceso superiores al rol y funciones a desempeñar por el usuario.

- ✓ Confidencialidad de la información: se prohíbe revelar información de carácter confidencial manejada en ASSALUD, a la cual tenga acceso debido al cumplimiento de su objeto contractual, se obliga enmarcado en las leyes de protección de datos a mantener la confidencialidad y protección de divulgación de toda la información de ASSALUD, sin previa autorización por la gerencia.

- ✓ Registro de acceso: debe mantener registro detallado de todo proceso que requiera de la utilización de su acceso superior a el sistema de información, sea estos y no limitándose, acceso a servidor, administración de plataforma, modificación de información, acceso como administrador a estaciones de trabajo, acceso a dispositivo de red.

11.2.7 Políticas para usuarios del sistema de información de ASSALUD.

- **Objetivo**: asegurar el uso seguro del sistema de información de la IPS ASSALUD por parte de los usuarios.

- **Aplicabilidad**: aplicadas a todo el personal vinculado a la IPS ASSALUD denomínese estos administrativos y asistenciales, en resumidas palabras aplican a toda persona que manipule o utilice la información de la IPS (planta de personal).

- **Directrices**:

  - ✓ Almacenamiento de información: ASSALUD suministra a todo usuario un espacio de alojamiento de información en el servidor con una capacidad de 2gb, el cual debe utilizarse en exclusividad para almacenar archivos generados en cumplimiento de su objeto contractual.

  - ✓ Instalación de software: se prohíbe la instalación de cualquier aplicativo por parte de los usuarios sin la previa autorización del administrador del sistema de información.

  - ✓ Dispositivos de almacenamiento externos: se prohíbe la conexión de cualquier medio de almacenamiento externo o interno a los equipos de cómputo, su uso no autorizado por el administrador del sistema de información, será tomado como una violación a la confidencialidad y tendrá repercusiones legales sobre el usuario.

  - ✓ Extracción de información: ASSALUD prohíbe la copia, extracción, respaldo y/o utilización de los datos, archivos, plataformas, aplicativos y equipos con los que cuenta su sistema de información, la ejecución de cualquiera de estas acciones será

tomada como una violación a la confidencialidad y tendrá repercusiones legales sobre el usuario.

- ✓ Responsabilidad sobre activos: ASSALUD responsabiliza sobre el uso de cualquier activo de información al usuario al cual se le ha asignado.

- ✓ Uso de las estaciones de trabajo: Se prohíbe usar las estaciones de trabajo para la realización de cualquier actividad distinta al objeto contractual que posea el usuario.

- ✓ Accesos a información: Los usuarios solo tendrán acceso a la información concerniente a su objeto contractual, el usuario debe mantener la confidencialidad sobre esta información, en caso de que esta tenga esa categorización y deberá abstenerse de divulgarla, en caso de que lo haga sobre el recaerán sanciones disciplinarias o legales dependiendo de la gravedad de la acción.

- ✓ Reporte o notificación de incidentes: Es responsabilidad del usuario notificar al administrador del sistema de información cualquier evento que atente contra la seguridad del sistema.

- ✓ Compartir información: El único medio autorizado para compartir información es la unidad de red creada para tal fin, se prohíbe el envió de información por otro medio distinto al estipulado por ASSALUD.

- ✓ Capacitaciones y cumplimiento de las normas: Es obligatoria la participación en todos los eventos de capacitación a los cuales le sea oficialmente invitado, es responsabilidad del usuario conocer y aplicar los manuales de funciones, y las normas de seguridad implementadas en ASSALUD.

11.2.8 Seguridad de los Recursos Humanos en ASSALUD

- **Objetivos**

  - ✓ Reducir los riesgos derivados al error humano, omisiones, comisión de ilícitos o uso no apropiado de los activos de información y equipos.

  - ✓ Mantener informado al personal sobre las responsabilidades en materia de seguridad incluso desde el proceso de selección, durante el tiempo en que la persona presta servicios a la institución y al momento de cesar en sus funciones.

  - ✓ Garantizar que los usuarios estén al tanto de las amenazas en materia de seguridad de la información y estén capacitados para respaldar la política de seguridad establecida por la IPS ASSALUD.

- **Aplicabilidad**: Esta Política es aplicable a todo el personal interno de la IPS ASSALUD, sin importar cual sea su situación, y al personal externo que se involucre en tareas dentro del ámbito del Organismo y relacionadas con la seguridad.

- **Directrices**:

  El departamento de gestión de talento humano deberá difundir entre los empleados e informar sobre las obligaciones con relación al cumplimiento de la política de seguridad de la información, además de dar a conocer la política de seguridad desde el proceso de selección.

  Los usuarios en general son responsables de cumplir la política de seguridad de la información y reportar las debilidades, amenazas, vulnerabilidades o cualquier incidente relacionado con la seguridad de la información al oficial de seguridad informática.

11.2.9 Seguridad física y ambiental de la IPS ASSALUD

- **Objetivos**

  - ✓ Evitar accesos no autorizados que causen daños o interferencia en los servicios informáticos, instalaciones y redes de la IPS Assalud.

  - ✓ Mantener protegido el equipamiento destinado a procesar la información de la IPS Assalud, tanto servidores como computadores de escritorio, portátiles, dispositivos de red, y demás, ubicándolos en áreas protegidas y con acceso restringido y controlado apropiadamente.

  - ✓ Proteger los activos sobre todo los de hardware que procesan información en caso de tener que ser trasladados fuera del perímetro protegido del debido a motivos de mantenimiento o reparaciones.

  - ✓ Gestionar y minimizar el riesgo de que factores ambientales de alguna manera puedan afectar el funcionamiento de la infraestructura informática de la institución.

  - ✓ Evitar perdida de equipos tanto en las oficinas, sala de servidores, o laboratorios de cómputo de la IPS Assalud.

- **Aplicabilidad**:

  Esta Política es aplicable a todos los elementos o recursos físicos que forman parte de la infraestructura, equipos de cómputo, servidores, medios de almacenamiento, dispositivos removibles, equipos de comunicación, cableado, redes no cableadas, y demás.

- **Directrices**:

  El oficial de seguridad informática en conjunto con las jefaturas de las diversas áreas deberá definir las áreas críticas que deben establecerse como zonas restringidas o dentro de un perímetro de seguridad así como la definición de las posibles amenazas ambientales para cada departamento y tomar las precauciones para mitigar el riesgo.

  El área de sistemas se encargara de seguir las indicaciones del Oficial de seguridad informática en cuanto a la implementación de las áreas protegidas y coordinara la contratación de empresas terceras en caso que se requiera. Las jefaturas departamentales definirán los niveles de acceso a establecerse para sus respectivas áreas.

12 RECOMENDACIONES

Como parte del estudio realizado, se tiene a consideración unas series de recomendaciones que ayudaran a reducir el índice de amenazas y riesgos en los activos de la IPS Assalud obtenidos en dicho estudio.

- Se recomienda mantener una constante revisión de la política de seguridad al SGSI y comprobar el cumplimiento de la misma por parte de los empleados de la IPS Assalud.

- Se recomienda establecer los mecanismos que permitan la identificación de nuevos activos de información, y también la cultura organizacional para tomar acciones correctivas frente a nuevas vulnerabilidades, amenazas o riesgos detectados; y con base en esa información tomar acciones preventivas.

- Se recomienda formar y capacitar de manera periódica al personal de la IPS Assalud en temas de seguridad de la información y así lograr que todos los involucrados o relacionados con los activos de información tengan los conocimientos claros frente a una necesidad.

13 DIVULGACIÓN

Con el fin de dar a conocer el presente proyecto se realizara un documento que será enviado a las directrices de la organización. Se selecciona este canal de comunicación teniendo en cuenta que el proyecto involucra información confidencial.

14 CONCLUSIONES

Luego de llevar a cabo el análisis de riesgo al sistema de información de la IPS ASSALUD, es coherente afirmar que la metodología MAGERIT es una metodología muy completa, cuya aplicación no genera gran dificultad y que junto a la herramienta EAR/PILAR, se consolida como un poderoso artefacto de análisis de riesgo, que permite una rápida ejecución de todas las fases contempladas por la metodología las cuales son rápidamente representadas en tablas que facilitan su comprensión.

El análisis realizado refleja que el sistema de la IPS ASSALUD se encuentra en una gran exposición a los riesgos, y en su gran mayoría se debe al poco conocimiento que tiene el personal sobre el manejo de la información, además de la carencia de políticas que controlen y marquen las pautas para el buen uso de este preciado activo.

Con la aplicación de los salvaguardas seleccionados y las políticas de seguridad sugerida se lograría una disminución significativa en los niveles de riesgos que presenta actualmente la IPS ASSALUD, está en manos de la gerencia la implementación y así evitar caer en un estado catastrófico y legalmente delicado debido al tipo de información que se maneja.

BIBLIOGRÁFICAS

- Alfonso García, Cervigón Hurtado, María del Pilar, (2011). Seguridad Informática. España – Madrid. (Pág. 19 - 20).

- ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. http://www.cybsec.com

- BUENAÑO QUINTANA, Jose Luis; GRANDES LUCES, Marcelo Alfonso, Planeacion y Diseño de un SGSI Basado en la Norma ISO/IEC 27001 – 27002. Tesis de Titulo como Ingeniero de Sistemas. Quito – Ecuador: Universidad Politécnica Salesiana. 2009.

- Congreso de Colombia. LEY 1273 DE 2009. [En Linea]. 1a ed. Bogota – Colombia. 2009. [18/Julio/2015]. Disponible en internet en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

- ERB, Markus. Amenazas y Vulnerabilidades en Seguridad Informáticos. [En Linea]. 3a ed. Madrid – España. Creative Commons Atribución-No Comercial-Compartir Obras Derivadas 2012. [12/Julio/2015] Disponible en Internet: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

- ERB, Markus. Análisis de Riesgos Informáticos. [En Linea]. 3a ed. Madrid – España. Creative Commons Atribución-No Comercial-Compartir Obras Derivadas 2012. [12/Julio/2015] Disponible en Internet: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

- ERB, Markus. Matriz para el Análisis de Riesgos. [En Linea]. 3a ed. Madrid – España. Creative Commons Atribución-No Comercial-Compartir Obras Derivadas 2012. [12/Julio/2015] Disponible en Internet: https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

- ERB, Markus. Seguridad de Informáticos y protección de datos. [En Linea]. 3a ed. Madrid – España. Creative Commons Atribución-No Comercial-Compartir Obras

Derivadas 2012. [12/Julio/2015] Disponible en Internet: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

- ERB, Markus. Seguridad Informáticos. [En Linea]. 3a ed. Madrid – España. Creative Commons Atribución-No Comercial-Compartir Obras Derivadas 2012. [12/Julio/2015] Disponible en Internet: https://protejete.wordpress.com/gdr_principal/definicion_si/

- FERNADEZ, Carlos M. Seguridad en sistemas informáticos. Ediciones Díaz de Santos S.A.. España. 1988. Página 105.

- GARCÍA ALFONSO; Hurtado Cervigón; ALEGRE RAMOS, María del Pilar. Seguridad informática. Madrid – España: Paraninfo SA. 2011.

- Gonzalo Morales, (2010). Seguridad Informática. España – Madrid. (Pág. 8 - 11)

- https://seguridadinformaticaufps.wikispaces.com/Conceptos+Basicos+Seguridad+Informatica

- ISO 27001. [En Linea]. 1a ed. Madrid – España. 2012. [18/Julio/2015]. Disponible en internet en: http://www.iso27000.es/sgsi.html

- Metodologia MAGERIT. [En Linea]. 1a ed. Madrid – España. 2012. [18/Julio/2015]. Disponible en internet en: https://seguridadinformaticaufps.wikispaces.com/MAGERIT

- PALLAS, Gustavo; CORTI María Eugenia. Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica. [En Linea]. 1a ed. Montevideo - Uruguay, Grupo de Seguridad Informática, Instituto de Computación, Facultad de Ingeniería, Universidad de la República. 2011. [18/Julio/2015]. Disponible en Internet: http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3%284%29.pdf

- RECIO, María Jesús. De la seguridad informática a la seguridad de la información. [En Linea]. 1a ed. Madrid – España. 2012. [18/Julio/2015]. Disponible en Internet: http://www.aec.es/c/document_library/get_file?uuid=e25028ca-cb3b-4ffd-ada0-4ce2efa86f80&groupId=10128

- REGUEIRO, Arturo. Autoridades de Certificación y Confianza Digital.[En Linea]. 1a ed. Madrid – España. 2012. [12/Julio/2015] Disponible en Internet: http://www.fundaciondike.org.ar/seguridad/firmadigital-autoridades.html

ANEXOS

ANEXO A

FORMATO ENCUESTA PARA EL PERSONAL ASISTENCIAL

ENCUESTA: SEGURIDAD INFORMÁTICA

Ésta información en confidencial y únicamente se usará para efectos de investigación dentro el proyecto de grado “Protocolo de Seguridad Informática para Universidades”.

Fecha de ingreso D_____M_____A_____

Cargo en la Empresa:

1. ¿Ha escuchado o sabe sobre la seguridad informática?

   Si
   No

2. ¿Le parece importante este Tema?

   Alto
   Medio
   Bajo
   No importante

3. En su tiempo libre que actividades se desempeña dentro de la red de la IPS Assalud (señale con una X):

Actividad	SI	NO
Trabajo		
Redes Sociales		
Descarga de Información		
Música		
Juegos en Línea		

4. ¿Conoce sobre políticas de seguridad informáticas implementadas en la universidad?

   SI

   NO

   ¿Cuáles? _____

GRACIAS POR SU ATENCIÓN

ANEXO B

FORMATO ENCUESTA PARA EL PERSONAL ADMINISTRATIVO

ENCUESTA: SEGURIDAD INFORMÁTICA

Ésta información en confidencial y únicamente se usará para efectos de investigación dentro el proyecto de grado “Protocolo de Seguridad Informática para Universidades”.

Fecha de ingreso D_____M_____A_____

Cargo en la Empresa:

5. ¿Ha escuchado o sabe sobre la seguridad informática?

   Si
   No

6. ¿Le parece importante este Tema?

   Alto
   Medio
   Bajo
   No importante

7. En su tiempo libre que actividades se desempeña dentro de la red de la IPS Assalud (señale con una X):

Actividad	SI	NO
Trabajo		
Redes Sociales		
Descarga de Información		
Música		
Juegos en Línea		

8. ¿Conoce sobre políticas de seguridad informáticas implementadas en la universidad?

   SI

   NO

   ¿Cuáles? _____

GRACIAS POR SU ATENCIÓN

ANEXO C

RESUMEN ANÁLITICO RAE.

Título de Documento.	DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA IPS ASSALUD DE COROZAL SUCRE, MEDIANTE LA IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT (V3.0) Y LA NORMA ISO 27001:2013
Autor	DIAZ RICARDO Luis Carlos
Palabras Claves	Activos, Metodología Margerit, Gestión de Riesgo, Sistemas de Información, Políticas de Seguridad Informáticas, Amenazas, Salvaguardas, ISO/IEC 27001- 27002, IPS Assalud, Información, Integridad, Disponibilidad, Confidencialidad, Trazabilidad, Autenticidad, Vulnerabilidad, Herramienta PILAR.
Descripción El proyecto Diseño de un Sistema de Gestión de la Seguridad de la Información en la IPS Assalud de Corozal Sucre, mediante la Implementación de la Metodología Margerit (v3.0) y la Norma ISO 27001:2013, es una monografía donde se analizaran las vulnerabilidades, amenazas y riesgos en los activos informáticos de esta entidad con el propósito de garantizar la protección de estos activos en cada una de sus dimensiones garantizando así un buen funcionamiento del Sistema de Información de la IPS Assalud.	
Fuentes Bibliográficas	BUENAÑO QUINTANA, Jose Luis; GRANDES LUCES, Marcelo Alfonso, Planeacion y Diseño de un SGSI Basado en la Norma ISO/IEC 27001 – 27002. Tesis de Titulo como Ingeniero de Sistemas. Quito – Ecuador: Universidad Politécnica Salesiana. 2009. Congreso de Colombia. LEY 1273 DE 2009. [En Linea]. 1a ed. Bogota – Colombia. 2009. [18/Julio/2015]. Disponible en internet en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492 ERB, Markus. Amenazas y Vulnerabilidades en Seguridad Informáticos. [En Linea]. 3a ed. Madrid – España. Creative Commons Atribución-No Comercial-Compartir Obras Derivadas 2012. [12/Julio/2015] Disponible en Internet: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

	ERB, Markus. Análisis de Riesgos Informáticos. [En Linea]. 3a ed. Madrid – España. Creative Commons Atribución-No Comercial-Compartir Obras Derivadas 2012. [12/Julio/2015] Disponible en Internet: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

Contenido:

Diseño de un Sistema de Gestión de la Seguridad de la Información en la IPS Assalud de Corozal Sucre, mediante la implementación de la Metodología Margerit (v3.0) y la Norma ISO 27001:2013

Descripción del Problema:

En la Institución Prestadoras de Servicios en Salud ASSALUD, no se le da la importancia necesaria a la seguridad informática, se puede decir que no tiene un buen diseño y estructura en su Sistema de Información, igualmente se observa que no tienen implementadas metodologías, técnicas o normas de seguridad estandarizadas que les permita garantizar la integridad del Sistema.

Actualmente en la IPS ASSALUD no se cuenta con ningún tipo de políticas de seguridad lo que incrementa los daños en los activos y peor aún dificultades para llevar a fin termino el desarrollo de su actividad principal, la cual consiste en atender a pacientes tanto en medicina general como especializada, manteniendo de esos pacientes su historial clínico y evoluciones por tratamientos.

Siendo esta la situación de la empresa y considerando que la información es un bien vital, se presenta una escenario critico el cual es la violación de la confidencialidad de la información ya que no se cuenta con perfiles designados para cada rol, todo usuario puede visualizar la información y además modificarla, lo que causa una gran falla en lo pertinente a la disponibilidad, confidencialidad e integridad de la información, si se mira desde la perspectiva de la metodología MAGERIT se encontrara una gran falencia en esas dimensiones de valoración de activo.

¿El diseño de un sistema de gestión de la seguridad de la información podrá minimizar las vulnerabilidades, amenazas y riesgos asociados al uso del sistema de información de la IPS ASSALUD?

Objetivo General.

Diseñar un Sistema de Gestión de la Seguridad de la Información adecuado para la corrección de los problemas de seguridad de la información de la IPS ASSALUD de Corozal-Sucre, mediante la implementación de la metodología MAGERIT y la norma ISO 27001:2013.

Objetivos Específicos.

- Identificar, clasificar y valorar los activos con los que cuenta el sistema de información de la IPS ASSALUD aplicando la metodología MAGERIT.

- Identificar y valorar las amenazas presentes en los activos del sistema de información de la IPS ASSALUD aplicando la metodología MAGERIT.

- Gestionar los riegos y especificar salvaguardas, que permitan controlar los riesgos posibles en la IPS ASSALUD, según lo dispuesto en la metodología MAGERIT.

- Crear un Sistema de Políticas de Seguridad que permita optimizar el sistema de seguridad de información manejado actualmente en la IPS ASSALUD.

Metodología.

La metodología de investigación a utilizar será de campo, la cual permitirá corroborar el estado actual del sistema de información con el que cuenta la IPS ASSALUD, partiendo de la identificación de sus activos y verificando que amenazas son propensas y como deberán ser manejadas en caso de materializarse.

Tomando como referencia la metodología MAGERIT y la norma ISO 27001:2013, la línea de investigación de este proyecto se enmarcara en el *Análisis y Gestión de Riesgos en los Activos.*

Referencia Teóricas	**Seguridad de la Información** (De este término se deriva el concepto de seguridad informática la cual según Aguilera López "Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información segura y confiable."(Aguilera López, Purificación, 2010)) **ISO/ IEC 27001** (La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) tomado de https://advisera.com/27001academy/es/que-es-iso-27001/) **Sistema de Gestión de Seguridad de la Información (SGSI).** (tomado de http://www.pmg-ssi.com/2015/07/que-es-sgsi/) **Metodología MAGERIT**. (Portal administración electrónica. MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los sistemas de información. [En línea]. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pe_Magerit.html#.VCmVZhZRVJQ)
Referencias Conceptuales	**Integridad:** Protección de la información respecto a modificaciones no autorizadas, tanto a la almacenada en los elementos computarizados de la organización como la usada como soporte. Estas modificaciones pueden llevarse a cabo de manera accidental, intencional, o por errores de hardware-software **Autenticidad:** Garantía que el usuario autorizado tiene para usar un recurso y que no sea suplantado por otro usuario. **Control de Acceso:** Posibilidad de controlar los permisos a cualquier usuario para acceder a servicios o datos de la organización. **Auditoría:** Capacidad para determinar todos los movimientos del sistema, como accesos, transferencias, modificaciones, etc., en el momento en que fueron llevados a cabo (fecha y hora). **Amenaza:** Será cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. De esta manera, el punto más débil.

	Vulnerabilidad: Consiste en cualquier debilidad que puede explotarse para causar pérdida o daño del sistema. De esta manera, el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.
Resultados	En base al estudio anteriormente realizado se puede diseñar un SGSI con el cual se lograra minimizar considerablemente los riesgos asociados al uso de la información y se mantendrán normalizado los procesos ya existente ajustándose a las necesidades de la IPS Assalud. Es importante tener en cuenta que se requerirá realizar cambios en los procesos Administrativos de la IPS, y existirá un impacto principalmente en el recurso humano durante el proceso de concienciación y adopción de cultura de Seguridad Informática.
Conclusiones	Luego de llevar a cabo el análisis de riesgo al sistema de información de la IPS ASSALUD, es coherente afirmar que la metodología MAGERIT es una metodología muy completa, cuya aplicación no genera gran dificultad y que junto a la herramienta EAR/PILAR, se consolida como un poderoso artefacto de análisis de riesgo, que permite una rápida ejecución de todas las fases contempladas por la metodología las cuales son rápidamente representadas en tablas que facilitan su comprensión. El análisis realizado refleja que el sistema de la IPS ASSALUD se encuentra en una gran exposición a los riesgos, y en su gran mayoría se debe al poco conocimiento que tiene el personal sobre el manejo de la información, además de la carencia de políticas que controlen y marquen las pautas para el buen uso de este preciado activo. Con la aplicación de los salvaguardas seleccionados y las políticas de seguridad sugerida se lograría una disminución significativa en los niveles de riesgos que presenta actualmente la IPS ASSALUD, está en manos de la gerencia la implementación y así evitar caer en un estado catastrófico y legalmente delicado debido al tipo de información que se maneja.

ANEXO D

Tabla de Impacto y Riesgo Acumulado