REALIZAR EL ANÁLISIS PARA GESTIÓN DE RIESGOS EN LOS SISTEMAS DE INFORMACIÓN DE LA IPS SOLIDARIOS SALUD DEL MUNICIPIO DE CUASPUD CARLOSAMA A PARTIR DE LA NORMA ISO 27001 APLICANDO LA METODOLOGÍA MAGERIT

FABIO ADALBERTO ARELLANO MONTENEGRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2018

REALIZAR EL ANÁLISIS PARA GESTIÓN DE RIESGOS EN LOS SISTEMAS DE INFORMACIÓN DE LA IPS SOLIDARIOS SALUD DEL MUNICIPIO DE CUASPUD CARLOSAMA A PARTIR DE LA NORMA ISO 27001 APLICANDO LA METODOLOGÍA MAGERIT

FABIO ADALBERTO ARELLANO MONTENEGRO

Trabajo de grado para optar el título de Especialista en Seguridad Informática

ASESOR
ING. MARTIN CAMILO CANCELADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2018

Nota de aceptación

Firma del Director

Firma del Jurado

Firma del Jurado

Pasto, 21 de Octubre 2018

DEDICATORIA

Este proyecto está dedicado a **DIOS,** por darme la vida a través de mis queridos **PADRES** quienes con su respecto, cariño, amor y ejemplo han hecho de mí una persona con valores para poder desenvolverme como: **HIJO, HERMANO Y PROFESIONAL.**

A mi **Esposa,** por apoyar y dedicar su tiempo para alcanzar y finalizar este proyecto.

A mis **Hermanos**, por estar siempre apoyándome incondicionalmente en el logro de mis objetivos propuestos.

A todos mis **Familiares y Amigos** que de alguna u otra manera han contribuido para que culmine esta meta anhelada.

AGRADECIMIENTOS

A la IPS Solidarios Ltda., por permitir realizar el presente proyecto y brindar toda la información necesaria para su desarrollo.

A la UNAD y sus docentes, por permitir adquirir nuevos conocimientos en materia de Seguridad Informática.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCIÓN

Sin duda alguna, desde el momento en que aparece la primera computadora ha producido efectos significativos en el que hacer de las personas y las organizaciones. Es inevitable su utilización en los diferentes ámbitos laborales, por permitir mejorar de manera más eficaz las tareas diarias, a través de diferentes herramientas de software y hardware, que facilitan, su organización, procesamiento y manera de presentar o transmitir la información, catalogándola ésta, como el activo más valioso. Además, el acelerado avance tecnológico, ha contribuido en proporcionar nuevas alternativas de agilizar y mejorar la realización de las actividades empresariales, pero a su vez, y al tiempo, han surgido diferentes maneras y técnicas de realizar ataques contra los sistemas informáticos de las organizaciones e individuos. En éste sentido, se resalta la necesidad de mantener la información, conservar y protegerla frente al acceso no autorizado de terceros o delincuentes informáticos que quieran apropiarse, causar daño alguno o sacar provecho de la misma; utilizando métodos y técnicas de hacking que para ello conlleve.

De esta manera, hoy en día las organizaciones han tomado conciencia de proteger su activo más importante, como es la información y sus recursos informáticos de posibles amenazas a que se ven expuestas. Por esta razón es necesario saber identificarlos, categorizar y darle un valor de acuerdo a su importancia dentro de la organización a fin de garantizar su confidencialidad, integridad y disponibilidad como pilares fundamentales de la seguridad de la información.

Con el presente proyecto de investigación se pretende realizar un estudio para el Análisis y Gestión de Riesgos de los Sistemas de Información en la IPS Solidarios Salud, ubicada en el municipio de Cuaspud Carlosama, aplicando el modelo

MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de información y comunicación.

La metodología planteada permite hacer una evaluación de los activos de la empresa, determinar las amenazas, salvaguardas, vulnerabilidades, impactos y riegos a que está expuesta la institución.

Lo anterior con el fin de identificar los riegos críticos y plantear las medidas de seguridad necesarias para enfrentarlos utilizando las salvaguardas ha lugar.

En este orden el proyecto de investigación tratará aspectos relativos a la IPS Solidarios Salud, como es, la reseña histórica, el tipo de entidad dentro del sector salud y la formalización de la plataforma estratégica, además los conceptos referentes de la Metodología MAGERIT v 3.0, el desarrollo y aplicabilidad en la IPS Solidarios Salud, como también, se efectuará el análisis e identificación de los riesgos como aporte central en el presente proyecto, y se culminará el trabajo con la Gestión de Riesgos.

1. TÍTULO DEL PROYECTO

Realizar el análisis para la gestión de riesgos en los sistemas de información de la IPS Solidarios Salud del municipio de Cuaspud Carlosama a partir de la norma ISO 27001 aplicando la Metodología MAGERIT.

2. DESCRIPCIÓN DEL PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

La IPS Solidarios es una institución que presta servicios de salud a la población de Cuaspud Carlosama, enfocando su quehacer en la recuperación de pacientes, a través de terapias proporcionadas en localidad. La IPS Solidarios cuenta con una red de computadoras e informática, que permite realizar sus actividades operativas y de administración, como es el caso de la facturación, generación de RIPS y presentación de informes a las diferentes entidades públicas, privadas y Entes de Control. De esta manera, ésta red de datos, se convierte en el medio indispensable y relevante para la realización, procesamiento y gestión de las actividades diarias que la institución oferta.

Desafortunadamente, la IPS Solidarios, carece de una debida protección y administración de sus recursos informáticos; el fácil acceso a sus equipos computacionales, pueden convertirlos en sistemas informáticos vulnerables por no contar con los debidos controles. También, el acceso no restringido de internet al personal de la institución, puede convertirse en un medio visible a posibles atacantes, generando consecuencias catastróficas como el robo de información, secuestro o encriptación por ransomware, e incluso su perdida.

De esta manera, se pretende como tema de investigación considerar la aplicación de la Metodología MAGERIT, para realizar un estudio del análisis y gestión de riesgos en los sistemas de información de la IPS Solidarios Salud del municipio de Cuaspud Carlosama. Cabe resaltar que por el momento no existe una valoración de los activos en la institución, de igual manera no se ha identificado las amenazas a que está expuesta, y no se cuenta con un documento o política institucional que tenga en cuenta la protección de la información y su custodia. Además el

desconocimiento de como salvaguardar la información que se procesa en la institución por parte del personal que ahí labora.

De acuerdo la evaluación preliminar efectuada, consecuencia de las entrevistas realizadas a los respectivos socios, observación y análisis de documentos se encuentra que la IPS Solidarios Salud, se encontró que no cuenta con un estudio relativo a un sistema de análisis y gestión de riesgos.

En este orden se prevé aplicar el modelo MAGERIT, para identificar, evaluar y gestionar los riegos derivados del uso de tecnologías de la información y comunicaciones.

Lo anterior, con el fin de establecer el nivel actual de los riegos e identificar las salvaguardas más apropiadas para mitigar su impacto.

2.2 FORMULACIÓN DEL PROBLEMA

¿A través del estudio del análisis y gestión de riesgos que prevé la metodología MAGERIT, apoyada en las normas ISO 27001 y 27002 se podría mejorar la seguridad de los sistemas de información de la empresa IPS Solidarios Salud del Municipio de Cuaspud Carlosama?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar el análisis para gestión de riesgos en los sistemas de información de la IPS Solidarios Salud del municipio de Cuaspud Carlosama a partir de la norma ISO 27001 aplicando la Metodología MAGERIT.

3.2 OBJETIVOS ESPECIFICOS

- Describir la institución objeto de estudio para determinar sus antecedentes, plataforma estratégica, portafolio de servicios y activos.
- Aplicar la metodología MAGERIT para el análisis de los riesgos, identificando los activos, las amenazas, vulnerabilidades, controles, impacto y riesgo.
- Aplicar la metodología MAGERIT para la gestión de riesgos estableciendo la interpretación de los valores de impacto y riesgo
- Verificar los controles existentes en la norma ISO 27002 que mejor se adecuen a la IPS Solidarios Salud.

4. JUSTIFICACIÓN

En la actualidad, toda organización que utilice recursos informáticos para la gestión de información, como es su captura desde diferentes fuentes, el almacenamiento, custodia, procesamiento y entrega final a las partes interesadas, además, del manejo de sus activos, como parte esencial del desarrollo de la gestión administrativa y operativa, se convierte en un posible objetivo de delincuentes informáticos, que pretendan obtener provecho de las vulnerabilidades del sistema de información y los deficientes controles que puedan existir, exponiéndolos a potenciales amenazas y de igual manera aun ataque informático. Su materialización, conduciría a consecuencias catastróficas como el robo de información, denegación del servicio, saboteo, eliminación de información y secuestro informático; entre otros peligros que se puedan generar, impidiendo que se puedan cumplir los objetivos misionales de la organización.

También, la gran mayoría de organizaciones aún no han evaluado la importancia de proteger la información como el recurso más valioso que conservan, independiente del tamaño organizacional que ésta sea. Al no disponer, perder o sufrir alguna alteración de éste recurso, las actividades operacionales y administrativas de la organización se verán afectadas y de este modo se reflejará en su bajo crecimiento y desarrollo institucional.

Por tanto, la IPS Solidarios, no es ajena a esta necesidad de tener una adecuada seguridad y protección de sus activos. La información contenida en el sistema de facturación, estadística, historias clínicas y contable, son recursos necesarios e indispensables que permiten lograr y cumplir los objetivos misionales.

Con esta investigación se pretende realizar un estudio para el Análisis y Gestión de Riesgos de los Sistemas de información de la IPS Solidarios Salud Cuaspud

Carlosama a partir de la ISO 27001 aplicando el modelo MAGERIT con el fin de apoyar y preservar los sistemas de información y comunicación.

La metodología MAGERIT es una de las herramientas más idóneas para aplicarla en la IPS Solidarios Salud, en consideración al portafolio de servicios que ofrece, pues le será de gran ayuda aplicar las conclusiones y recomendaciones que se deriven del presente estudio frente al manejo de información contenida en sus equipos de cómputo. La información, específicamente se refiere a historias Clínicas, facturación, contabilidad; insumos para presentar los informes a los Entes de Control, estadísticas, entre otras.

Al finalizar el estudio la IPS Solidarios Salud, afianzará los pilares de la seguridad informática que son confidencialidad, integridad y disponibilidad de la información.

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

El presente proyecto se desarrollará en la IPS Solidarios Salud, con domicilio principal en el municipio de Cuaspud Carlosama (Nariño), con el fin de realizar un estudio para el Análisis y Gestión de Riesgos de los Sistemas de información en la IPS Solidarios Salud, aplicando la Metodología MAGERIT y los estándares ISO/IEC 27001 e ISO/IEC 27002 para la verificación de controles existentes, a fin de contribuir a la mejora del actual proceso que se lleva a cabo en la entidad, buscando promover en los funcionarios mejores prácticas sobre el tratamiento, administración, custodia y protección de la información, propiciando una adecuada cultura en materia de seguridad informática.

6. METODOLOGÍA

6.1 TIPO DE INVESTIVACION

Según el nivel de medición y análisis de la información se realizará una investigación documental, específicamente, descriptiva, por permitir observar y describir como la IPS SOLIDARIOS SALUD, desarrolla actualmente sus procesos, identifica y custodia los activos, la manera como el personal realiza las actividades en la entidad y la interrelación con las entidades externas que la controlan; también, por dar cuenta de la existencia jurídica de la IPS Solidarios Salud y de su funcionamiento, a fin de establecer un estudio del análisis y gestión de riesgos de los sistemas de información de la institución a través de la Metodología MAGERIT, a partir de la ISO 27001.

También se realiza una investigación cualitativa por establecer relación de los activos, con las posibles vulnerabilidades encontradas, las amenazas que se puedan producir y la determinación del nivel riesgo en que se encuentre los sistemas de información de la entidad, si llegaran a materializar.

Además, para aplicar la Metodología MAGERIT, se identificarán los activos, se los valorará, se en listaran las amenazas, vulnerabilidades, salvaguardas y tratamiento, y posteriormente presentar las conclusiones y recomendaciones sobre la efectividad de los controles existentes y los que resulten necesarios implementar.

La Metodología MAGERIT es la idónea para elaborar el análisis y gestión de riesgos en una organización, toda vez que permite gestionar la Seguridad de Información.

6.2 POBLACION Y MUESTRA

La población objeto del proyecto son las personas que interactúan en los procesos informáticos de la IPS Solidarios Salud del Municipio de Cuaspud Carlosama. Para el presente estudio, se tendrá en cuenta el siguiente personal:

Tabla 1 Usuarios Objeto de Estudio

Cargo	Cantidad
Gerente	1
Secretaria	1
Facturador	1
Terapeutas	3
Sistemas	1
Asesor	1
Servicios Generales	1
Contador Público	1
Total	**10**

Fuente: El Autor

También se tiene en cuenta, el aporte entregado por los 3 Socios de la entidad.

6.3 TECNICAS DE ANALISIS Y PROCESAMIENTO DE DATOS

La Metodología MAGERIT, permitirá aplicar toda la información recogida para consolidarla y evaluarla. Se acudirá a entrevistas directas a los socios de la empresa, al personal, se realizará visita a las áreas de trabajo y revisión de activos.

6.4 METODOLOGIA DE DESARROLLO

Las actividades requeridas para el proceso de análisis y gestión de riesgos de la IPS Solidarios Salud, van a estar definidas por la metodología de gestión de riesgos MAGERIT, y son las siguientes:

a) Actividades preliminares
   - ✓ Visita y reconocimiento de la empresa
   - ✓ Identificar la información y procesos de la empresa
   - ✓ Entrevistas directas a socios y gerente
   - ✓ Entrevistas al personal.

b) Análisis de riesgos
   - ✓ Realizar el inventario de activos de información
   - ✓ Identificar y valorar las amenazas a las que están expuesta los activos.
   - ✓ Determinación del impacto potencial
   - ✓ Determinación del riesgo potencial
   - ✓ Estimar el estado del riesgo.
   - ✓ Gestión del Riesgo.
   - ✓ Determinar los controles según ISO 27001 y 27002

7. MARCO REFERENCIAL

7.1 MARCO DE ANTECEDENTES

Para el desarrollo de esta investigación se presentó los siguientes estudios de referencia:

Yamile Quintero, presenta en su trabajo de grado la aplicación de la metodología Magerit versión 3, enfocado al análisis y gestión de riesgos de los sistemas de información de la alcaldía municipal de Tuluá durante el año 2015, la que define la gestión del riesgo en dos fases: la etapa de análisis y la etapa de tratamiento del riesgo. En la primera etapa centraliza su estudio en la identificación de activos, identificación de amenazas y la determinación de salvaguardas para mitigar el riesgo, en la etapa de tratamiento del riesgo determina las posibles acciones que deben abordar en temas de seguridad para minimizarlo, y finalmente con los resultados que se obtuvieron en las etapas anteriores, se realizan la formalización de políticas de seguridad.

Este proyecto permitirá fortalecer el conocimiento sobre la aplicabilidad de la metodología Magerit y obtener una mejor visión sobre la etapa de análisis y tratamiento de los riesgos.

Antonio Lucero y John Valverde, formalizan un proyecto de grado sobre el análisis y gestión de riesgos de los sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo durante el año 2012, proponiendo como objetivo la Aplicación de la Metodología Magerit versión 2., el que les permite contribuir a la institución posea un conocimiento claro sobre los riesgos que puedan presentarse en sus sistemas de información. También formalizan la utilización de la herramienta PILAR Basic, permitiéndoles mejorar la identificación de los activos, las amenazas y la incorporación de salvaguardas a fin de minimizar el riesgo.

Este proyecto ayudará a contextualizar y mejorar la identificación de los activos, amenazas, vulnerabilidades y riesgos utilizando alternativamente algunas herramientas y tecnologías informáticas en la IPS Solidarios.

El Ingeniero Luis Enrique Giraldo Cepeda, realiza un estudio y análisis para la implementación de un sistema de gestión de la seguridad de la información según la norma ISO 27001 en la empresa SERVIDOC S.A durante la vigencia 2016. El análisis lo formaliza por medio de fases, donde incluye entrevistas, observación directa y la aplicación de la metodología de análisis de riesgos Magerit Versión 3., la que le permitió realizar un análisis para la implementación de un Sistema de Gestión de Seguridad Informática que le ayude a identificar amenazas, vulnerabilidades y riesgos que pueden afectar la organización específicamente en las áreas de contabilidad, facturación e Historias clínicas. Al final y obtenido sus resultados, se identificaron los riesgos y la forma de mitigarlos, dejando en claro recomendaciones y sugerencias a proyectos que la empresa debe implementar para cubrir estas debilidades; también logró identificar el nivel en que se encontraba la seguridad informática de la organización.

El proyecto se relaciona con la presente investigación, por hacer uso de la norma ISO 27001 y la utilización de la metodología Magerit Ver. 3.0 para la identificación de activos, amenazas, vulnerabilidades y la gestión del riesgo.

Yeinny Bolivar, presenta en su trabajo de grado el diseño de un sistema de gestión de seguridad de la información en la intranet del Policlínico del sur Olaya Bogotá, bajo la norma ISO 27001 durante la vigencia 2016, cuyo objetivo fundamental fue el análisis y gestión de riesgos de la organización, el estudio de la metodología Magerit, y la norma ISO 27001, realizando la identificación de los activos, amenazas, el impacto y riesgo que estos presentan dentro de la Institución, para con estos datos luego llegar a la obtención de la matriz de riesgos con la finalidad de escoger los controles y objetivos más adecuados de la norma ISO 27001.

De igual manera lo expuesto anteriormente se relaciona con la presente investigación, por hacer uso de la norma ISO 27001 y la utilización de la metodología Magerit Ver. 3.0 para la identificación de activos, amenazas, vulnerabilidades y la gestión del riesgo.

Henry Bastidas, Iván López y Hernando Peña. Realizan un estudio sobre el análisis de riesgos y recomendaciones de seguridad de la información al área de información y tecnología del Hospital Susana López de Valencia de la ciudad de Popayán durante la vigencia 2014. Que buscan mediante el uso de controles, estándares, herramientas y recomendaciones vigentes, determinar el diagnóstico de seguridad de la información en la División de Tecnologías de la Información y las Comunicaciones del Hospital Susana López de Valencia de la ciudad de Popayán con el fin de establecer políticas y procedimientos en relación a los objetivos de la institución, en busca de minimizar los riesgos en la alteración de la información.

Los anteriores estudios aportan a este trabajo, bases de orientación, relacionadas con la identificación de activos, la determinación de amenazas e impacto y la gestión del riesgo, a través de metodologías como lo es Magerit v.30 y la ISO 27001, enfocada a la creación de sistemas de información de gestión del además el establecimiento de políticas de seguridad de información para su mejor control y mitigación.

7.2 MARCO CONTEXTUAL

SOLIDARIOS SALUD IPS

Reseña Histórica

En cuanto a la empresa Solidarios Salud IPS limitada se debe indicar que se encuentra ubica en el municipio de Cuaspud Carlosama al sur occidente del

Departamento de Nariño. Es una Institución Prestadora de Servicios de Salud de Segundo Nivel. Presta servicios de terapias a la población del municipio de Cuaspud y sus alrededores; fue creada en el mes de agosto del año 2008 gracias a la idea de 3 profesionales de la salud y con el deseo de brindar servicios terapéuticos en el mismo municipio para ayudar a que los pacientes no realizaran desplazamientos largos a otros municipios para recibir una buena atención.

Figura 1 Instalaciones Físicas de la IPS Solidarios

Fuente: El Autor

Figura 2 Servicios de Salud Prestados.

Fuente. El Autor

PORTAFOLIO SE SERVICIOS[1], es una persona jurídica cuyo portafolio de servicios básicamente comprende Atención Para Rehabilitación Funcional en las áreas de Terapia Física, Terapia Ocupacional, Terapia del Lenguaje y Psicología, a través de terapeutas ocupacionales, fisioterapeutas, fonoaudiólogos y psicólogos.

La IPS se fundó por un grupo de profesionales de la salud con el ideal de crear un centro de apoyo integral para las personas que requerían ese tipo de servicios de salud con calidad humana.

La MISIÓN de la IPS es ser *"una Institución Prestadora de Servicios de Salud comprometida en los procesos de atención integral que busca mejorar la calidad de vida del individuo con disfunción física, cognitiva, sensorial, comportamental y alteraciones temporales, de acuerdo a la etapa de vida en la que se encuentre, que afecte su funcionalidad e independencia en su realización personal, familiar y social brindando servicios de apoyo en las áreas de Fonoaudiología, Fisioterapia, Psicología y Terapia Ocupacional"*[2]

VISIÓN es ser *"pionera en la atención personalizada que permita satisfacer las necesidades de la población con respecto a su salud mental, física y sensorial, a través de procesos óptimos y de talento humano comprometido, altamente calificado que garanticen la prestación de servicios de reconocida calidad y eficiencia".*[3]

La IPS, existe desde el año 2008 y con el transcurrir del tiempo fue adquiriendo diferentes tipos de software para organizar las historias clínicas, la facturación y la contabilidad de la empresa; de igual modo, la empresa requiere presentar información tributaria ante la Dirección de Impuestos y Aduanas Nacionales DIAN

[1] IPS SOLIDARIOS SALUD. Portafolio de Servicios. 2008
[2] Ibíd., p. 3.
[3] Ibíd., p. 3.

(retención en la fuente, información exógena, impuesto como el CREE, en fin) y otro tipo de información ante las Autoridades de Salud.

Ahora bien, siendo la información el activo más valioso de la Empresa, encontramos que la IPS permite que la misma circule sin mayor prevención, por ello, se ha formulado el problema planteado en el presente proyecto.

7.3 MARCO CONCEPTUAL

Activos: Se puede decir que los activos son todos los elementos que hacen parte de un sistema de información, estos pueden ser hardware, software, instalaciones, los servicios prestados.

Amenaza: Son problemas que pueden afectar los activos de la organización, esas pueden ser origen humano que a su vez pueden ser sin intención como las causadas por negligencia y las malintencionadas que pueden ser internas o externas, el otro tipo de amenazas son las causadas por fenómenos de origen natural.

Vulnerabilidad: Se considera como vulnerabilidad la debilidad que posee un bien y que puede ser aprovechada por una amenaza para materializarse, esta es la razón por la cual se debe trabajar bastante en aspectos de seguridad informática.

Impacto: Son las consecuencias que sufre un activo cuando una amenaza se materializa.

Riesgo: Es la probabilidad de que ocurra un evento y sus consecuencias negativas ocasionando daños o perdidas.

Disponibilidad: La información siempre está disponible, es caso de presentarse alguna falla, debe estar en capacidad de recuperarse rápidamente

Confidencialidad: La información solo puede ser consultada y modificada por personal autorizado.

Integridad: Que la información no haya sido modificada, es decir que sea igual a los datos de origen.

Desastres de origen natural: Accidentes causados por fenómenos naturales (terremotos, inundaciones,…).

Desastres de origen industrial: Accidentes causados por desastres industriales (contaminación, fallos eléctricos,…).

Errores y fallos no intencionados: Estos accidentes normalmente son causados por personal con permisos para acceder al sistema y causan fallas en el sistema por error o por omitir algunos procesos.

Ataques intencionados: Este tipo de ataques es causado por personal con acceso a la información y atacan el sistema con intenciones de conseguir un beneficio propio.

7.4 MARCO TEORICO

DESCRIPCION DE LA METODOLOGIA MAGERIT:

La utilización de tecnologías de la información y comunicaciones (TIC) como lo describe el Libro I de MAGERIT – Versión 3.0 considera unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben gestionarse

prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios. De igual forma, estamos llamados a considerar que la información es el activo más preciado de la empresa, razón por la cual, debe preservase en su integridad, disponibilidad y confidencialidad.

Integridad: Representa la probidad de la información para el correcto funcionamiento de la empresa.

Disponibilidad: Garantiza el acceso a la información permitiendo que la misma circule entre los integrantes de la organización.

Confidencialidad: Significa que la información de la empresa únicamente llega al personal debidamente autorizado.

En este sentido, el análisis y la gestión de riesgos hace parte de la seguridad de la información que manejan las empresas, por ello resulta necesario identificar, evaluar y controlar los riesgos a los cuales está expuesta la información, implementando la metodología que ha bien tengan para su administración.

Riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización[4]. De ahí que resulte necesario enlistar loso activos con sus respectivas características a fin de identificar los peligros a los que se encuentran expuestos.

El análisis del riesgo es un proceso sistemático para estimar la magnitud de los riesgos a que está expuesta la organización[5] . Este proceso cuantifica los activos de la empresa respeto de su protección actual.

[4] ESPAÑA PAE. G. d. (26 de 09 de 2014). Agencia Estatal Boletín Oficial del Estado. Obtenido de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-9741
[5] ESPAÑA, op. cit, p.15.

La gestión de los riesgos, consiste en la selección e implementación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riegos identificados[6]. La gestión de los riesgos conlleva a la determinación de las políticas de seguridad de la empresa para el manejo de la información y comunicación.

Como ocurre para el desarrollo de la presente investigación, se implementara la metodología MAGERIT, dicha metodología fue elaborada por el Consejo Superior de Administración Electrónica de España (hoy Comisión de Estrategia TIC - Real Decreto 806/2014, de 26 de septiembre[7]), para analizar y gestionar los riesgos derivados del uso de tecnologías de la información y comunicaciones, esto, con el fin de implementar las medidas de control más adecuadas para mitigar los riesgos.

Tabla 2 Comparación de Versiones de Magerit

MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información		
MAGERIT V.3	**MAGERIT V 2.0**	**MAGERIT V 1.0**
Se publicó en 2012 Se encuentra la herramienta computarizada PILAR Comprende tres libros: Libro I o Método: Conserva la estructura contenida en MAGERIT V 2.0 pero acoge los fundamentos ISO Libro II o Catálogo de Elementos	Se publicó en 2005 Tiene los siguientes libros: Libro I o Método: relativo a los argumentos fundamento del modelo previsto para la gestión de riesgos Libro II o Catálogo de Elementos: Contiene la relación de activos	Se publicó en 1997 No incluía la conceptualización del el denominado Sub modelo de Elementos, activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas. La fase de “sub estados de seguridad” ahora se denomina “dimensiones”, que incluye novedosos

[6] Ibíd., p. 15
[7] Ibíd., p. 15

MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información		
MAGERIT V.3	**MAGERIT V 2.0**	**MAGERIT V 1.0**
Libro III o Guía de Técnicas En general, los cambios que acoge MAGERIT V.3 son beneficios por lo siguiente: Recoge las sugerencias de las experiencias comunicadas y los dictámenes de las normas internacionales de ISO como referente obligado. Contiene un texto más amigable en su lectura y comprensión. MAGERIT persigue los siguientes objetivos: Directos: Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC) Ayudar a descubrir y planificar el tratamiento oportuno para mantener los	con sus posibles características de valoración, así como una relación de amenazas y controles por observar. En este aparte se pueden revisar ejemplos de análisis con diferentes técnicas. Libro III o Guía de Técnicas: Propone las técnicas para el análisis de riesgos. Se encuentra la herramienta computarizada PILAR.	parámetros para identificar y definir los activos. El sub modelo de procesos aparece bajo el epígrafe de “estructuración del proyecto de análisis y gestión de riesgos”. Incluye siete libros, cuyos contenidos, específicamente han evolucionado en lo relativo a los aspectos técnicos de los sistemas de información y comunicación. Libro I. Guía de aproximación a la seguridad de los sistemas de información. Libro II. Guía de procedimientos Libro III. Guía de técnicas Libro IV. Guía para desarrolladores de aplicaciones Libro V. Guía para responsables del dominio protegible

MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información		
MAGERIT V.3	**MAGERIT V 2.0**	**MAGERIT V 1.0**
riesgos bajo control Indirectos: Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso MAGERIT versión 3 se ha estructurado en tres libros: "Método", "Catálogo de Elementos" y "Guía de Técnicas".		Libro VI. Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos Libro VII. Referencia de normas legales y técnicas

Fuente: El Autor

En la página web institucional del Centro de Transferencia de Tecnología de España[8] , se indica que: “MAGERIT permite Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.

Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios”.

[8] ELECTRONICA, op. cit, p.11.

El análisis y gestión de los riesgos a través dela Metodología MAGERIT[9], es beneficioso para la empresa porque permite generar conciencia de su existencia, examinarlos, tratarlos y por ende la debida preparación para enfrentar a las auditorias, certificaciones o acreditaciones gubernamentales.

El análisis y gestión de riesgos dentro de una Organización, se estructura como uno de los principales pilares para resguardar la seguridad de la misma, entendida como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o mal intencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles[10] .

Actualmente se encuentra vigente MAGERIT versión 3 por lo tanto, la investigación seguirá los libros y las Guía de Técnicas que la integran, pues implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los interesados tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

El Proceso de Gestión de Riesgos, como se señala en libro I de la Metodología (página 19), es un conjunto de actividades encaminadas al análisis del riesgo para establecer cómo es, cuánto vale y que tan protegido se encuentra el sistema de acuerdo a sus objetivos, políticas y estrategias a fin de elaborar el respectivo plan

[9] BOCANEGRA QUINTERO, Yamilet, Análisis y gestión de riesgos de los sistemas de información de la alcaldía municipal de Tuluá aplicando la metodología MAGERIT. Obtenido de http://repository.unad.edu.co/handle/10596/3632

[10] ESPAÑA, MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, octubre 2012.- NIPO: 630-12-171-8. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WNxY_G81_IU

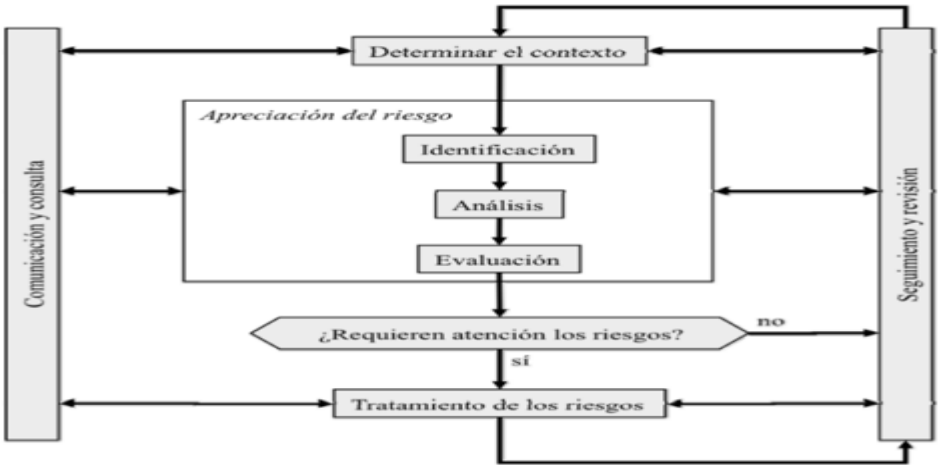
de seguridad. De igual modo, se establece una segunda etapa que concierne al tratamiento de los riesgos (página 19), para enfrentar en la debida forma las situaciones que se sobrevengan.

Figura 3 Gestión de Riesgos

Fuente: Metodología Magerit V3.

La metodología MAGERIT propone el siguiente esquema para la gestión de los riesgos:

Figura 4 Proceso de gestión de riesgos (ISO: 31000)



Fuente: Metodología Magerit V3.

En virtud de lo expuesto, se pretende desarrollar los siguientes ítems:

Método de análisis de riesgos:

Permitirá determinar los activos, las amenazas a las que están expuestos, las salvaguardas dispuestas y el impacto o el daño sobre el activo derivado de la materialización de la amenaza. Esto, con el fin de estimar el riesgo.
Análisis del riesgo:

Permitirá determinar los impactos y riesgos. Los impactos recogen los daños posibles y los riegos el daño probable. A partir del análisis efectuado se puede determinar que se quiere proteger y como. Es decir, es la evaluación y tratamiento en sí mismas consideradas.

Tratamiento del riesgo:

Permite eliminar o mitigar el riesgo.
Determinación del plan de seguridad.
Permite materializar las decisiones adoptadas para el tratamiento del riesgo.

7.5 MARCO LEGAL

Se presenta las siguientes normas y leyes como pilares de la protección de la información y su preservación:

Ley estatutaria 1266 de 2008 (Diciembre 31): Disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países[11].

[11] COLOMBIA, SECRETARIA DEL SENADO. Ley 1266 de 2008. Consultado el 10 de Junio de 2018 en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Decreto 1151 de 2008 (Abril 14). Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005 y se dictan otras disposiciones[12].

Ley 1273 de 2009 (Enero 05): 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[13].

Ley 1581 de 2012 (Octubre 17). Por la cual se dictan disposiciones generales para la protección de datos personales[14].

Decreto 1377 de 2013 (Junio 27). Por el cual se reglamenta parcialmente la Ley 1581 de 2012[15].

Ley 1341 de 2009. Por la cual se definen "Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC", se crea la Agencia Nacional del Espectro, entre otras[16].

ISO/IEC 27001:2013: Es la norma principal de la serie ISO 27K y contiene los requisitos del Sistema de Gestión de Seguridad de la Información.[17].

---

[12] COLOMBIA, MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Decreto 1151 de 2008. Consultado el 10 de Junio de 2018 en: https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf

[13] COLOMBIA, SECRETARIA DEL SENADO. Ley 1273 de 2009. Consultado el 10 de Junio de 2018 en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

[14] COLOMBIA, MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Ley 1581 de 2012. Consultado el 10 de Junio de 2018 en: https://www.mintic.gov.co/portal/604/w3-article-4274.html.

[15] COLOMBIA, MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Decreto 1377 de 2013. Consultado el 10 de Junio de 2018 en: https://www.mintic.gov.co/portal/604/w3-article-4274.html.

[16] COLOMBIA, MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Ley 1341 de 2009. Consultado el 10 de Junio de 2018 en: https://www.mintic.gov.co/portal/604/w3-article-3707.html.

[17] NORMAS ISO. ISO/IEC 27001:013. Consultado e 10 de Junio de 2018 en: http://www.normas-iso.com/iso-27001/

ISO/IEC 27002:2013: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a Seguridad de la Información[18].

MAGERIT. Es una metodología que responde a lo que se denomina Proceso de Gestión de los Riesgos de los sistemas de información[19].

[18] EL PORTAL DE ISO 27002 EN ESPAÑOL. ISO/IEC 27002:2013. Consultado el 10 de Junio de 2018 en: http://www.iso27000.es/iso27002.html

[19] ESPAÑA, PAE. Portal de Administración Electrónica. MAGERIT v.3 2012. Consultado el 10 de Junio de 2018 en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W8y1YHtKjIU

8. PRODUCTO RESULTADO A ENTREGAR

Realizada la correspondiente evaluación de los activos de la IPS Solidarios, la identificación de vulnerabilidades, la valoración de las amenazas, la determinación del impacto y los riegos a que está expuesta la institución, como parte fundamental del análisis de riesgos que conlleva la metodología Magerit, se pretende establecer, el plan de tratamiento de riesgos, la identificación de los controles según la ISO 27001, el nivel de madurez en que se encuentra el sistema de información de la entidad y la generación de políticas de seguridad y procedimientos para su implementación para materializar las decisiones adoptadas para el tratamiento de los riesgos.

9. RECURSOS NECESARIOS PARA EL DESARROLLO

Para logró y desarrollo de las actividades del presente proyecto, se debe disponer de recursos necesarios que permitan apoyar y alcanzar las etapas que se han planificado. Los recursos que se necesitan en éste proyecto son los humanos, tecnológicos, materiales y financieros.

9.1 RECURSOS HUMANOS

Gerente IPS, Socios, Estudiante Investigador, Tutores del proyecto.

9.2 RECURSOS TECNOLÓGICOS

Hardware: Computadora Portátil, dispositivos de almacenamiento USB, Celular.
Software: Procesador de texto, Hoja de Cálculo, Internet.

9.3 RECURSOS MATERIALES

Papelería General, Fotocopias, Medios opticos de almacenamiento.

9.4 RECURSOS FINANCIEROS O PRESUPUESTO

La IPS Solidarios Salud proporcionará toda la información necesaria para llevar a feliz término el presente proyecto.

No obstante, se hace necesario trasladarse al municipio de Cuaspud Carlosama Nariño para practicar las entrevistas propuestas, revisar los archivos, verificar las instalaciones, identificar la red informática, determinar el software que utilizan los equipos informáticos, la operación de los procesos, realizar el registro fotográfico y tomar fotocopias.

Finalmente se incluirán los costos generados para la producción de los textos que se requieran. Lo anterior se puede apreciar en la siguiente tabla.

Tabla 3 Presupuesto para el desarrollo del proyecto

Ítem	VALOR		FINANCIACIÓN			
	Valor Unitario	**Cantidad**	**Universidad**	**Empresa**	**Estudiante**	**Total**
Textos			X			0
Fotocopias	50	2.000			X	10.000
Internet					X	100.000
Pasajes	30.000	10			X	300.000
Digitación					X	100.000
Impresión	300	1.000			X	300.000
Empastes /Argollados	10.000	5			X	50.000
Otros					X	500.000
						1.360.000

Fuente: El Autor

10. CRONOGRAMA DE ACTIVIDADES

Tabla 4 Descripción de Actividades

Actividad	Mes 1				Mes 2				Mes 3				Mes 4			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Planificación y Elaboración del Proyecto																
Aprobación del Proyecto																
Recolección de datos																
Organización y Procesamiento de la información																
Redacción del proyecto																
Presentación de la proyecto																
Sustentación del proyecto																
Aprobación Final del proyecto																

Fuente: El Autor

11. DESARROLLO DEL PROYECTO

11.1 ACTIVIDADES PRELIMINARES

a. Visita y reconocimiento de la empresa

Entidad: IPS Solidarios Salud Ltda.

Ubicación: Municipio de Cuaspud Carlosama. Barrió Fundadores. Cra. 2 No. 1-09.

Actividad Económica: Institución Prestadora de Servicios de Salud de Segundo Nivel de Atención.

Descripción de la Entidad: Es una Institución Prestadora de Servicios de Salud de Segundo Nivel. Presta servicios de atención para la rehabilitación funcional en las áreas de terapias como: Terapia Física, Terapia Ocupacional, Terapia del Lenguaje y Psicología, a través de terapeutas ocupacionales, fisioterapeutas, fonoaudiólogos y psicólogos.

11.2 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS

Como ya se describió en el marco teórico, Magerit es la metodología idónea para desarrollar el análisis y gestión de riesgos a los sistemas de información de la IPS Solidarios; permitiendo determinar dentro de este proceso de evaluación, los activos, su valoración, las amenazas, las vulnerabilidades, controles, impacto y el riesgo que puedan ser objeto los activos. Además, con la identificación de los riesgos se define un plan para su tratamiento, que asociados y en relación con la

ISO 27001 e ISO 27002, se establecen unas políticas y procedimientos para su control.

Teniendo en cuenta la metodología Magerit, el análisis de riesgos se lo puede representar como una secuencia organizada de pasos para determinar el riesgo, en el presente estudio de procedió a realizar lo siguiente:

1. Identificación de los activos relevantes de la entidad, su dependencia y valoración de acuerdo a sus características.
2. Identificación de amenazas que pueden estar expuestos los activos previamente reconocidos.
3. Identificación de vulnerabilidades que pueden ser utilizadas para causar daño alguno sobre los activos.
4. Análisis de Riesgos

11.3 APLICACIÓN DE LA METODOLOGÍA MAGERIT

Teniendo en cuenta los pasos descritos en la metodología Magerit para la identificación y gestión de riesgos sobre los activos de la IPS Solidarios, se presenta en su orden las siguientes actividades:

11.4 IDENTIFICACION DE ACTIVOS

Identificar los activos permite determinar y conocer su valor dentro de la organización, realizar la valoración e identificar las amenazas a las que están expuestos.

[D] Datos / Información. Permiten a la Entidad prestar sus servicios. La información se almacenará o transmitida en dispositivos o equipos según su fin.

Ficheros
Datos de Configuración. Servidor principal
Datos de control de Acceso

[K] Claves criptográficas. Permite proteger la integridad de la información y la confidencialidad de los usuarios que necesiten autenticarse dentro del medio o red informática.

Claves de firma digital

[S] Servicios. Es el servicio prestado a los usuarios, mediante los sistemas informáticos y de información.

Existen servicios como:
- Internet
- Correo electrónico.
- Impresión
-Transferencia de ficheros.

[SW] Software – Aplicaciones Informáticas. Son los programas desarrollados por terceros o software tercerizados.

Se relacionan

- Sistema de Contabilidad – World Office
- Sistema de Facturación, Estadística y Generación de Informes
- Sistemas Operativo - Windows
- Access
- Ofimática
- Antivirus

[HW] Equipamiento Informático (Hardware).

Son los dispositivos físicos computacionales que permiten gestionar los servicios que presta la organización

Dentro de los equipos informáticos que posee la organización tenemos:

-
- Computadoras Portátiles.
- Computadoras de Escritorio.
- Router
- Switch
- Impresora multifuncional

[COM] Redes de Comunicaciones. Son los diferentes medios de comunicación para la transmisión de información entre las diferentes unidades de negocio de la institución o también servicios de comunicación contratados a terceros.

Entre los medios de transporte, tenemos los siguientes:

- Red Local –LAN
- Internet

[MEDIA] Soportes de información. Permiten almacenar la información de manera permanente o en por tiempos estipulados. Puede ser dispositivos institucionales o tercerizados.

Generalmente se utilizan los siguientes soportes de información:

- Respaldo en la Nube.
- Dispositivos USB.
- Material Impreso
- Historias Clínicas

- Discos formatos DVD
- Discos formatos CD

[AUX] Equipamiento Auxiliar. Ayudan al soporte de los sistemas de información.

- Fuentes de alimentación
- Cableado de datos.
- UPS (Sistemas de Poder Ininterrumpido)

[L] Instalaciones. La infraestructura donde se localiza los sistemas de información y comunicaciones, es la IPS Solidarios Salud, ubicado en el Barrio “Los Fundadores” Carrera 2ª No. 1 – 09.

[P] Personal. Dentro del personal con que cuenta la IPS Solidarios para el soporte de sistemas y Soporte Tecnológico se relaciona a:

Tabla 5 Personal Sistemas

CARGO	PERFIL
Administrador de Sistemas	Ingeniero de Sistemas

Fuente: El Autor.

11.5 LISTA IDENTIFICACIÓN DE ACTIVOS

Se presenta listado Resumen de la clasificación de activos según la Metodología Magerit.

Tabla 6 Lista de identificación de activos

TIPO	COD	DESCRIPCION
[D] Datos / Información	[files]	Ficheros
	[conf_sv]	Datos de Configuración. Servidor

TIPO	COD	DESCRIPCION
	[acl]	Datos de control de Acceso
[K] Claves criptográficas.	[public_signature]	Claves de firma digital
[S] Servicios	[Internet]	Internet
	[email]	Correo electrónico
[SW] Software – Aplicaciones Informáticas.	[sub_Fact]	Sistema de Facturación y Estadística
	[sub_Con]	Sistema de Contabilidad
	[os]	Sistema Operativos Windows
	[dbms_access]	Bases de Datos Access
	[office]	Ofimática
	[av]	Antivirus
	[firewall]	Firewall
	[browser]	Navegador Web
[HW] Equipamiento Informático (Hardware).	[mid]	Equipo Host -(Aplicaciones)
	[mobile]	Computadores Portátiles
	[router]	Router
	[switch]	Switch
	[printer]	Impresora Multifuncional
[COM] Redes de Comunicaciones	[lan]	Red Local –LAN
	[Internet]	Internet
[MEDIA] Soportes de información	[san_cld]	Servicio Respaldo (Drive)
	[usb]	Dispositivos USB.
	[printed]	Historias Clínicas
[AUX] Equipamiento Auxiliar	[power]	Fuentes de alimentación
	[cabling]	Cableado de datos.

TIPO	COD	DESCRIPCION
	[ups]	UPS (Sistemas de Poder Ininterrumpido)
[L] Instalaciones	[Edificio Principal]	Edificio Principal
[P] Personal	[op]	Ingeniero en Sistemas

Fuente: IPS Solidarios - Metodología Magerit -Activos

11.6 DEPENDENCIA DE ACTIVOS

Se establece la dependencia entre los activos, determinando la medida en que un activo superior impacta a otro activo inferior tras la materialización de una amenaza. Se puede decir que de arriba hacia abajo se generan las dependencias entre los activos, mientras que de abajo hacia arriba da origen a la propagación del daño o perjuicio al materializarse la amenaza, esto puede observar en la siguiente tabla.

Tabla 7 Dependencia de Activo

TIPO	COD	DESCRIPCION	[files]	[conf_sv]	[acl]	[public_signature]	[Internet]	[email]	[sub_Fact]	[sub_Con]	[os]	[dbms_access]	[office]	[av]	[firewall]	[browser]	[mid]	[mobile]	[router]	[switch]	[lan]	[Internet]	[san_cld]	[usb]	[printed]	[power]	[cabling]	[ups]	[Edificio Principal]	[op]
[D] Datos / Información	[files]	Ficheros		X	X																									X
	[conf_sv]	Datos de Configuración. Servidor			X				X	X	X			X				X	X	X	X									X
	[acl]	Datos de control de Acceso					X	X	X	X	X	X	X					X	X	X	X									X
[K] Claves criptográficas.	[public_signature]	Claves de firma digital					X	X																						X
[S] Servicios	[Internet]	Internet						X			X			X	X	X	X	X					X							X
	[email]	Correo electrónico											X			X	X	X			X		X	X	X					X
[SW] Software – Aplicaciones Informáticas.	[sub_Fact]	Sistema de Facturación y Estadística									X			X	X		X	X	X	X	X									X
	[sub_Con]	Sistema de Contabilidad									X			X	X		X	X	X	X	X									X
	[os]	Sistema Operativos Windows												X	X		X	X												X
	[dbms_access]	Bases de Datos Access															X	X												X
	[office]	Ofimática									X	X					X	X												X
	[av]	Antivirus					X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X						X
	[firewall]	Firewall					X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X						X
	[browser]	Navegador Web					X	X									X	X					X							X
[HW] Equipamiento Informático (Hardware).	[mid]	Equipo Host -(Aplicaciones)							X	X							X													X
	[mobile]	Computadores Portátiles																												X
	[router]	Router							X	X							X					X	X							X
	[switch]	Swith							X	X							X					X	X							X
[COM] Redes de Comunicaciones	[lan]	Red Local –LAN																											X	X
	[Internet]	Internet																											X	X
[MEDIA] Soportes de información	[san_cld]	Servicio Respaldo (Drive)																											X	X
	[usb]	Dispositivos USB.							X	X																				X
	[printed]	Historias Clínicas							X	X							X	X											X	X
[AUX] Equipamiento Auxiliar	[power]	Fuentes de alimentación															X	X											X	X
	[cabling]	Cableado de datos.							X	X							X												X	X
	[ups]	UPS (Sistemas de Poder Ininterrumpido)							X	X							X												X	X
[L] Instalaciones	[Edificio Principal]	Edificio Principal																												
[P] Personal	[op]	Técnico en Sistemas																												

Fuente: El Autor

11.7 VALORACIÓN DE ACTIVOS

Se determina en que dimensión es valioso el activo y el valor que tiene para la organización en que caso de sufrir destrucción. La dimensión es una propiedad o característica que da valor a un activo, es de gran utilidad por permitir la valoración de los efectos de la materialización de una amenaza.

Las dimensiones básicas evaluadas son la Confidencialidad, la Integridad y la Disponibilidad, representando mayor importancia en el proceso de valoración de activos y se incluyen la Integridad y Trazabilidad, como medida de valoración especifica de algunos activos del sistema, entre ellos, los servicios de directorio, las claves de firma digital, registros de actividad, entre otros.

Disponibilidad: Por disponible entendemos aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos, lo que refiere a los métodos de precaución contra posibles daños.

Integridad: Hace referencia a la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

Confidencialidad: La información puede ser accedida únicamente por las personas o sistemas que tienen autorización para hacerlo. Se articula con la protección de la información para que no sea interceptada y leída por terceros.

Autenticidad: Hace referencia a una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Permite valorar el grado de perjuicio causado, si una entidad no autorizada hace uso de los servicios de la organización.

Trazabilidad: Permite identificar en cualquier momento quien y cuando utilizó un servicio.

Como resultado de su valoración se obtiene el informe Modelo de valor.

Para designar las dimensiones utilizadas en la valoración de los activos, amenazas e impacto se utilizará la siguiente tabla.

Tabla 8 Dimensiones

Dimensiones	Identificador
Disponibilidad	D
Integridad	I
Confidencialidad	C
Autenticidad	A
Trazabilidad	T

Fuente: Adaptación Libro II Magerit V.3.0

VALORACION CUALITATIVA

Permite identificar un activo y darle un valor a sus dimensiones de acuerdo a su importancia dentro de la entidad. Para éste proyecto la escala de valores que se manejará es la siguiente:

Tabla 9 Escala cualitativa de valoración

Valor	Abreviatura	Criterio
Muy Alto	MA	Daño muy grave
Alto	A	Daño grave
Medio	M	Daño importante
Bajo	B	Daño menor
Muy Bajo	MB	Daño depreciable

Fuente: Adaptación -Libro II Magerit V.3.0 Catalogo de Elementos

El valor asignado al activo a través de sus dimensiones describirá la magnitud de la valoración y el daño o afectación que podría alcanzar.

PROCESO DE VALORACIÓN DE LOS ACTIVOS

La evaluación del activo se realizó teniendo en cuenta la tabla 4 lista de identificación de activos, la tabla 6 dimensiones y la tabla 7 Escala cualitativa de valoración de la siguiente manera:

Tabla 10 Proceso de valoración de activos

ACTIVOS	**DIMENSIONES**				
	D	**I**	**C**	**A**	**T**
ACTIVO 1	Valoración	Valoración	Valoración	Valoración	Valoración
ACTIVO 2	Valoración	Valoración	Valoración	Valoración	Valoración
…	…	…	…	…	…
ACTIVO N	Valoración	Valoración	Valoración	Valoración	Valoración

Fuente: El Autor.

Al realizar la valoración de todos los activos según las dimensiones se logrará observar su importancia dentro de la entidad.

El resultado obtenido de realizar la valoración de activos de la IPS Solidarios, se puede apreciar en la siguiente tabla:

Tabla 11 Valoración cualitativa de activos según dimensiones

TIPO	ORDEN	CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	PROCESO PROPIETARIO DEL ACTIVO	RESPONSABLE	DIMENSIONES				
						DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD
[D] Datos / Información	1	[files]	Ficheros	Sistemas	Ingeniero de Sistemas	MA	MA	MA	M	M
	2	[conf_sv]	Datos de Configuración. Servidor	Sistemas	Ingeniero de Sistemas	MA	M	A	B	B
	3	[acl]	Datos de control de Acceso	Sistemas	Ingeniero de Sistemas	MA	M	A	M	B
[K] Claves criptográficas	4	[public_signature]	Claves de firma digital	Sistemas	Ingeniero de Sistemas	MA	MA	MA	A	M
[S] Servicios	5	[Internet]	Internet	Sistemas	Ingeniero de Sistemas	A	B	M	MB	MB
	6	[email]	Correo electrónico	Sistemas	Ingeniero de Sistemas	M	M	A	B	A
[SW] Software – Aplicaciones Informáticas	7	[sub_Fact]	Sistema de Facturación y Estadística	Sistemas	Ingeniero de Sistemas	MA	MA	MA	MA	MA
	8	[sub_Con]	Sistema de Contabilidad	Sistemas	Ingeniero de Sistemas	MA	MA	MA	MA	MA
	9	[os]	Sistema Operativos Windows	Sistemas	Ingeniero de Sistemas	MA	MA	MA	A	M
	10	[dbms_access]	Bases de Datos Access	Sistemas	Ingeniero de Sistemas	A	M	M	MB	MB
	11	[office]	Ofimática	Sistemas	Ingeniero de Sistemas	MB	MB	MB	MB	MB
	12	[av]	Antivirus	Sistemas	Ingeniero de Sistemas	M	B	B	B	B
	13	[firewall]	Firewall	Sistemas	Ingeniero de Sistemas	A	M	M	B	B
	14	[browser]	Navegador Web	Sistemas	Ingeniero de Sistemas	A	M	M	B	B
[HW] Equipamiento Informático (Hardware)	15	[mid]	Equipo Host - (Aplicaciones)	Sistemas	Ingeniero de Sistemas	M	M	M	B	B
	16	[mobile]	Computadores Portátiles	Sistemas	Ingeniero de Sistemas	A	MB	M	MB	MB

TIPO	ORDEN	CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	PROCESO PROPIETARIO DEL ACTIVO	RESPONSABLE	DIMENSIONES				
						DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD
	17	[router]	Router	Sistemas	Ingeniero de Sistemas	MA	MA	MA	A	B
	18	[switch]	Switch	Sistemas	Ingeniero de Sistemas	A	B	B	B	B
	19	[printer]	Impresora Multifuncional	Sistemas	Ingeniero de Sistemas	B	B	B	B	B
[COM] Redes de Comunicaciones	20	[lan]	Red Local –LAN	Sistemas	Ingeniero de Sistemas	MA	MA	MA	A	M
	21	[Internet]	Internet	Sistemas	Ingeniero de Sistemas	MA	MA	MA	A	B
[MEDIA] Soportes de información	22	[san_cld]	Servicio Respaldo (Drive)	Sistemas	Ingeniero de Sistemas	MA	MA	MA	A	A
	23	[usb]	Dispositivos USB.	Sistemas	Ingeniero de Sistemas	MA	MA	MA	A	B
	24	[printed]	Historias Clínicas	Sistemas	Ingeniero de Sistemas	MA	MA	MA	MA	A
[AUX] Equipamiento Auxiliar	25	[power]	Fuentes de alimentación	Sistemas	Ingeniero de Sistemas	MA	A	MA	B	B
	26	[cabling]	Cableado de datos.	Sistemas	Ingeniero de Sistemas	MA	MA	MA	B	M
	27	[ups]	UPS (Sistemas de Poder Ininterrumpido)	Sistemas	Ingeniero de Sistemas	MA	MA	M	MB	MB
[L] Instalaciones	28	[Edificio Principal]	Edificio Principal	Sistemas	Ingeniero de Sistemas	MA	M	MA	M	M
[P] Personal	29	[op]	Ingeniero en Sistemas	Sistemas	Ingeniero de Sistemas	MA	MA	MA	A	M

Fuente: El Autor

Como se observa en la anterior tabla, la evaluación realizada a los activos de la IPS Solidarios teniendo en cuenta los criterios de la tabla 8 se puede determinar lo siguiente:

Que los activos:

El sistema de Facturación y Estadística
El sistema de contabilidad
El servicio de respaldo (Backup)
Historias Clínicas

Presentan una valoración Muy Alta (MA) y Alta (A) respectivamente en sus dimensiones, representando dentro de la entidad un alto nivel de importancia por ser activos que permiten a diario desarrollar y apoyar las actividades operativas y misionales de la organización, y son el pilar y su razón de ser.

Y los activos:

Ofimática (Hojas de Cálculo, Procesadores Texto, Presentador de Ideas)
Computadores Portátiles
Impresora Multifuncional

Presentan una valoración Muy Baja (MB) y B (Baja) respectivamente en sus dimensiones, representando en la entidad un bajo nivel de importancia. En consecuencia, si llegará a perderse o sufrir daño alguno, se podría reemplazar el activo y/o restaurar la información mediante las copias de seguridad que realiza la entidad, sin afectar las actividades operativas y misionales de la entidad.

Los activos restantes, presentan la valoración de sus activos como se observa en la tabla 9, y por representar diferentes magnitudes de valoración en sus

dimensiones, debe prestársele considerable atención a fin de evitar daño o pérdida de los mismos.

VALORACION CUANTITATIVA

Para realizar esta valoración de los activos, se tiene en cuenta la evaluación cualitativa, guardando relación entre su magnitud y el valor numérico que para ésta clase de medición se establezca en cada una de las dimensiones evaluadas. Se tiene en cuenta la siguiente tabla:

Tabla 12 Escala cuantitativa de valoración

Abreviación	Calificación Activo	Probabilidad	% ocurrencia
MA	Critico	10	100
A	Importante	9	80
M	Apreciable	8	60
B	Bajo	5	40
MB	Despreciable	2	20

Fuente: Adaptación -Libro II Magerit V.3.0 Catalogo de Elementos

Proceso de valoración cuantitativa

Para realizar esta valoración de los activos, se tiene en cuenta la tabla 8, donde se evalúa su dimensión, según la importancia que represente para la entidad. Se asigna el valor correspondiente teniendo en cuenta los criterios definidos en la citada tabla.

El resultado de evaluación de los activos se representa en la siguiente tabla.

Tabla 13 Valoración cuantitativa de activos según dimensiones

TIPO	CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	DIMENSION					VALOR PROMEDIO	CALIFICACION DEL ACTIVO
			D	I	C	A	T		
[D] Datos / Información	[files]	Ficheros	10	10	10	8	8	9	IMPORTANTE
	[conf_sv]	Datos de Configuración. Servidor	10	8	9	5	5	7	APRECIABLE
	[acl]	Datos de control de Acceso	10	8	9	8	5	8	APRECIABLE
[K] Claves criptográficas	[public_signature]	Claves de firma digital	10	10	10	9	8	9	IMPORTANTE
[S] Servicios	[Internet]	Internet	9	5	8	2	2	5	BAJO
	[email]	Correo electrónico	8	8	9	5	9	8	APRECIABLE
[SW] Software – Aplicaciones Informáticas	[sub_Fact]	Sistema de Facturación y Estadística	10	10	10	10	10	10	CRITICO
	[sub_Con]	Sistema de Contabilidad	10	10	10	10	10	10	CRITICO
	[os]	Sistema Operativos Windows	10	10	10	9	8	9	IMPORTANTE
	[dbms_access]	Bases de Datos Access	9	8	8	2	2	6	APRECIABLE
	[office]	Ofimática	2	2	2	2	2	2	DESPRECIABLE
	[av]	Antivirus	8	5	5	5	5	6	APRECIABLE
	[firewall]	Firewall	9	8	8	5	5	7	APRECIABLE
	[browser]	Navegador Web	9	8	8	5	5	7	APRECIABLE
[HW] Equipamiento Informático (Hardware)	[mid]	Equipo Host - (Aplicaciones)	8	8	8	5	5	7	APRECIABLE
	[mobile]	Computadores Portátiles	9	2	8	2	2	5	BAJO
	[router]	Router	10	10	10	9	5	9	IMPORTANTE
	[switch]	Switch	9	5	5	5	5	6	APRECIABLE
	[printer]	Impresora Multifuncional	5	5	5	5	5	5	BAJO

TIPO	CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	DIMENSION					VALOR PROMEDIO	CALIFICACION DEL ACTIVO
			D	I	C	A	T		
[COM] Redes de Comunicaciones	[lan]	Red Local –LAN	10	10	10	9	8	9	IMPORTANTE
	[Internet]	Internet	10	10	10	9	5	9	IMPORTANTE
[MEDIA] Soportes de información	[san_cld]	Servicio Respaldo (Drive)	10	10	10	9	9	10	CRITICO
	[usb]	Dispositivos USB.	10	10	10	9	5	9	IMPORTANTE
	[printed]	Historias Clínicas	10	10	10	10	9	10	CRITICO
[AUX] Equipamiento Auxiliar	[power]	Fuentes de alimentación	10	9	10	5	5	8	APRECIABLE
	[cabling]	Cableado de datos.	10	10	10	5	8	9	IMPORTANTE
	[ups]	UPS (Sistemas de Poder Ininterrumpido)	10	10	8	2	2	6	APRECIABLE
[L] Instalaciones	[Edificio Principal]	Edificio Principal	10	8	10	8	8	9	IMPORTANTE
[P] Personal	[op]	Ingeniero en Sistemas	10	10	10	9	8	9	IMPORTANTE

Fuente: El Autor

Como se observa en la anterior tabla, la evaluación realizada a los activos de la IPS Solidarios teniendo en cuenta los criterios de la tabla 8, se puede determinar lo siguiente:

Que los activos:

El sistema de Facturación y Estadística
El sistema de contabilidad
El servicio de respaldo (Backup)
Historias Clínicas

Presentan un valor promedio de 10 en sus respectivas dimensiones, calificando el activo como crítico respectivamente en sus dimensiones, representando para la entidad mayor importancia para la entidad por contribuir a desarrollar y apoyar las actividades operativas y misionales de la organización.

Y el activo:

Ofimática (Hojas de Cálculo, Procesadores Texto, Presentador de Ideas).

Presenta un valor promedio de 2 en las dimensiones evaluadas, calificando el activo como despreciable, representando en la entidad un bajo nivel de importancia. En consecuencia, si llegará a perderse o sufrir daño alguno, se podría reemplazar el activo sin afectar las actividades operativas y misionales de la entidad.

Los activos restantes, presentan la calificación de los activos como se observa en la tabla 11, y por representar diferentes promedios de valoración en sus dimensiones, debe prestársele considerable atención a fin de evitar daño o pérdida de los mismos.

11.8 PRUEBAS PRACTICADAS

Para determinar que posibles vulnerabilidades pueden afectar los activos de la IPS Solidarios, se realizaron pruebas de observación, fotográficas, pruebas con herramientas de software y documental. Sin embargo, por directriz del gerente general de la IPS Solidarios, solo autoriza que se presente los hallazgos o posibles vulnerabilidades como evidencia del proyecto, y la demás información, solo sea de conocimiento de quien los representa.

En observancia, a la directriz emanada por el gerente de la IPS solidarios, se presenta las siguientes pruebas realizada a los activos:

Archivos: Se evidencia posibles errores en la manipulación de los archivos, que pueden conllevar a una alteración incidental de la información o presentarse fugas de información por parte de los trabajadores.

Perfiles de Usuario. Cuando un trabajador termina su contrato laboral, no se notifica oportunamente a secretaria general para que realice el bloqueo y restricción de usuario, quedando activo ese perfil y con oportunidad de acceso.

Copias de seguridad: Falta de verificación periódica del procedimiento de restauración de Backups para determinar su estado, confiabilidad y calidad.

Contraseñas: Las contraseñas son utilizadas para hacer el login de inicio de sesión hacia el host central. Para los usuarios operativos de la institución la asignación de contraseñas no mantiene una estructura lógica de identificación y son fácil de identificar, al tener un número limitado de caracteres menor a ocho (8), además esta nunca se cambia.

Manejo de Dispositivos USB: Dentro de las acciones de prevención y protección de la información, se formaliza el cuidado que se debe tener con los medios de almacenamiento externo o usb (Pendrive); sin embargo el control al personal que labora en la empresa es mínimo.

Protección de Backups Realizados: Falta de existencia de una caja fuerte para la custodia y salvaguardar las backups realizados.

Capacitación: Escasa formación en temas de seguridad de la información, dirigida al personal y la falta de concientización sobre el buen uso de los recursos informáticos, en especial a lo referente a Ingeniería Social.

Recuperación: No existen planes y políticas que permitan socializar al personal, para la recuperación de desastres que se puedan presentar en la organización.

Servicios de Respaldo (Nube). No se evidencia un procedimiento claro sobre la utilización de servicios gratuitos de respaldo en la nube como lo es Google drive.

Servicios WEB -Internet: No hay servicios de internet redundante en el caso de presentar inconvenientes con el proveedor principal.

Instalación de Software (usuarios). Falta de control en la instalación de aplicaciones de software no autorizadas por parte de los funcionarios de la institución sin supervisión alguna.

Protecciones generales: Escaso conocimiento por los funcionarios de la organización sobre el uso de extintores contra incendio.

Mantenimiento: Los mantenimientos y cambios del equipamiento en general están sujetos a los procesos contractuales y estos a su vez a la disponibilidad presupuestal, por lo cual se hacen un poco lentos.

Análisis de pruebas clasificado por activos

Activos Datos - Información

1. **Error cometidos por usuarios de la institución**: A pesar de recibir capacitación técnica sobre la manera de configurar los diferentes equipos computacionales para el acceso y almacenamiento de información, el ingreso y procesamiento de los datos

por parte del usuario final no posee un control para determinar la calidad esperada, que posiblemente afecten la disponibilidad de la información y su integridad.

2. **El administrador** – Como el nivel superior del control de la información, acceso y su almacenamiento, al no administrar de manera adecuada los diferentes aplicativos y sistemas de gestión de datos de la institución, puede incurrir en frecuentes errores e inconsistencias por su inoportuna gestión, que también podría incidir en la disponibilidad e integridad de la información. No ha existido una auditoria para su control como medida preventiva.

Datos Criptográficos

3. Los firmas digitales con que cuenta la organización para el proceso de firmado y envió de información a las Entidades de Control y las empresas que requieran, es dispuesta al usuario final responsable del envió de la información, que posiblemente al no haber una custodia centralizada de la firma criptográfica estas se pueda extraviar y ser usada en procesos indebidos, afectando su disponibilidad.

Servicios

4. La caída del sistema por agotamiento de recursos puede ocasionar la parada del sistema por la falta de monitorización de los recursos utilizados por los usuarios de la empresa. Lo anterior puede ser el resultado de los bajos controles a los usuarios finales en la utilización de aplicaciones sin autorización y que no ayudan a la operatividad misional como (Facebook, Videos, streaming, audios) congestionan el ancho de banda de la red.

5. En complemento a la indebida utilización e instalación de aplicaciones sin autorización por los usuarios internos de la organización, puede exponerse a un

ataque de denegación del servicio, siendo su principal medio de difusión el mismo personal de la institución, pero también a externos. No hay un control más exhaustivo y generándose una vulnerabilidad muy evidente.

Aplicaciones

6. En esta categoría sigue presentándose los errores no intencionados del administrador como un riesgo alto, que puede obedecer a la falta de computadoras alternos que sirvan de pruebas para la configuración e instalación de nuevas aplicaciones que se utilizaran. Pueden afectar su disponibilidad e integridad.

7. Los programas dañinos y su difusión pueden ser el riesgo más frecuente que se presenta en la institución, esto teniendo en cuenta la falta de control en las instalaciones de aplicaciones no autorizadas, los correos no deseados y la utilización de pendrives, siendo una vulnerabilidad latente en la organización y que afectan su disponibilidad e integridad por el daño que causan a los archivos del usuario y del sistema.

8. El acceso no autorizado y el abuso de privilegios pueden afectar directamente la integridad de los datos, de esta manera se evidencia la falta de aplicación de políticas de seguridad de información en cuanto a los controles de identificación y autenticación de usuarios con las suficiente medidas de prevención y protección.

Red de comunicaciones

9. A pesar de contar con firewalls para la protección contra intrusos, además del bloqueo de aplicaciones indebidas para evitar el uso, no ha existido el control suficiente para contrarrestarlo y la concientización sobre seguridad a los trabajadores.

Soportes de información

10. Para la protección contra el fuego existen extintor como medida para contrarrestarla, sin embargo no existe una debida capacitación al personal sobre su uso. Y para lo correspondiente a desastres naturales es un riesgo inesperado y latente, y que la entidad no ha formalizado un plan de emergencias, pero que aun así al presentarse su mitigación es relativa.

Equipamiento auxiliar e instalaciones

11. Los riesgos por causa del fuego o incendio afectaran en gran medida la información, además no se encuentra implementado sensores de humo.

12. Los desastres naturales como ya se mencionó pueden causar un daño mayor en la organización y en sus activos.

Personal

13. La única persona que conocen el proceso de recuperación y puesta en marcha de los equipos de respaldo son el técnico de sistemas y soporte, caso de no estar disponible o ausente, se podría generar una interrupción temporal de los servicios. También tiene relevancia el riesgo por desconocimiento y falta de capacitación al personal sobre temas de ingeniería social, que son los ataques informáticos más frecuentes por la vulnerabilidad psicológica y social de las personas.

11.9 IDENTIFICACION DE AMENAZAS

Las amenazas son problemas que pueden afectar los activos de la organización. Obtienen provecho de las vulnerabilidades existentes en el sistema de información y lograr de esta manera afectar o causar daño a los activos.

Se Identifican las amenazas teniendo en cuenta la metodología Magerit (Libro II), para cada tipo de activo.

Clasificación de las amenazas

• De origen natural.
• Del entorno.
• Causadas por las personas de forma accidental.
• Causadas por las personas de forma deliberada.

Las amenazas se valoran en cada dimensión de la seguridad del activo como lo es: La Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad. La valoración se la realiza de mayor a menor relevancia, de esta manera si a una dimensión la califican con el valor 3 significa que esa amenaza afectaría y tendrá más relevancia en dicha dimensión para el activo evaluado, la valoración 2 significa que la amenaza la afectaría de manera moderada, y la valoración 1 refiere a una afectación del activo de manera baja en la dimensión valorada.

Tabla 14 Identificación de Amenazas

CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	COD	AMENAZAS	DIMENSIONES				
				D	I	C	A	T
[files]	Ficheros	**[E.1]**	Errores de los usuarios	1	3	2		
		[E.15]	Alteración accidental de la información		3			
		[E.19]	Fugas de información			3		
[conf_sv]	Datos de Configuración Servidor	**[E.2]**	Errores del administrador	3	2	1		
		[E.15]	Alteración accidental de la información		3			
		[E.19]	Fugas de información			3		
[acl]		**[A.5]**	Suplantación de la identidad del usuario		1	3	2	

CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	COD	AMENAZAS	DIMENSIONES				
				D	I	C	A	T
	Datos de control de Acceso	**[A.15]**	Modificación deliberada de la información		3			
		[A.18]	Destrucción de información	3				
[public_signature]	Claves de firma digital	**[E.1]**	Errores de los usuarios	1	3	2		
		[E.19]	Fugas de información			3		
[Internet]	Internet	**[E.24]**	Caída del sistema por agotamiento de recursos	3				
[email]	Correo electrónico	**[A.5]**	Suplantación de la identidad del usuario		1	3	2	
		[A.6]	Abuso de privilegios de acceso	1	2	3		
		[A.11]	Acceso no autorizado		2	3		
		[A.18]	Destrucción de información	3				
		[E.19]	Fugas de información			3		
[sub_Fact]	Sistema de Facturación y Estadística	**[E.1]**	Errores de los usuarios.	1	3	2		
		[E.2]	Errores del administrador	3	2	1		
		[E.8]	Difusión de software dañino	3	2	1		
		[E.15]	Alteración accidental de la información		3			
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3			
		[A.6]	Abuso de privilegios de acceso	1	2	3		
		[A.11]	Acceso no autorizado		2	3		
		[A.18]	Destrucción de información	3				
		[A.19]	Divulgación de información			3		
[sub_Con]		**[E.1]**	Errores de los usuarios.	1	3	2		

CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	COD	AMENAZAS	DIMENSIONES				
				D	I	C	A	T
	Sistema de Contabilidad	**[E.2]**	Errores del administrador	3	2	1		
		[E.8]	Difusión de software dañino	3	2	1		
		[E.15]	Alteración accidental de la información		3			
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3			
		[A.6]	Abuso de privilegios de acceso	1	2	3		
		[A.11]	Acceso no autorizado		2	3		
		[A.18]	Destrucción de información	3				
		[A.19]	Divulgación de información			3		
[os]	Sistema Operativos Windows	**[E.2]**	Errores del administrador	3	2	1		
		[E.4]	Errores de configuración		3			
		[E.15]	Alteración accidental de la información		3			
		[E.18]	Destrucción de información	3				
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3			
		[A.6]	Abuso de privilegios de acceso	1	2	3		
		[A.11]	Acceso no autorizado		2	3		
		[A.18]	Destrucción de información	3				
		[A.19]	Divulgación de información			3		

CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	COD	AMENAZAS	DIMENSIONES				
				D	I	C	A	T
		[A.22]	Manipulación de Programas	1	2	3		
[dbms_access]	Bases de Datos Access	**[E.1]**	Errores de los usuarios.	1	3	2		
		[E.2]	Errores del administrador	3	2	1		
		[E.15]	Alteración accidental de la información		3			
		[E.18]	Destrucción de información	3				
		[A.11]	Acceso no autorizado		2	3		
		[A.18]	Destrucción de información	3				
		[A.19]	Divulgación de información			3		
[office]	Ofimática	**[E.1]**	Errores de los usuarios.	1	3	2		
[av]	Antivirus	**[E.2]**	Errores del administrador	3	2	1		
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3			
[firewall]	Firewall	**[E.2]**	Errores del administrador	3	2	1		
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3			
[browser]	Navegador Web	**[E.8]**	Difusión de software dañino	3	2	1		
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3			
		[A.22]	Manipulación de Programas	1	2	3		
[mid]	Equipo Host - (Aplicaciones)	**[I.3]**	Contaminación mecánica	3				
		[I.5]	Avería de origen físico o lógico	3				

CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	COD	AMENAZAS	DIMENSIONES				
				D	I	C	A	T
		[I.6]	Corte del suministro eléctrico	3				
		[E.23]	Errores de mantenimiento / actualización de Equipos (hardware)	3				
		[A.25]	Robo	3		2		
[mobile]	Computadores Portátiles	**[I.3]**	Contaminación mecánica	3				
		[I.5]	Avería de origen físico o lógico	3				
		[I.6]	Corte del suministro eléctrico	3				
		[E.23]	Errores de mantenimiento / actualización de Equipos (hardware)	3				
		[A.25]	Robo	3		2		
[router]	Router	**[A.11]**	Acceso no autorizado		2	3		
		[A.25]	Robo	3		2		
		[E.2]	Errores del administrador	3	2	1		
		[E.4]	Errores de configuración		3			
		[I.5]	Avería de origen físico o lógico	3				
		[I.6]	Corte del suministro eléctrico	3				
[switch]	Switch	**[A.25]**	Robo	3		2		
		[I.6]	Corte del suministro eléctrico	3				
[printer]	Impresora Multifuncional	**[I.3]**	Contaminación mecánica	3				
		[I.5]	Avería de origen físico o lógico	3				
		[E.23]	Errores de mantenimiento / actualización de Equipos (hardware)	3				

CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	COD	AMENAZAS	DIMENSIONES				
				D	I	C	A	T
		[A.25]	Robo	3		2		
[lan]	Red Local – LAN	**[I.8]**	Fallo de servicios de comunicaciones	3				
		[E.2]	Errores del administrador	3	2	1		
		[E.24]	Caída del sistema por agotamiento de recursos	3				
		[A.7]	Uso no previsto	3	1	2		
		[A.11]	Acceso no autorizado		2	3		
		[A.24]	Denegación de servicio	3				
[Internet]	Internet	**[I.8]**	Fallo de servicios de comunicaciones	3				
		[E.24]	Caída del sistema por agotamiento de recursos	3				
		[A.7]	Uso no previsto	3	1	2		
		[A.11]	Acceso no autorizado		2	3		
		[A.24]	Denegación de servicio	3				
[san_cld]	Servicio Respaldo (Drive)	**[E.1]**	Errores de los usuarios	1	3	2		
		[E.2]	Errores del administrador	3	2	1		
		[A.18]	Destrucción de información	3				
		[A.24]	Denegación de servicio	3				
[usb]	Dispositivos USB.	**[A.15]**	Modificación deliberada de la información		3			
		[I.5]	Avería de origen físico o lógico	3				
		[A.25]	Robo	3		2		
[printed]	Historias Clínicas	**[I.1]**	Fuego	3				
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3				
		[I.10]	Degradación de los soportes de	3				

CODIGO	NOMBRE DEL ACTIVO DE INFORMACION	COD	AMENAZAS	DIMENSIONES				
				D	I	C	A	T
			almacenamiento de la información					
		[N.7]	Desastres naturales	3				
[power]	Fuentes de alimentación	**[I.6]**	Corte del suministro eléctrico	3				
[cabling]	Cableado de datos.	**[I.1]**	Fuego	3				
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3				
[ups]	UPS (Sistemas de Poder Ininterrumpido)	**[I.1]**	Fuego	3				
		[N.7]	Desastres naturales	3				
[Edificio Principal]	Edificio Principal	**[I.1]**	Fuego	3				
		[N.7]	Desastres naturales	3				
		[I.*]	Desastres Industriales	3				
[op]	Ingeniero en Sistemas	**[E.28]**	Indisponibilidad del personal	3				
		[A.30]	Ingeniería Social (Picaresca)	1	2	3		

Fuente: El Autor – Libro II Magerit

11.10 IDENTIFICACION DE VULVERABILIDADES

Se considera como vulnerabilidad la debilidad que posee un bien y que puede ser aprovechada por una amenaza para materializarse o bien causar daño alguno.

Se realiza la clasificación de la amenaza como se describe a continuación:

N: Desastres naturales.

I: De origen Industrial.

E: Errores y fallos no intencionados.

A: Ataques Intencionados.

Con base en las pruebas realizadas en los Activos de la IPS Solidarios, se encontró posibles vulnerabilidades, que de no controlarse pueden ser aprovechadas por las amenazas, materializando el riesgo o daño para los activos.

En la tabla siguiente, se presenta como ejemplo las posibles vulnerabilidades en el activo [SW] Software – Aplicaciones Informáticas: Sistema de Facturación e Informática.

Tabla 15 Identificación de Vulnerabilidades

NOMBRE DEL ACTIVO DE INFORMACION	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES
Sistema de Facturación y Estadística	E	**[E.1]**	Errores de los usuarios.	Bajo conocimiento del Sistema de Facturación y estadística por el personal operativo
		[E.2]	Errores del administrador	Configuración inadecuada del Sistema de Facturación por el personal administrador
		[E.8]	Difusión de software dañino	Utilización de sistemas de protección de prueba o libres (freeware o shareware)

NOMBRE DEL ACTIVO DE INFORMACION	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES
		[E.15]	Alteración accidental de la información	Manipulación errada de información por parte del personal de la institución
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Actualizaciones o mantenimiento no efectivo y eficaz por parte del proveedor del software
	A	**[A.6]**	Abuso de privilegios de acceso	conocimiento e Ingreso al sistema como superusuario, por cualquier trabajador del sistema de la institución
		[A.11]	Acceso no autorizado	No existe mecanismos de autenticación e identificación adecuados
		[A.18]	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo
		[A.19]	Divulgación de información	Personal con bajo compromiso institucional y falta de ética en el manejo de la información reservada

Fuente: El Autor

Para los demás activos, se identificaron las vulnerabilidades, según la clasificación de las amenazas y teniendo en cuenta la estructura presentada en el anterior ejemplo. Lo anunciado se puede evidenciar el Anexo 1.

11.12. ANALISIS DE RIESGOS

Se realizará un diagnóstico para establecer la magnitud de los riesgos informáticos existentes en los sistemas de información de la IPS Solidarios de Cuaspud, estableciendo su probabilidad de ocurrencia y el impacto generado.

ESTIMACIÓN DEL IMPACTO

Al realizar la estimación del impacto, se pretende determinar el daño del activo originado por la materialización de las amenazas sobre los activos de información de la IPS Solidarios.

A partir de los datos obtenidos en las fases anteriores, se procede a estimar el impacto. El primer dato requerido es el "Valor del activo" valorado cuantitativa y/o cualitativamente, con base en las tablas de doble entrada que se presentan. Ver tabla 14 Estimación del impacto cuantitativo y tabla 15 Estimación del impacto cualitativo. Además se establecerá el impacto de las amenazas sobre cada activo, con la conversión de las tablas mencionadas como se presenta en la tabla 12.

El segundo dato para la valoración del impacto es la Degradación[20]: Valor en porcentaje que indica en cuanto puede perjudicarse una activo si se materializa la amenaza. Esta degradación se valorará según las tablas 14 y 15.

Tabla 16 Estimación del impacto cuantitativo

Impacto		**Degradación**		
		1	10	100
Valor del activo	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Libro Magerit v 3.0 - Adaptación

[20] ESPAÑA. PAE. Portal de Administración Electrónica. Metodología Magerit Libro II. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W8zH83tKjIU

Tabla 17 Estimación del impacto cualitativo

Impacto		Degradación		
		1	10	100
Valor del activo	MA	3	4	5
	A	2	3	4
	M	1	2	3
	B	1	1	2
	MB	1	1	1

Fuente: Libro Magerit v 3.0 - Adaptación

De las anteriores tablas, la estimación del impacto cualitativo y cuantitativo podemos realizar su conversión para poder establecer su nivel de valoración.

Tabla 18 Conversión del Impacto – Valoración Cuantitativo vs Cualitativo

Impacto	Valor Cuantitativo	Valor Cualitativo	Descripción
Crítico	5	MA	Impacta fuertemente en la operatividad de los procesos.
Importante	4	A	Impacta en la operatividad de los procesos.
Apreciable	3	M	Impacta en la operatividad del macro proceso.
Bajo	2	B	Impacta en la operatividad del proceso
Despreciable	1	MB	Impacta levemente en la operatividad del proceso.

Fuente: Libro 3 Magerit v 3.0 – Adaptación

Teniendo en cuenta el resultado que se presenta en la tabla 11. Valoración cuantitativa de los activos según sus dimensiones, se evalúa los posibles efectos que podrían presentarse al materializarse una amenaza y la posible degradación del activo. Según lo anunciado, se presenta el impacto del resultado del análisis al activo [SW] Software – Aplicaciones Informáticas: Sistema de Facturación e Informática y se muestra en la tabla siguiente:

Tabla 19 Estimación del Impacto

NOMBRE ACTIVO	COD	AMENAZAS	VULNERABILIDAD	VALOR ACTIVO	DEGRAD.	IMPACTO	
Sistema de Facturación y Estadística	**[E.1]**	Errores de los usuarios.	Bajo conocimiento del Sistema de Facturación y estadística por el personal operativo	MA	1	3	M
	[E.2]	Errores del administrador	Configuración inadecuada del Sistema de Facturación por el personal administrador	MA	10	4	A
	[E.8]	Difusión de software dañino	Utilización de sistemas de protección de prueba o libres (freeware o shareware)	MA	100	5	MA
	[E.15]	Alteración accidental de la información	Manipulación errada de información por parte del personal de la institución	MA	10	4	A
	[E.21]	Errores de mantenimiento / actualización de programas (software)	Actualizaciones o mantenimiento no efectivo y eficaz por parte del proveedor del software	MA	10	4	A
	[A.6]	Abuso de privilegios de acceso	conocimiento e Ingreso al sistema como superusuario, por cualquier trabajador del sistema de la institución	MA	100	5	MA
	[A.11]	Acceso no autorizado	No existe mecanismos de autenticación e identificación adecuados	MA	100	5	MA
	[A.18]	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo	MA	100	5	MA
	[A.19]	Divulgación de información	Personal con bajo compromiso institucional y falta de ética en el manejo de la información reservada	MA	10	4	A

Fuente: El Autor

Para el análisis del impacto de los activos restantes, teniendo en cuenta su valoración y degradación, se puede observar en el Anexo 1 Valoración del riesgo sobre los activos IPS Solidarios.

- **ESTIMACIÓN DE LA PROBABILIDAD**

La estimación de la probabilidad busca determinar la posible frecuencia donde una amenaza puede materializarse con base en el número de veces de su ocurrencia. Es decir, la relación entre las vulnerabilidades y la amenaza es directamente proporcional, a mayor número de vulnerabilidades que pueda presentar un activo, mayor probabilidad de ocurrencia de la amenaza. Para determinar la frecuencia de materialización de las amenazas se utilizó la siguiente escala:

Tabla 20 Frecuencia materialización de amenazas

1	Raro	**MB**	Puede ocurrir una vez cada 2 años.
2	Muy baja	**B**	Al año.
3	Baja	**M**	En 6 meses.
4	Media	**A**	Al mes.
5	Alta	**MA**	A la semana.

Fuente: Libro Magerit v 3.0 - Adaptación

En la siguiente tabla se visualiza el impacto y la frecuencia de materialización de cada una de las amenazas sobre el activo [SW] Software – Aplicaciones Informáticas: Sistema de Facturación e Informática Servidor.

Tabla 21 Determinación de la Frecuencia

NOMBRE ACTIVO	CLASIF. AMENAZA	COD	AMENAZAS	VULNERABILIDAD	FRECUENCIA	
Sistema de Facturación y Estadística	E	**[E.1]**	Errores de los usuarios.	Bajo conocimiento del Sistema de Facturación y estadística por el personal operativo	2	B
		[E.2]	Errores del administrador	Configuración inadecuada del Sistema de Facturación por el personal administrador	3	M
		[E.8]	Difusión de software dañino	Utilización de sistemas de protección de prueba o libres (freeware o shareware)	3	M
		[E.15]	Alteración accidental de la información	Manipulación errada de información por parte del personal de la institución	1	MB
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Actualizaciones o mantenimiento no efectivo y eficaz por parte del proveedor del software	3	M
	A	**[A.6]**	Abuso de privilegios de acceso	conocimiento e Ingreso al sistema como superusuario, por cualquier trabajador del sistema de la institución	4	A
		[A.11]	Acceso no autorizado	No existe mecanismos de autenticación e identificación adecuados	4	A
		[A.18]	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo	3	M
		[A.19]	Divulgación de información	Personal con bajo compromiso institucional y falta de ética en el manejo de la información reservada	3	M

Fuente: El Autor

Para el análisis del impacto y la frecuencia de materialización de cada una de las amenazas sobre los activos restantes, se puede observar el Anexo 1 Valoración del riesgo sobre los activos IPS Solidarios.

- **ESTIMACIÓN DEL RIESGO**

Una vez determinado el impacto sobre los activos mediante su valoración y degradación, y además estimada la probabilidad con base en la frecuencia de materialización de las amenazas respecto al tiempo, se procede a realizar la estimación del riesgo, establecido por la relación entre el impacto vs la probabilidad de ocurrencia sobre los activos valorados.

Tabla 22 Estimación del riesgo

Riesgo		**Probabilidad**				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	MA	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Libro3 Magerit v 3.0 - Adaptación

Se presenta la estimación del riesgo como resultado de la aplicación de la tabla 20 Estimación del riesgo al activo [SW] Software – Aplicaciones Informáticas: Sistema de Facturación e Informática y se evidencia a continuación:

Tabla 23 Ejemplo Estimación del Riesgo

NOMBRE DEL ACTIVO	COD	AMENAZAS	VULNERABILIDAD	FX.		IMPACTO		RIESGO
Sistema de Facturación y Estadística	**[E.1]**	Errores de los usuarios.	Bajo conocimiento del Sistema de Facturación y estadística por el personal operativo	B	1	3	M	B
	[E.2]	Errores del administrador	Configuración inadecuada del Sistema de Facturación por el personal administrador	M	10	4	A	A
	[E.8]	Difusión de software dañino	Utilización de sistemas de protección de prueba o libres (freeware o shareware)	M	100	5	MA	A
	[E.15]	Alteración accidental de la información	Manipulación errada de información por parte del personal de la institución	MB	10	4	A	B
	[E.21]	Errores de mantenimiento / actualización de programas (software)	Actualizaciones o mantenimiento no efectivo y eficaz por parte del proveedor del software	M	10	4	A	A
	[A.6]	Abuso de privilegios de acceso	conocimiento e Ingreso al sistema como superusuario, por cualquier trabajador del sistema de la institución	A	100	5	MA	MA
	[A.11]	Acceso no autorizado	No existe mecanismos de autenticación e identificación adecuados	A	100	5	MA	MA
	[A.18]	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo	M	100	5	MA	A

NOMBRE DEL ACTIVO	COD	AMENAZAS	VULNERABILIDAD	FX.		IMPACTO		RIESGO
	[A.19]	Divulgación de información	Personal con bajo compromiso institucional y falta de ética en el manejo de la información reservada	M	10	4	A	A

Fuente: El Autor

Como se observa en la tabla anterior se determinó los riesgos para el activo [SW] Software – Aplicaciones Informáticas: Sistema de Facturación e Informática, presentando 7 riesgos que lo exponen al peligro de ser afectado. Estos posibles riesgos se identifican con color naranja (5 riesgos) y color rojo (2 riesgos), que por el resultado de su valoración deben ser tratados de manera inmediata y monitoreo permanente. En el presente estudio se realizará el tratamiento a los activos que presentan mayor dificultad o que se encuentra en como riesgos Altos (A - color naranja) y Muy Altos (MA - color rojo), lo demás riesgos que están por fuera de esta valoración se pueden resolver y tratar a su tiempo dentro del proceso de gestión de la entidad.

Para la estimación del riesgo sobre los activos restantes, se puede observar el Anexo 1 Valoración del riesgo sobre los activos IPS Solidarios.

- **EVALUCIÓN DE RIESGOS**

Una vez terminado la evaluación anterior se pueden evidenciar los riesgos a los que están expuestos los activos de la organización. La alta dirección determinará el plan de seguridad a seguir considerando los siguientes aspectos: - cumplimiento de obligaciones, determinación de costos de implementación del plan de tratamiento

de riesgos, beneficios derivados de mejorar las actividad que incluye riesgos como: factores técnicos, económicos, culturales, políticos, ambiental etc.

En cuanto a los riesgos donde el nivel es depreciable y bajo se finaliza el proceso, y se pueden resolver y tratar a su tiempo dentro de la gestión de la entidad, para los riesgos determinados como apreciable, importante y crítico es necesario evaluar el tratamiento del riesgo para precisar si se transfiere, evita o mitiga por medio de los controles.

El tipo del tratamiento que se le puede dar a los riesgos es el siguiente:

Tabla 24 Evaluación de riesgos

NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
Despreciable	Finaliza el proceso.
Bajo	Finaliza el proceso.
Apreciable	Una de las tres opciones: a. Se transfiere el riesgo por ejemplo tomando un seguro. b. Se evita el riesgo retirando el activo de información. c. Se reduce o mitiga el riesgo por medio de controles.
Importante	
Critico	

Fuente: Libro3 Magerit v 3.0 - Adaptación

Una vez terminado la evaluación anterior se pueden evidenciar los riesgos a los que está expuesta la organización. La alta dirección determinará el plan de seguridad a seguir considerando los siguientes aspectos: - cumplimiento de obligaciones - Beneficios derivados de una actividad que incluye riesgos, factores técnicos, económicos, culturales, políticos, etc.

- **PLAN DE TRATAMIENTO DE RIESGOS**

Con el resultado obtenido en la estimación de riesgos sobre los activos, es necesario establecer el **Plan de Tratamiento de Riesgos** (**PTR**), el cual permite establecer las bases de seguridad para la entidad. Para este proceso se tienen en cuenta los riesgos que representan inmediata atención y monitoreo, representados por su valoración alta y muy alta.

Tabla 25 Plan de Tratamiento de Riesgos

NOMBRE ACTIVO	COD	AMENAZAS	VULNERABILIDADES	RIESGO	PTR
Ficheros	**[E.19]**	Fugas de información	Carencia de políticas en el manejo de la información por parte del personal operativo.	A	Generar Políticas de reserva y confidencialidad de información dirigidas al personal.
Claves de firma digital	**[E.19]**	Fugas de información	Carencia de medidas de control y de protección sobre los dispositivos criptográficos.	A	Generar Políticas de control, protección y custodia de los dispositivos electrónicos (Token).
Sistema de Facturación y Estadística	**[E.2]**	Errores del administrador	Configuración inadecuada del Sistema de Facturación por el personal administrador.	A	Capacitar al Coordinador y/o administrador del Sistema de Facturación sobre el uso y configuración.
	[E.8]	Difusión de software dañino	Utilización de sistemas de protección de prueba o básicos (freeware o shareware).	A	Disponer de Herramientas de monitoreo y protección, que permitan establecer reglas de detección y control de manera eficaz.
	[E.21]	Errores de mantenimiento / actualización de programas (software)	Actualizaciones o mantenimiento no efectivo y eficaz por parte del proveedor del software.	A	Disponer de Copia de seguridad del Sistema de Facturación y/o Contable.
	[A.6]	Abuso de privilegios de acceso	Conocimiento e Ingreso al sistema como superusuario, por cualquier	MA	Establecer roles y perfiles de ingreso al sistema, según el cargo asignado.

NOMBRE ACTIVO	COD	AMENAZAS	VULNERABILIDADES	RIESGO	PTR
			trabajador del sistema de la institución.		
	[A.11]	Acceso no autorizado	No existen mecanismos de autenticación e identificación adecuados.	MA	Establecer roles y perfiles de ingreso al sistema, según el cargo asignado. Establecer políticas de confidencialidad de la información.
	[A.18]	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo.	A	Generar políticas sobre la gestión y uso de contraseñas.
	[A.19]	Divulgación de información	Personal con bajo compromiso institucional y falta de ética en el manejo de la información reservada.	A	Generar Acuerdos Contractuales de confidencialidad de la información al personal de la entidad.
Sistema de Contabilidad	**[E.2]**	Errores del administrador	Configuración inadecuada del Aplicativo de Contabilidad por el personal administrador.	A	Capacitar al Coordinador y/o administrador del Aplicativo de Contabilidad sobre el uso y configuración.
	[E.8]	Difusión de software dañino	Utilización de sistemas de protección de prueba o libres (freneare o shareware).	A	Disponer de Herramientas de monitoreo y protección, que permitan establecer reglas de detección y control de manera eficaz.
	[E.21]	Errores de mantenimiento / actualización de programas (software)	Actualizaciones o mantenimiento no efectivo y eficaz por parte del proveedor del software.	A	Disponer de Copia de seguridad del Aplicativo de Contabilidad.
	[A.6]	Abuso de privilegios de acceso	Conocimiento e Ingreso al sistema como superusuario, por cualquier trabajador del sistema de la institución.	MA	Establecer roles y perfiles de ingreso al sistema, según el cargo asignado.

NOMBRE ACTIVO	COD	AMENAZAS	VULNERABILIDADES	RIESGO	PTR
	[A.11]	Acceso no autorizado	No existen mecanismos de autenticación e identificación adecuados.	MA	Establecer roles y perfiles de ingreso al sistema, según el cargo asignado. Establecer políticas de confidencialidad de la información.
	[A.18]	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo.	A	Generar políticas sobre la gestión y uso de contraseñas.
	[A.19]	Divulgación de información	Personal con bajo compromiso institucional y falta de ética en el manejo de la información reservada.	A	Generar Acuerdos Contractuales de confidencialidad de la información al personal de la entidad.
Sistemas Operativos Windows	**[A.6]**	Abuso de privilegios de acceso	Falta de creación de privilegios y perfiles para los usuarios, todos pueden ser Super usuarios.	MA	Creación de Privilegios y perfiles de seguridad, que permitan identificar de manera exclusiva al personal teniendo en cuenta el cargo desempeñado.
	[A.11]	Acceso no autorizado	No existe control para el acceso e identificación a los usuarios. Se verifican puertos abiertos que sirven de puertas traseras para ingresar al sistema.	MA	Creación de Privilegios y perfiles de seguridad, que permitan identificar de manera exclusiva al personal teniendo en cuenta el cargo desempeñado.
Bases de Datos	**[A.11]**	Acceso no autorizado	No existe mecanismos de restricción al acceso a las bases de datos	A	Creación de Privilegios y perfiles de seguridad, que permitan identificar de manera exclusiva al personal teniendo en cuenta el cargo desempeñado
Router	**[A.11]**	Acceso no autorizado	No existen mecanismos de restricción a los dispositivos de comunicación o rejillas de protección.	MA	Implementar Controles de acceso a personal no autorizado, a fin de evitar su manipulación y robo.

NOMBRE ACTIVO	COD	AMENAZAS	VULNERABILIDADES	RIESGO	PTR
	[I.6]	Corte del suministro eléctrico	No se identifica fuentes de alimentación regulada y alterna.	A	Disponer de una UPS de Mayor Potencia (Vatios), en caso de presentarse una falta del servicio de energía eléctrica.
Red Local - LAN	**[A.11]**	Acceso no autorizado	No existe control de ingreso a los equipos informáticos para personal externo.	MA	Implementar Controles de acceso a personal no autorizado, a fin de evitar su manipulación y robo.
Internet	**[A.11]**	Acceso no autorizado	No existe control de ingreso a los equipos informáticos para personal externo.	A	Implementar Controles de acceso a personal no autorizado, a fin de evitar su manipulación.
Servicio Respaldo (Drive)	**[E.2]**	Errores del administrador	Falta de conocimiento de los procesos de administración y configuración de los procedimientos de respaldo de la información por el personal administrador.	A	Capacitar al personal que administra los servicios de respaldo de información.
Historias Clínicas	**[I.7]**	Condiciones inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.	A	Disponer de Dispositivos de medición y control de temperatura
	[I.10]	Degradación de los soportes de almacenamiento de la información	No existe un manejo técnico y adecuado del archivo de historias clínicas, en cuanto a almacenamiento, custodia y disposición final.	A	Políticas de conservación y preservación de los documentos.
Edificio Principal	**[I.*]**	Desastres Industriales	No se identifica fuentes de alimentación regulada y alterna. Posibles fluctuación eléctrica	A	Establecer políticas y normas de seguridad para la regulación de fuentes de suministro de energía.

Fuente: El Autor.

IDENTIFICACION DE CONTROLES ISO 27002

Para este proceso de identificación de controles, se toma como fundamento la norma ISO 27001, catalogada como principal de la serie de las ISO 27K y contiene los requisitos del sistema de gestión de seguridad la información y la gestión del riesgo de los sistemas de información. Además, esta norma, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2013, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI[21].

La ISO 27002:2013, reúne para su evaluación 14 Dominios, 35 Objetivos de Control y 114 Controles, que en aplicación a los sistemas de información de la IPS Solidarios se procedió a realizar una lista de chequeo con la información presentada en esta norma. Lo anterior permitió establecer el grado o nivel de madurez que se encuentran los sistemas de información de la IPS solidarios, y de esta manera establecer la declaración de aplicabilidad de los controles necesarios para la entidad.

La aplicación de los controles de la ISO 27002:2013, para la evaluación de los sistemas de información de la IPS Solidarios, consiste en interrogar y cuestionar, si cada control se aplica o no, estableciendo a final de la evaluación, el nivel de madurez del SGSI.

En la tabla 24, se muestra un ejemplo de la aplicación de la ISO 27002:2013, en la IPS Solidarios. Se evalúa el dominio 7, referente a la Seguridad ligada al recurso humano. Como se observa, existe un total de 6 controles, que al momento de la

[21] El PORTAL DE ISO 27001 EN ESPAÑOL. ISO/IEC 27001:2013. Disponible en: http://www.iso27000.es/iso27000.html

evaluación 4 respondieron afirmativamente (SI) y 2 de manera negativa (NO), generando como resultado un nivel de cumplimiento o madures del dominio del 67%, siendo la razón de dividir el total de preguntas afirmativas (SI) sobre el número de controles de ese dominio, multiplicado por 100.

Como se evidencia el cumplimiento para el dominio es del 67%, permitiendo inferir que la entidad debe mejorar los procesos establecidos durante la contratación, la responsabilidad que debe asumir cada trabajador y el buen manejo de la información y la concientización y capacitación en seguridad informática dirigida al personal de la entidad.

Tabla 26 Lista de chequeo evaluación controles de la seguridad ligada a los recursos humanos.

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)
	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.		**4**	**2**	**6**	**67**
Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.	**7.1 Antes de la contratación.**					
	7.1.1 Investigación de antecedentes.	¿La empresa verifica los antecedentes de los empleados nuevos?	X			
	7.1.2 Términos y condiciones de contratación.	¿La organización realiza contratos con los empleados determinando los términos y condiciones del trabajo?	X			
Asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.	**7.2 Durante la contratación.**					
	7.2.1 Responsabilidades de gestión.	¿La organización verifica el cumplimiento de políticas de seguridad para con sus empleados?		X		
	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	¿La organización capacita, entrena y actualiza a sus empleados?		X		
	7.2.3 Proceso disciplinario.	¿La organización abre proceso disciplinario en caso que un empleado	X			

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)
		incumpla los términos o condiciones?				
Proteger los intereses de la organización durante el proceso de cambio o finalización de empleo por parte de empleados y contratistas.	**7.3 Cese o cambio de puesto de trabajo.**					
	7.3.1 Cese o cambio de puesto de trabajo.	¿La empresa tiene un proceso para cesar las actividades de un empleado o contrato?	X			

Fuente: El Autor

El proceso descrito anteriormente, se aplicó de igual manera a los demás dominios que se muestran en el Anexo 2 Lista de Chequeo, Controles y Dominios ISO 27002:2013.

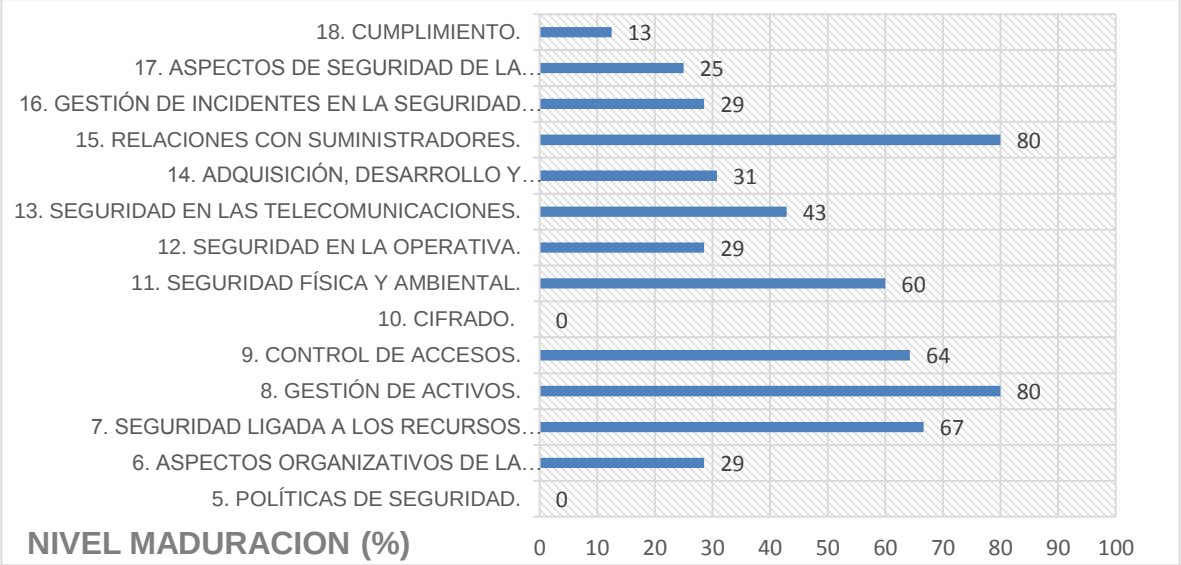
Se representa mediante una tabla y gráficamente, la evaluación de los sistemas de información de la IPS Solidarios mediante los controles de la ISO 27002:2013.

Tabla 27 Nivel de madures de los dominios IPS Solidarios

NIVEL DE MADUREZ DE LOS DOMINIOS	
DOMINIO	NIVEL MADURACION
5. POLÍTICAS DE SEGURIDAD.	0
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	29
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	67
8. GESTIÓN DE ACTIVOS.	80
9. CONTROL DE ACCESOS.	64
10. CIFRADO.	0
11. SEGURIDAD FÍSICA Y AMBIENTAL.	60
12. SEGURIDAD EN LA OPERATIVA.	29
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	43
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	31
15. RELACIONES CON SUMINISTRADORES.	80
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	29
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	25
18. CUMPLIMIENTO.	13

Fuente: El autor

Figura 5 Gráfico de Nivel de Madures Dominios IPS Solidarios



Fuente: El Autor

- **MATRIZ DE APLICABILIDAD**

Esta matriz es el resultado de evaluar los controles de la ISO 27002 en la IPS Solidarios, en relación al proceso de evaluación de los activos y la determinación de los riesgos que fueron asociados al realizar su estimación. Se debe formalizar si el control es aplicable a la entidad, se está aplicando o la razón del porque no debe aplicarse. Para este proceso se evaluó la lista de chequeo de controles de la citada norma. Además de debe tener en cuenta las razones para la selección del control al momento de la evaluación según la información siguiente:

Razones para la selección

L: Requerimiento Regulatorio

C: Obligación contractual

N: Requerimiento del negocio/Adopción de buenas prácticas

R: Análisis de riesgos

Tabla 28 Matriz de aplicabilidad Dominio 7 Seguridad ligada a los recursos humanos

Objetivo de Control	Dominio	Pregunta Existencia Control	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
				L	C	N	R
	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.						
Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.	**7.1 Antes de la contratación.**						
	7.1.1 Investigación de antecedentes.	¿La empresa verifica los antecedentes de los empleados nuevos?	La entidad verifica los antecedentes de los trabajadores que ingresan por primera vez.		X	X	
	7.1.2 Términos y condiciones de contratación.	¿La organización realiza contratos con los empleados determinando los términos y condiciones del trabajo?	La entidad formaliza los términos y condiciones laborales en las minutas contractuales entre cada trabajador y la entidad.		X	X	

Fuente: El Autor

La matriz de aplicabilidad para todos los dominios de la ISO 27002 evaluando los sistemas de información de la IPS Solidarios se presenta en el Anexo 2 Lista de Chequeo, Controles y Dominios ISO 27002:2013.

11.13 POLITICAS DE SEGURIDAD

Realizada la evaluación de los activos y también la estimación de los riesgos, se elaboró el plan de tratamiento de riesgos (PTR), además se evaluó los controles de la ISO 27002 que pueden ser aplicados en la IPS Solidarios a fin de mitigar los riesgos. De esta manera se formalizaron una serie de políticas en relación al plan de tratamiento de riesgos vs los controles establecidos para la entidad, como se presentan a continuación:

PTR	Generar Políticas de reserva y confidencialidad de información dirigidas al personal.
DOMINIO	5 Políticas de Seguridad
CONTROL	5.1.1 Conjunto de políticas para la seguridad de la información.
POLITICA	Definir un conjunto de políticas para la seguridad y confidencialidad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes.
PROCEDIMIENTO	• Todos los datos de propiedad de la empresa se deben clasificar dentro de las categorías que determine la organización. • La responsabilidad para definir la clasificación de la información debe ser tanto del dueño de la información, como del área de Sistemas. • Toda Información que sea clasificada como sensible (secreta, confidencial o privada) debe tener un respaldo, además debe tener copias recientes completas en un sitio externo a la empresa. • Todos los trabajadores deben estar obligados a garantizar la reserva de la información de cualquier tipo. • Formalizar acuerdos de confidencialidad, en donde se establezcan penalidades por las infracciones cometidas. • Toda divulgación de Información secreta, confidencial o privada requerida por terceras personas debe estar acompañada por un contrato donde se describa explícitamente qué información es restringida y cómo puede o no ser usada.
COSTO	Ninguno. Es el valor agregado que resulta de la planeación estratégica que realice la alta dirección en conjunto con el área de sistemas.

PTR	Generar Políticas de control, protección y custodia de los dispositivos.
DOMINIO	10. Cifrado.
CONTROL	10.1.1 Política de uso de los controles criptográficos.
POLITICA	Definir un conjunto de políticas de control, protección y custodia de los dispositivos criptográficos.
PROCEDIMIENTO	• Designar un administrador de la responsabilidad y custodia del dispositivo. • Asignar la administración responsable de las claves del dispositivo. • En caso de pérdida del dispositivo, establecer el procedimiento de su reemplazo y recuperación de claves. • Realizar las actualizaciones periódicas en atención a la seguridad requerida y nuevas técnicas para la mejora del cifrado. • Evaluar los controles aplicados.
COSTO	Ninguno. El establecimiento de la gestión responsable de uso y protección de los dispositivos criptográficos.

PTR	Capacitar al Coordinador y/o administrador del Sistema de Facturación y/o Contable sobre el uso y configuración.
DOMINIO	7. Seguridad ligada a los recursos humanos.
CONTROL	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
POLITICA	Establecer plan de capacitación al personal sobre las tecnologías utilizadas en la entidad y seguridad informática.
PROCEDIMIENTO	• Definir las tecnologías que ameriten mejorar el conocimiento en su administración y configuración. • Definir las temáticas que necesiten fortalecer su comprensión y sean de mayor relevancia en seguridad informática para la entidad. • Establecer la frecuencia de capacitaciones. • Evaluar la eficacia de las acciones de mejora propuestas.
COSTO	El costo depende de la necesidad, interés e importancia de las temáticas.

PTR	Disponer de Herramientas de monitoreo y protección, que permitan establecer reglas de detección y control de manera eficaz.
DOMINIO	12 Seguridad Operativa.
CONTROL	12.2.1 Controles contra el código malicioso.
POLITICA	Disponer y mantener actualizado los sistemas de prevención y detección de software malicioso, evaluando la eficacia y efectividad ofrecida.
PROCEDIMIENTO	• Buscar herramientas de prevención y detección que permitan mejorar los controles de seguridad. • Adquirir la herramienta que brinde mejore solución en seguridad y protección de la información. • Evaluar la eficacia de la solución informática adquirida.
COSTO	Entre $ 250.000 y $ 500.000 por un año. Numero de dispositivos protegidos de 3 a 5.

PTR	Disponer de Copia de seguridad del Sistema de Facturación y/o Contable.
DOMINIO	12 Seguridad Operativa
CONTROL	12.3.1 Copias de seguridad de la información.
POLITICA	Realizar diariamente copias de seguridad de las bases de datos de los aplicativos misionales de la entidad.
PROCEDIMIENTO	• Identificar el equipo host o servidor donde se encuentran las bases de datos de los aplicativos misionales. • Realizar la copia de seguridad de las bases de datos de los aplicativos. • Etiquetar de manera descriptiva la copia realizada, especificando además la fecha y hora de su realización. • Guardar la copia generada en un equipo diferente al servidor. • Realizar prueba de restauración de la copia en un equipo diferente al servidor.
COSTO	Ninguno. Solo el beneficio de disponer respaldo de la información sensible de la entidad.

PTR	Establecer roles y perfiles de ingreso al sistema, según el cargo asignado.
DOMINIO	9 Control de Accesos
CONTROL	9.2.2 Gestión de los derechos de acceso asignados a usuarios.
POLITICA	Controlar y restringir el acceso no autorizado a los sistemas de información de la entidad, utilizando perfiles de acceso según las necesidades del negocio.
PROCEDIMIENTO	• Definir la categoría y el alcance de los perfiles de acceso, según la función o denominación del cargo del trabajador. • Realizar en los equipos informáticos la configuración de los perfiles definidos. • Administrar los perfiles. • Evaluar la eficacia de los perfiles definidos.
COSTO	Ninguno. Solo el beneficio de implementar perfiles para el acceso a los diferentes equipos informáticos.

PTR	Generar políticas sobre la gestión y uso de contraseñas.
DOMINIO	9 Control de Accesos
CONTROL	9.4.3 Gestión de contraseñas de usuario.
POLITICA	Gestionar de manera adecuada la creación y establecimiento de contraseñas seguras.
PROCEDIMIENTO	• La longitud mínima de la contraseña debe ser de 8 caracteres. • La contraseña debe estar conformada por números, letras (mayúsculas y minúsculas), caracteres especiales. • Que permita recordarse fácilmente y su escritura evite la menor observancia al teclado. • La contraseña se cambie con una cierta regularidad, como mínimo un mes. • Evaluar la efectividad de las contraseñas implantadas, con herramientas informáticas para este fin.
COSTO	Ninguno. Se logra implementar mejores medidas y buenas prácticas de seguridad para el acceso e identificación de los usuarios a los equipos informáticos.

PTR	Implementar controles de acceso a personal no autorizado, a fin de evitar su manipulación y/o robo.
DOMINIO	11 Seguridad física y ambiental.
CONTROL	11.2.1 Emplazamiento y protección de equipos.
POLITICA	Restringir el acceso a la sala de servidores y equipos a personal no autorizado y/o externo.
PROCEDIMIENTO	• Identificar mediante un carnet al personal de la entidad. • Instalar a la entrada de la sala de servidores y equipos cámaras de vigilancia. • Asegurar con cerraduras en acceso a la sala. • Realizar seguimiento a las novedades presentadas mediante los registros de las cámaras de vigilancia.
COSTO	$ 2.000.000.oo Cámaras de vigilancia y monitoreo.

PTR	Disponer de una UPS de Mayor Potencia (Vatios), en caso de presentarse una falta del servicio de energía eléctrica. Establecer políticas y normas de seguridad para la regulación de fuentes de suministro de energía.
DOMINIO	11 Seguridad física y ambiental.
CONTROL	11.2.2 Instalaciones de suministro.
POLITICA	Disponer de equipos eléctricos o electrónicos con capacidad suficiente, en caso de corte en el suministro de energía eléctrica.
PROCEDIMIENTO	• Identificar el número de equipos informáticos de la entidad. • Determinar la capacidad del sistema de alimentación ininterrumpida a utilizar, con base a los equipos disponibles y en uso. • Realizar las pruebas de la UPS, con los equipos disponibles y en Uso. • Determinar la efectividad del equipo. • Realizar la compra del equipo de apoyo UPS.
COSTO	$ 2.500.000 a $ 5.000.000, (UPS para unos 10 pc, tiempo de respaldo 20 minutos.).

PTR	Capacitar al personal que administra los servicios de respaldo de información.
DOMINIO	7. Seguridad ligada a los recursos humanos.
CONTROL	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
POLITICA	La administración debe proveer, mantener y dar entrenamiento sobre los sistemas de prevención, protección y respaldo necesarios para asegurar la continuidad del servicio.
PROCEDIMIENTO	• Establecer las temáticas relevantes a prevención, protección y métodos de respaldo de información. • Contratar experto en seguridad informática. • Convocar al personal designado. • Evaluar la eficacia de la aplicabilidad sobre los temas tratados.
Costo	$ 3.000.000. Dependiendo de las temáticas tratadas.

PTR	Disponer de Dispositivos de medición y control de temperatura. Políticas de conservación y preservación de los documentos.
DOMINIO	11. Seguridad física y ambiental.
CONTROL	11.1.4 Protección contra las amenazas externas y ambientales.
POLITICA	Mantener espacios físicos y ambientales adecuados para la protección de los activos y minimizar su degradación o deterioro.
PROCEDIMIENTO	• Identificar las áreas que puedan presentar un riesgo ambiental (Humedad, exceso temperatura). • Adquirir dispositivos de medición de temperatura ambiental para el control. • Instalar los dispositivos de control de temperatura en las áreas identificadas. • Mantener un registro diario de los resultados arrojados por los dispositivos de control de temperatura.

	• Establecer directrices que orienten la conservación de los documentos desde su producción hasta su disposición final, garantizando su integridad física y funcional, sin alterar su contenido • Evaluar la eficacia del control y sobre las mediciones registradas. • Establecer mejoras y adecuación de las áreas si es el caso.
Costo	$ 100.000.

PTR	Establecer políticas y normas de seguridad para la regulación de fuentes de suministro de energía.
DOMINIO	11. Seguridad física y ambiental.
CONTROL	11.1.4 Protección contra las amenazas externas y ambientales.
POLITICA	Adecuar el sistema de cableado eléctrico con base a la normatividad vigente en Colombia.
PROCEDIMIENTO	• Contratar personal idóneo para la verificación del sistema eléctrico. • Identificar las áreas que puedan presentar un riesgo en la fluctuación eléctrica. • Instalar el cableado eléctrico en las áreas identificas. • Instalar tomas que permitan identificar y determinar el tipo de energía suministrada (regulada y no regulada). • Evaluar la eficacia del control en base a las pruebas realizadas. • Establecer mejoras y adecuación de las áreas si es el caso.
Costo	$ 2.000.000.

CONCLUSIONES

La IPS Solidarios Salud no cuenta con un proceso metodológico para el análisis y tratamiento de riesgos en seguridad informática, siendo el presente proyecto aplicado un apoyo para la identificación de posibles riesgos y su gestión.

Con la identificación y el tratamiento que se den a los riesgos, fortalecerá la seguridad de la información de la IPS Solidarios.

La utilización de la metodología Magerit, contribuye a identificar de manera estructurada las dificultades existentes por la escasa seguridad informática de la entidad.

Se constató la ausencia de capacitaciones al personal de la IPS Solidarios en seguridad y protección de la información, siendo el recurso humano el medio más vulnerable en temas de seguridad.

El proceso desarrollado en las diferentes fases de identificación de riesgos ha despertado mayor interés en la gerencia de la IPS Solidarios por propender al mejoramiento de la seguridad de la información y la protección de los datos en esta entidad.

RECOMENDACIONES

Implementar una política institucional en seguridad de la información, a fin de definir, concientizar y formalizar criterios sobre la seguridad informática a todo el personal de la entidad.

Formalizar el análisis y gestión de los riesgos en temas de seguridad como un proceso aplicable en la IPS Solidarios a fin de mejorar la seguridad informática de la institución.

Capacitar al personal de la institución en temas relacionados con la prevención de amenazas y lo relacionado a seguridad de la información, promoviendo de esta manera la protección de los activos empresariales.

Notificar oportunamente los incidentes de seguridad de la información que se presenten en el desarrollo de las actividades diarias en la IPS Solidarios, para lograr corregir o mitigar el riesgo que pueda ocasionar.

Verificar frecuentemente los controles que se hayan formalizado como la detección y prevención de riesgos.

BIBLIOGRAFÍA

Ministerio de Hacienda y Administraciones públicas, MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, octubre 2012. {En línea}. {Consultado Marzo 2017}. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WNxY_G81_IU

AMAYA, Camilo. "MAGERIT: metodología práctica para gestionar riesgos". {En línea}. {Consultado Marzo 2017}. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

SGSI-Blog especializado en Sistemas de Gestión de Seguridad de la Información. "ISO 27001: El método MAGERIT". {En línea}. {Consultado Marzo 2017}. Disponible en: http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

EAR. EAR/PILAR-documentación Magerit. {En línea}. {Consultado Marzo 2017}. Disponible en: http://www.ar-tools.com/magerit/index.html

Dirección de Estándares y Arquitectura de TI del Ministerio de las Tecnologías de Información y las Comunicaciones de la República de Colombia. (2014). Generalidades del Marco de Referencia – versión 1.0. {En línea}. {Consultado Marzo 2017}. Disponible en: http://www.mintic.gov.co/marcodereferencia/624/articles-8102_generalidades.pdf

Ley 1273 de 2009. Delitos informáticos en Colombia. {En línea}. {Consultado Marzo 2017}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Ministerio de la Tecnologías de Información y Comunicación-Tic. Ley 1341 de 2009. Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-. {En línea}. {Consultado Marzo 2017}. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3707.html

Gobierno de España. Agencia Estatal Boletín Oficial del Estado. {Consultado Marzo 2017}. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-9741

BOCANEGRA, Yamilet. Análisis y Gestión de Riesgos de los Sistemas de Información de la Alcaldía Municipal de Tuluá aplicando la metodología MAGERIT. {En línea}. {Consultado Marzo 2017}. Disponible en: http://repository.unad.edu.co/handle/10596/3632.

IPS SOLIDARIOS SALUD. Portafolio de Servicios. {Consultado Marzo 2017}. 2008.

ANEXOS

Anexo A Formato de Encuesta

FORMATO ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador:

_____

Cargo:

_____

Fecha:

_____

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?
   SI ☐ NO ☐

2. ¿El computador donde labora cuenta con contraseñas de seguridad?
   SI ☐ NO ☐

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?
   SI ☐ NO ☐

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?
   WIFI ☐ CABLE ☐ OTRO ☐ _____

5. ¿Descarga archivos (programas, música, video.) de internet?
   SI ☐ NO ☐

6. ¿Realiza copias de respaldo de los datos e información que trabaja?
   SI ☐ NO ☐

7. ¿La entidad, ha realizado capacitación sobre temas relacionados a seguridad de información?

SI ☐ NO ☐

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

SI ☐ NO ☐

Fuente: El autor

Anexo B Aplicación del Formato de encuesta

FORMATO DE ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador: Paola Cristina Valencia

Cargo: Fonoaudiologa

Fecha: 30 Mayo 2018

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?

SI ☒ NO ☐

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

SI ☐ NO ☒

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

SI ☐ NO ☒

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

WIFI ☐ CABLE ☒ OTRO ☐ _____

5. ¿Descarga archivos (programas, música, video?) de internet?

SI ☒ NO ☐

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

SI ☐ NO ☒

7. ¿La entidad, ha realzado capacitación sobre temas relacionados a seguridad de información?

SI ☐ NO ☒

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

SI ☐ NO ☒

FORMATO DE ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador: Yeremia Mabel Paredes Cadena

Cargo: Secretaria

Fecha: Mayo - 30 - 2018

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?

   SI [X] NO [ ]

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

   SI [ ] NO [X]

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

   SI [ ] NO [X]

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

   WIFI [ ] CABLE [X] OTRO [ ] _____

5. ¿Descarga archivos (programas, música, video?) de internet?

   SI [ ] NO [X]

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

   SI [ ] NO [X]

7. ¿La entidad, ha realzado capacitación sobre temas relacionados a seguridad de información?

   SI [ ] NO [X]

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

   SI [ ] NO [X]

FORMATO DE ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador:
Betsy Xiomara Ortega Martinez

Cargo:
Fisioterapeuta.

Fecha:
30 De Mayo De 2016

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?

   SI [X] NO [ ]

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

   SI [ ] NO [X]

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

   SI [ ] NO [X]

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

   WIFI [ ] CABLE [X] OTRO [ ] _____

5. ¿Descarga archivos (programas, música, video?) de internet?

   SI [X] NO [ ]

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

   SI [ ] NO [X]

7. ¿La entidad, ha realzado capacitación sobre temas relacionados a seguridad de información?

   SI [ ] NO [X]

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

   SI [ ] NO [X]

FORMATO DE ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador: Elizabeth Cadena Mejía

Cargo: Terapeuta Ocupacional

Fecha: Mayo - 30 - 2018

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?

   SI [X] NO [ ]

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

   SI [ ] NO [X]

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

   SI [ ] NO [X]

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

   WIFI [ ] CABLE [X] OTRO [ ] _____

5. ¿Descarga archivos (programas, música, video?) de internet?

   SI [X] NO [ ]

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

   SI [ ] NO [X]

7. ¿La entidad, ha realzado capacitación sobre temas relacionados a seguridad de información?

   SI [ ] NO [X]

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

   SI [ ] NO [X]

FORMATO DE ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador:
Betsy Xiomara Ortega Martinez

Cargo:
Fisioterapeuta.

Fecha:
30 De Mayo De 2018

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?

   SI [X] NO [ ]

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

   SI [ ] NO [X]

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

   SI [ ] NO [X]

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

   WIFI [ ] CABLE [X] OTRO [ ] _____

5. ¿Descarga archivos (programas, música, video?) de internet?

   SI [X] NO [ ]

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

   SI [ ] NO [X]

7. ¿La entidad, ha realzado capacitación sobre temas relacionados a seguridad de información?

   SI [ ] NO [X]

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

   SI [ ] NO [X]

FORMATO DE ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador:
Clara Carlosama

Cargo:
Servicios Generales

Fecha:
Mayo -30 de 2018

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?

   SI ☐ NO ☒

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

   SI ☐ NO ☒

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

   SI ☐ NO ☒

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

   WIFI ☐ CABLE ☒ OTRO ☐ _____

5. ¿Descarga archivos (programas, música, video?) de internet?

   SI ☐ NO ☒

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

   SI ☐ NO ☒

7. ¿La entidad, ha realzado capacitación sobre temas relacionados a seguridad de información?

   SI ☐ NO ☒

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

   SI ☐ NO ☒

FORMATO DE ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador:
Libardo Ortega Palacios

Cargo:
Facturador

Fecha:
Mayo. 30-2015

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?

   SI [X] NO [ ]

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

   SI [ ] NO [X]

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

   SI [ ] NO [X]

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

   WIFI [ ] CABLE [X] OTRO [ ] _____

5. ¿Descarga archivos (programas, música, video?) de internet?

   SI [X] NO [ ]

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

   SI [ ] NO [X]

7. ¿La entidad, ha realzado capacitación sobre temas relacionados a seguridad de información?

   SI [ ] NO [X]

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

   SI [ ] NO [X]

FORMATO DE ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador: Fabio Alberto Revelo Messa

Cargo: Ingeniero de Sistemas

Fecha: 05-30-2018

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?

   SI [X] NO [ ]

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

   SI [X] NO [ ]

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

   SI [X] NO [ ]

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

   WIFI [ ] CABLE [X] OTRO [ ] _____

5. ¿Descarga archivos (programas, música, video?) de internet?

   SI [X] NO [ ]

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

   SI [X] NO [ ]

7. ¿La entidad, ha realzado capacitación sobre temas relacionados a seguridad de información?

   SI [ ] NO [X]

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

   SI [ ] NO [X]

FORMATO DE ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador: Fabio Arcilla

Cargo: Asesor

Fecha: 30-Mayo-2018

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?

   SI [X] NO [ ]

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

   SI [X] NO [ ]

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

   SI [ ] NO [X]

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

   WIFI [X] CABLE [ ] OTRO [ ] _____

5. ¿Descarga archivos (programas, música, video) de internet?

   SI [ ] NO [X]

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

   SI [X] NO [ ]

7. ¿La entidad, ha realzado capacitación sobre temas relacionados a seguridad de información?

   SI [ ] NO [X]

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

   SI [ ] NO [X]

FORMATO DE ENCUESTA

Objetivo:

Obtener de los trabajadores de la IPS Solidarios, información sobre el uso y conocimiento de temas referentes a seguridad informática, como fuente para el análisis e identificación de posibles riesgos que puede ser objeto la información de la entidad.

Nombre trabajador: Natalia Diaz

Cargo: Contadora

Fecha: 30 Mayo 2018

Preguntas.

1. ¿Su computador donde labora, tiene instalado antivirus?

   SI [X] NO [ ]

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

   SI [X] NO [ ]

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

   SI [X] NO [ ]

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

   WIFI [X] CABLE [ ] OTRO [ ] _____

5. ¿Descarga archivos (programas, música, video) de internet?

   SI [ ] NO [X]

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

   SI [X] NO [ ]

7. ¿La entidad, ha realzado capacitación sobre temas relacionados a seguridad de información?

   SI [ ] NO [X]

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

   SI [ ] NO [X]

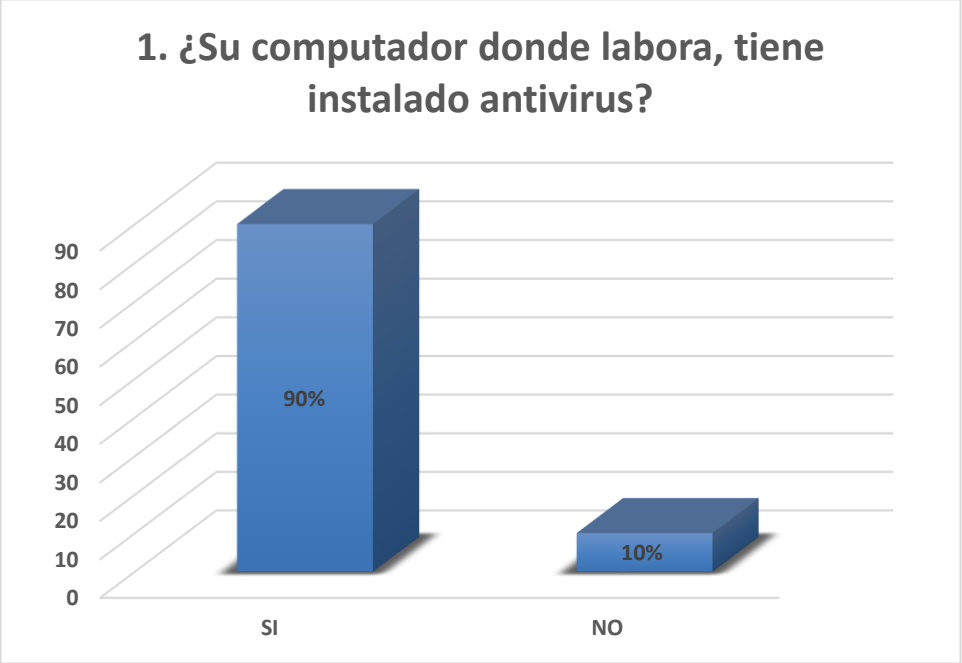
Fuente: Autor

Anexo C Tabulación de la encuesta

Obtenido los resultados de la encuesta realizada en la IPS Solidarios, se procede a realizar el análisis estadístico siguiente:

1. ¿Su computador donde labora, tiene instalado antivirus?

Figura 6 Tabulación Pregunta No. 1 – Trabajadores IPS Solidarios



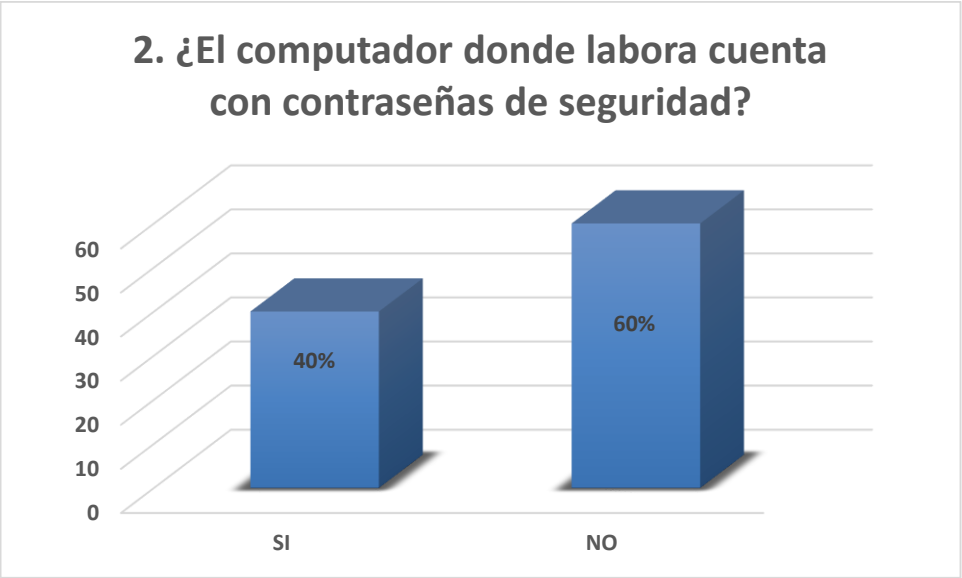
Fuente: El Autor

El 90% de los encuestados, responden afirmativamente a esta necesidad de prevención y protección de la información, y el 10% aseguran lo contrario.

Observación: En la visita a la institución se verificó, que el antivirus que se encontraba instalado es freeware, por lo que se concluye, que tiene una función básica y restringida para la detección de posibles virus informáticos.

2. ¿El computador donde labora cuenta con contraseñas de seguridad?

Figura 7 Tabulación Pregunta No. 2 – Trabajadores IPS Solidarios



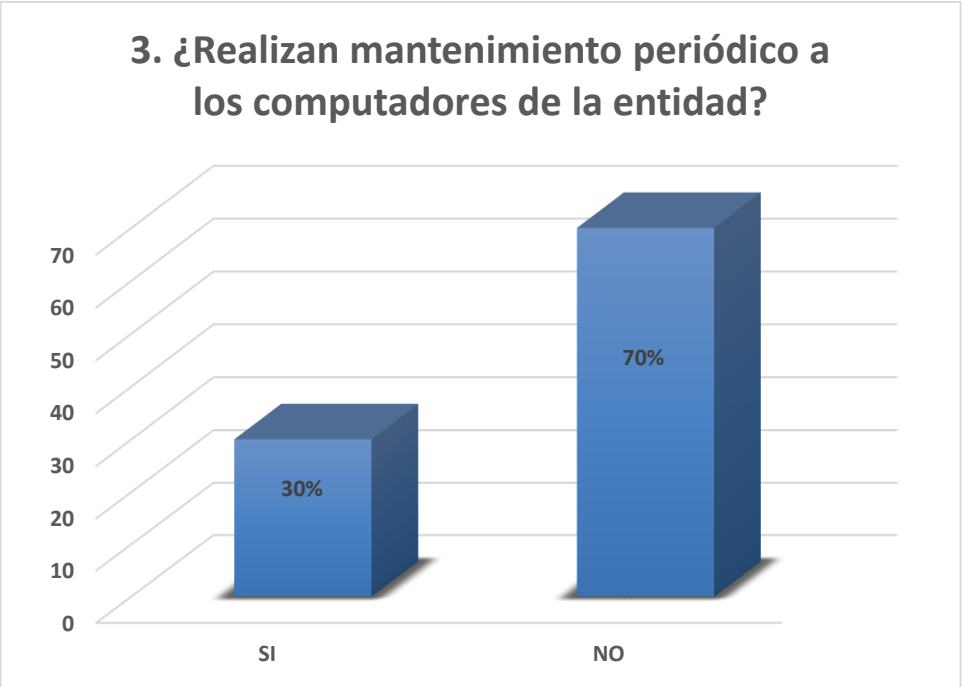
Fuente: El Autor

De los encuestados, el 40% respondió que el ingreso a computador para el desarrollo de sus actividades, tiene una contraseña como medio de control, y el 60% ingresa sin restricción alguna al computador o no tienen protección de contraseña.

Por tanto; se concluye que los equipos informáticos que no cuentan con esta medida de protección por contraseña, puede correr alto riesgo de uso indebido, fuga de información, perdida confidencialidad y robo de información.

3. ¿Realizan mantenimiento periódico a los computadores de la entidad?

Figura 8 Tabulación Pregunta No. 3 – Trabajadores IPS Solidarios



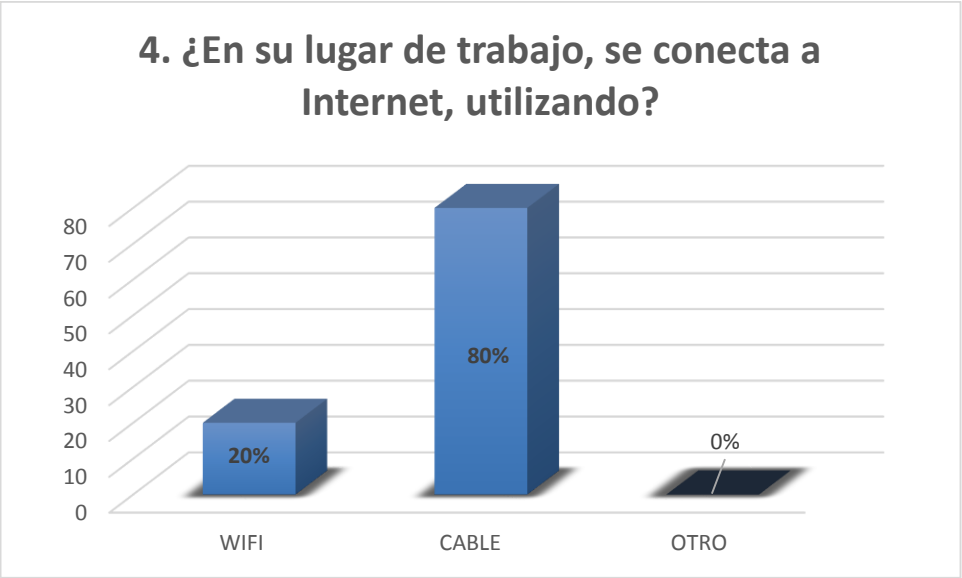
Fuente: El Autor

De la población encuestada, el 30% afirma que se ha realizado mantenimiento a los computadores de la institución, mientras que el 70% argumenta que no ha realizado mantenimiento de los equipos.

Se observó en la entidad, que en ocasiones cuando un computador presenta inconvenientes, el personal de sistemas realiza el soporte necesario para subsanarlo, y aprovecha la actividad para realizar el mantenimiento necesario; es decir éste no es periódico.

4. ¿En su lugar de trabajo, se conecta a Internet, utilizando?

Figura 9 Tabulación Pregunta No. 4 – Trabajadores IPS Solidarios



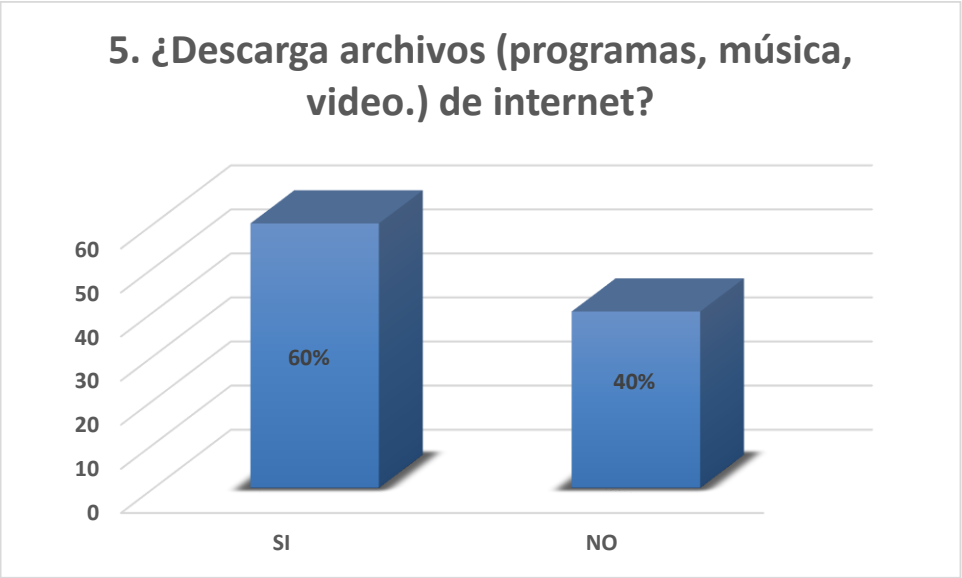
Fuente: El Autor

El 20% de la población, especifica que para conectarse a internet utiliza WIFI, y el 80% de la población objeto, lo realiza mediante la conexión a través de la red de la institución.

Como se puede concluir, existe personal de la institución que utiliza un medio no autorizado para conectarse a internet, contribuyendo a generar un posible riesgo por el uso indebido de los medios informáticos dispuestos para la comunicación.

5. ¿Descarga archivos (programas, música, video) de Internet?

Figura 10 Tabulación Pregunta No. 5 – Trabajadores IPS Solidarios



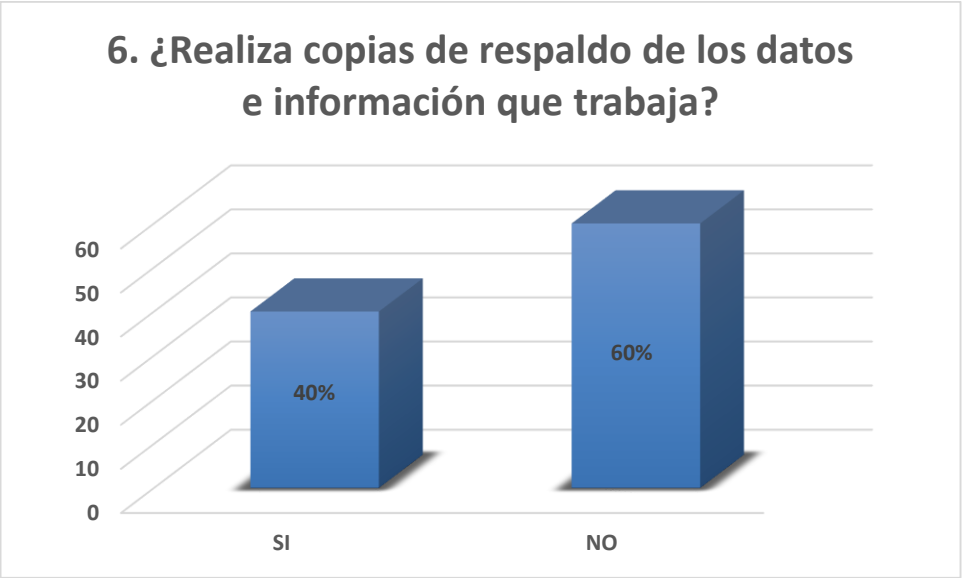
Fuente: El Autor

Como se evidencia el 60% de la población encuestada, asegura haber descargado algún tipo de servicio de Internet durante el desarrollo de su labor empresarial, y el 40%, ha manifestado no realizarlo.

Se observa, que no existe restricción alguna sobre el uso de internet, presentándose como un alto riesgo sobre la confidencialidad, integridad y disponibilidad de la información en la entidad.

6. ¿Realiza copias de respaldo de los datos e información que trabaja?

Figura 11 Tabulación Pregunta No. 6 – Trabajadores IPS Solidarios



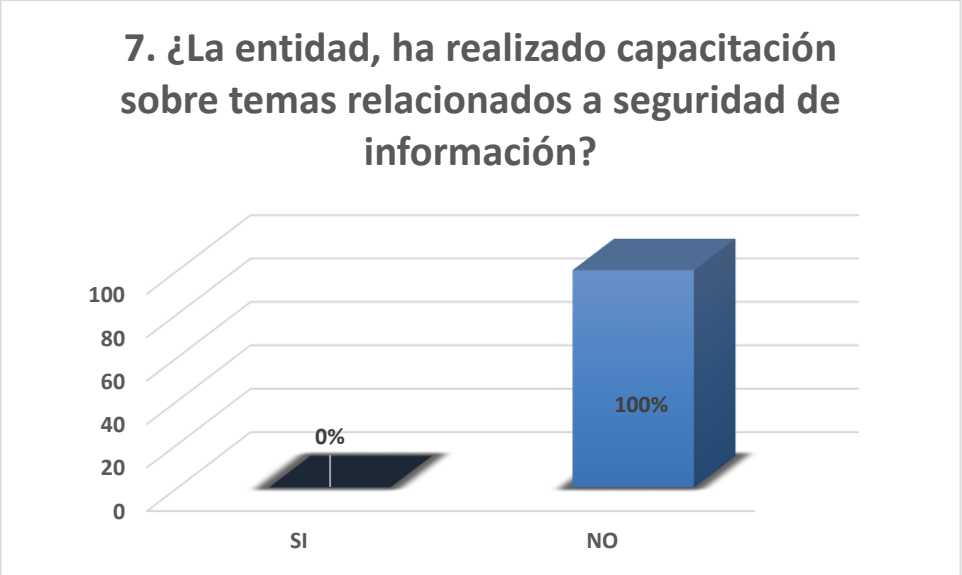
Fuente: El Autor

Como se presenta, por parte del 40% de los encuestados, afirma que si guardan copia de la información que procesan, y el 60% admite que no la realizan.

Al analizar esta pregunta, los trabajadores no tienen una cultura de proteger la información que procesan, y la importancia de la misma es vista en un segundo plano.

7. ¿La entidad, ha realizado capacitación sobre temas relacionados a seguridad de información?

Figura 12 Tabulación Pregunta No. 7 – Trabajadores IPS Solidarios



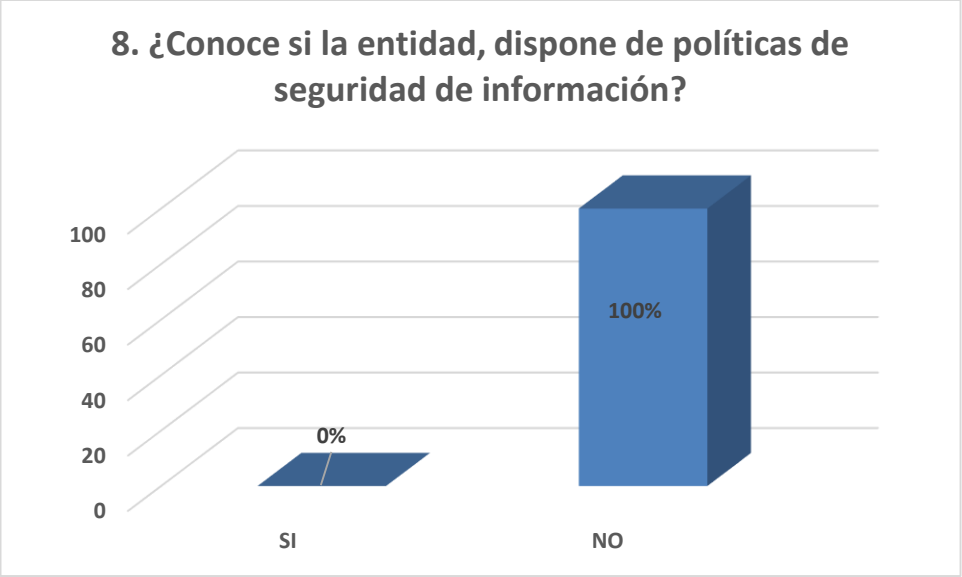
Fuente: El Autor

El 100% de la población asegura que no han recibido capacitación sobre temáticas relacionadas con seguridad de la información.

Se concluye, la importancia de realizar el diagnóstico, identificación y análisis sobre los riesgos que pueden afectar a la entidad.

8. ¿Conoce si la entidad, dispone de políticas de seguridad de información?

Figura 13 Tabulación Pregunta No. 8 – Trabajadores IPS Solidarios



Fuente: El Autor

De la población encuestada, el 100% responde que no se han establecido políticas de seguridad en la entidad.

Con lo anterior se puede determinar, que la IPS Solidarios del municipio de Cuaspud Carlosama, es necesario contar con medidas preventivas, sustentadas en unas políticas de seguridad como directriz para el buen uso de los activos informáticos.

Anexo D Entrevistas a Socios

Socio 1

ENTREVISTA A SOCIOS

¿Qué opinión merece el uso de las computadoras y los aplicativos de software en su entidad?

Que son útiles para que los trabajadores de la empresa desarrollen sus actividades.

¿Qué importancia es para Uds. proteger la información que procesa su entidad?

Es importante porque los usuarios merecen todo el respeto de la empresa.

¿Existe personal calificado en seguridad informática?

Hay una persona que hace mantenimiento a los computadores.

¿La entidad cuenta con medidas de seguridad para proteger la información?

No lo sé, pero hay personal de sistemas.

¿Existen políticas de seguridad definidas en su entidad?

No lo sé, es aspecto de gerencia y el personal que maneja los computadores.

¿Se han realizado capacitaciones al personal sobre temas de prevención y protección de la información?

No lo sé.

¿En la entidad se han presentado daños por problemas de seguridad informática?

No lo sé, pero suele presentarse suspensión del fluido eléctrico.

¿Apoya el desarrollo de este proyecto sobre identificación de riesgos en su entidad?

Sí, porque se mejorará la empresa en el manejo de la información.

Socio 2

ENTREVISTA A SOCIOS

¿Que Opinión merece el uso de las computadoras y los aplicativos de software en su entidad? Son indispensables, frente a procesos de organizacion, sistematizacion, seguridad y Agilidad de información

¿Qué importancia es para ustedes proteger la información que procesa su entidad?
De gran importancia, en referencia a procesos de historias Clinicas facturacion, contabilidad.

¿Existe personal calificado en seguridad informática?
Se encarga un Ingeniero de sistemas, en lo referente a equipos de computo en mantenimiento y actualizacion de software.

¿La entidad cuenta con medidas de seguridad para proteger la información?
Algunos encomendados, como antivirus, claves, información de respaldo

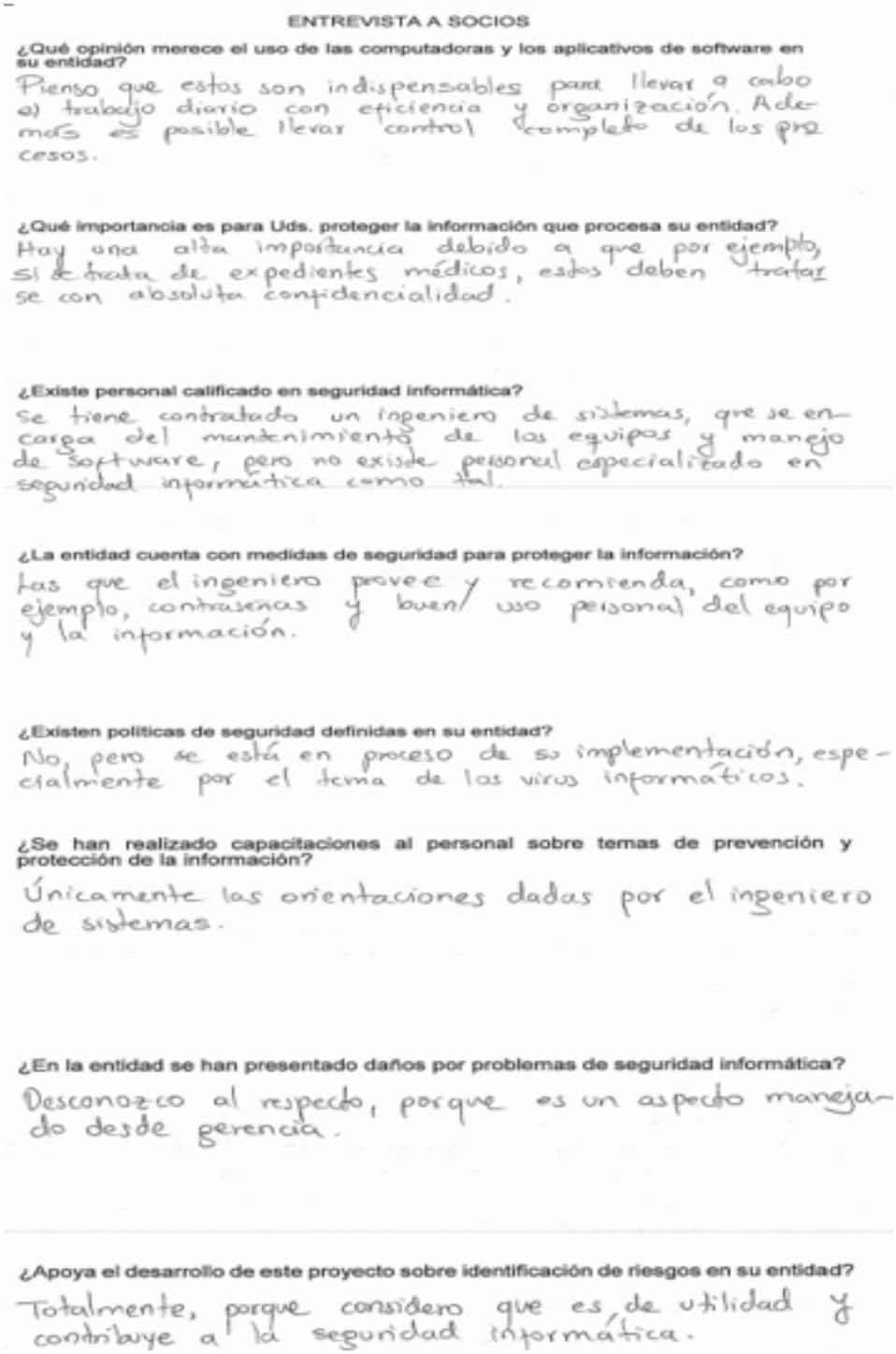
¿Existen políticas de seguridad definidas en su entidad?
Se ha hablado de la posibilidad de implementar ya que es necesario frente a virus informaticos, ante todo el manejo de información

¿Se han realizado capacitaciones al personal sobre temas de prevención y protección de la información?
Recomendaciones brindadas por el Ingeniero de Sistemas.

¿En la entidad se han presentado daños por problemas de seguridad informática?
En alguna ocasion daños menores a equipos de sistemas, y a software de facturación

¿Apoya el desarrollo de ese Proyecto sobre identificación de riesgos en su entidad?
Es necesario e indispensable, y servira para el fortalecimiento de seguridad informatico.

Socio 3



ENTREVISTA A SOCIOS

¿Qué opinión merece el uso de las computadoras y los aplicativos de software en su entidad?

Pienso que estos son indispensables para llevar a cabo el trabajo diario con eficiencia y organización. Además es posible llevar control completo de los procesos.

¿Qué importancia es para Uds. proteger la información que procesa su entidad?

Hay una alta importancia debido a que por ejemplo, si se trata de expedientes médicos, estos deben tratarse con absoluta confidencialidad.

¿Existe personal calificado en seguridad informática?

Se tiene contratado un ingeniero de sistemas, que se encarga del mantenimiento de los equipos y manejo de software, pero no existe personal especializado en seguridad informática como tal.

¿La entidad cuenta con medidas de seguridad para proteger la información?

Las que el ingeniero provee y recomienda, como por ejemplo, contraseñas y buen uso personal del equipo y la información.

¿Existen políticas de seguridad definidas en su entidad?

No, pero se está en proceso de su implementación, especialmente por el tema de los virus informáticos.

¿Se han realizado capacitaciones al personal sobre temas de prevención y protección de la información?

Únicamente las orientaciones dadas por el ingeniero de sistemas.

¿En la entidad se han presentado daños por problemas de seguridad informática?

Desconozco al respecto, porque es un aspecto manejado desde gerencia.

¿Apoya el desarrollo de este proyecto sobre identificación de riesgos en su entidad?

Totalmente, porque considero que es de utilidad y contribuye a la seguridad informática.

Fuente: El Autor

Comentarios de la entrevista a socios:

Los socios, resaltan la importancia del usar las computadoras en la entidad en el desarrollo de sus actividades, como es el caso de facturación, controles y agilidad en los procesos. También, refieren que se debe proteger la información, en especial la confidencialidad de las historias clínicas de los usuarios. Además, especifican que cuentan con un ingeniero de sistemas que es el encargado de dar soporte a los equipos informáticos, pero no hay personal especializado en seguridad informática. Informan, que las medidas de protección son las que el personal de sistemas establece, como instalar antivirus y crear contraseñas; piensan en la posibilidad de crear políticas de seguridad para unos temas, como el caso de los virus informáticos. Comentan, que se han presentado problemas en algunos equipos de la entidad, por suministro de fluido eléctrico y algunos daños menores en los equipos de sistemas y de facturación. Resaltan la importancia del presente proyecto por ayudar a fortalecer el manejo de la información y la seguridad informática.

Anexo E Valoración del riesgo sobre los activos IPS Solidarios

Clasificación de las amenazas:

N: Desastres naturales.
I: De origen Industrial.
E: Errores y fallos no intencionados.
A: Ataques Intencionados.

Tabla 29 Identificación de activos, amenazas, vulnerabilidades y valoración del riesgo en la IPS Solidarios

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
[files]	Ficheros	E	**[E.1]**	Errores de los usuarios	Falta de mecanismos de protección y control en el ingreso de información por parte del personal operativo	A	2	B	1	2	B	B
			[E.15]	Alteración accidental de la información	Falta de mecanismos de control al momento de Manipular la información	A	1	MB	10	3	M	MB
			[E.19]	Fugas de información	Carencia de políticas en el manejo de la información por parte del personal operativo	A	3	M	100	4	A	A
[conf_sv]	Datos de Configuración. Servidor	E	**[E.2]**	Errores del administrador	Bajo conocimiento e Ingreso de información errada por parte del administrador	M	3	M	10	2	B	M

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
			[E.15]	Alteración accidental de la información	Manipulación errada de información por parte del administrador	M	1	MB	10	2	B	MB
			[E.19]	Fugas de información	Carencia de políticas en el manejo de la información por parte del administrador	M	3	M	100	3	M	M
[acl]	Datos de control de Acceso	A	**[A.5]**	Suplantación de la identidad del usuario	No existen mecanismos de identificación y restricción de usuarios	M	2	B	100	3	M	B
			[A.15]	Modificación deliberada de la información	No existen mecanismos de identificación y restricción de usuarios	M	2	B	100	3	M	B
			[A.18]	Destrucción de información	No existen mecanismos de identificación y restricción de usuarios	M	3	M	100	3	M	M
[public_signature]	Claves de firma digital	E	**[E.1]**	Errores de los usuarios	Bajo conocimiento del manejo de los dispositivos criptográficos	A	2	B	1	2	B	B
			[E.19]	Fugas de información	carencia de medidas de control y de protección sobre los dispositivos criptográficos	A	3	M	100	4	A	A
[Internet]	Internet	E	**[E.24]**	Caída del sistema por agotamiento de recursos	bajos recursos suficientes para el procesamiento de información	B	3	M	10	1	MB	B

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
[email]	Correo electrónico	A	**[A.5]**	Suplantación de la identidad del usuario	No hay Controles adecuados de Ingreso a los equipos de computo	M	2	B	100	3	M	B
			[A.6]	Abuso de privilegios de acceso	Deficiencia en la creación de perfiles de usuario, por parte del administrador de la red	M	2	B	100	3	M	B
			[A.11]	Acceso no autorizado	No existe mecanismos de autenticación e identificación adecuados	M	2	B	100	3	M	B
			[A.18]	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo	M	2	B	100	3	M	B
		E	**[E.19]**	Fugas de información	Ausencia de capacitaciones al Personal sobre seguridad y protección de la información	M	3	M	100	3	M	M
[sub_Fact]	Sistema de Facturación y Estadística	E	**[E.1]**	Errores de los usuarios.	Bajo conocimiento del Sistema de Facturación y estadística por el personal operativo	MA	2	B	1	3	M	B
			[E.2]	Errores del administrador	Configuración inadecuada del Sistema de Facturación por el personal administrador	MA	3	M	10	4	A	A

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
			[E.8]	Difusión de software dañino	Utilización de sistemas de protección de prueba o libres (freeware o shareware)	MA	3	M	100	5	MA	A
			[E.15]	Alteración accidental de la información	Manipulación errada de información por parte del personal de la institución	MA	1	MB	10	4	A	B
			[E.21]	Errores de mantenimiento / actualización de programas (software)	Actualizaciones o mantenimiento no efectivo y eficaz por parte del proveedor del software	MA	3	M	10	4	A	A
		A	**[A.6]**	Abuso de privilegios de acceso	conocimiento e Ingreso al sistema como superusuario, por cualquier trabajador del sistema de la institución	MA	4	A	100	5	MA	MA
			[A.11]	Acceso no autorizado	No existe mecanismos de autenticación e identificación adecuados	MA	4	A	100	5	MA	MA
			[A.18]	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo	MA	3	M	100	5	MA	A
			[A.19]	Divulgación de información	Personal con bajo compromiso institucional y falta de ética en el manejo de la información reservada	MA	3	M	10	4	A	A

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
[sub_Con]	Sistema de Contabilidad	E	**[E.1]**	Errores de los usuarios.	Bajo conocimiento del Aplicativo de Contabilidad por el personal operativo	MA	2	B	1	3	M	B
			[E.2]	Errores del administrador	Configuración inadecuada del Aplicativo de Contabilidad por el personal administrador	MA	3	M	10	4	A	A
			[E.8]	Difusión de software dañino	Utilización de sistemas de protección de prueba o libres (freneare o shareware)	MA	3	M	100	5	MA	A
			[E.15]	Alteración accidental de la información	Manipulación errada de información por parte del personal de la institución	MA	1	MB	10	4	A	B
			[E.21]	Errores de mantenimiento / actualización de programas (software)	Actualizaciones o mantenimiento no efectivo y eficaz por parte del proveedor del software	MA	3	M	10	4	A	A
		A	**[A.6]**	Abuso de privilegios de acceso	conocimiento e Ingreso al sistema como superusuario, por cualquier trabajador del sistema de la institución	MA	4	A	100	5	MA	MA
			[A.11]	Acceso no autorizado	No existe mecanismos de autenticación e identificación adecuados	MA	4	A	100	5	MA	MA

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
			[A.18]	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo	MA	3	M	100	5	MA	A
			[A.19]	Divulgación de información	Personal con bajo compromiso institucional y falta de ética en el manejo de la información reservada	MA	3	M	10	4	A	A
[os]	Sistema Operativos Windows	E	**[E.2]**	Errores del administrador	Falta de conocimiento en los procesos de administración y/ instalación del Sistema Operativo por el personal administrador	A	3	M	10	3	M	M
			[E.4]	Errores de configuración	Configuración inadecuada del Sistema Operativo por el personal administrador	A	3	M	10	3	M	M
			[E.15]	Alteración accidental de la información	Manipulación errada de información por parte del administrador al configurar el SO	A	1	MB	10	3	M	MB
			[E.18]	Destrucción de información	No existe una adecuada administración de los directorios del SO	A	1	MB	100	4	A	B
			[E.21]	Errores de mantenimiento / actualización de programas (software)	Falta de frecuencia de actualización y mantenimiento del SO	A	3	M	10	3	M	M

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
		A	**[A.6]**	Abuso de privilegios de acceso	Falta de creación de privilegios y perfiles para los usuarios, todos pueden ser superusuarios.	A	4	A	100	4	A	MA
			[A.11]	Acceso no autorizado	No existe control para el acceso e identificación a los usuarios. SE verifican puertos abiertos que sirven de puertas traseras para ingresar al sistema.	A	4	A	100	4	A	MA
			[A.18]	Destrucción de información	Falta de realización frecuente de copias de respaldo de la informaron sensible	A	3	M	100	4	A	A
			[A.19]	Divulgación de información	No existe medidas de control al procesar información sensible	A	3	M	10	3	M	M
			[A.22]	Manipulación de Programas	Configuraciones deficientes o modificaciones de aplicaciones que permiten el control y seguridad del sistema	A	2	B	100	4	A	M
[dbms_access]	Bases de Datos Access	E	**[E.1]**	Errores de los usuarios.	Bajo conocimiento del manejo de Bases de Datos	M	2	B	1	1	MB	MB
			[E.2]	Errores del administrador	Falta de conocimiento en los procesos de administración de las Bases de Datos por el personal administrador	M	3	M	10	2	B	M

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
			[E.15]	Alteración accidental de la información	Manipulación errada de información por parte del personal de la institución	M	1	MB	10	2	B	MB
			[E.18]	Destrucción de información	No existe una adecuada administración y protección de los directorios donde residen las bases de datos	M	1	MB	100	3	M	MB
		A	**[A.11]**	Acceso no autorizado	No existe mecanismos de restricción al acceso a las bases de datos	M	4	A	100	3	M	A
			[A.18]	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo	M	2	B	100	3	M	B
			[A.19]	Divulgación de información	Personal con bajo compromiso institucional y falta de ética en el manejo de la información reservada	M	3	M	10	2	B	M
[office]	Ofimática	E	**[E.1]**	Errores de los usuarios.	Bajo conocimiento del personal en el manejo de las aplicaciones de oficina y error al ingresar la información.	MB	2	B	1	1	MB	MB
[av]	Antivirus	E	**[E.2]**	Errores del administrador	Falta de conocimiento en los procesos de administración y configuración del	M	3	M	10	2	B	M

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
					Antivirus por el personal administrador.							
			[E.21]	Errores de mantenimiento / actualización de programas (software)	Instalación de Antivirus de versiones de prueba o versiones reducidas.	M	3	M	10	2	B	M
[firewall]	Firewall	E	**[E.2]**	Errores del administrador	Falta de conocimiento en los procesos de administración y configuración del Firewall por el personal administrador.	M	3	M	10	2	B	M
			[E.21]	Errores de mantenimiento / actualización de programas (software)	Instalación de Firewalls de versiones de prueba o versiones reducidas.	M	3	M	10	2	B	M
[browser]	Navegador Web	E	**[E.8]**	Difusión de software dañino	Instalación de complementos innecesarios que pueden permitir captura de información sensible	M	3	M	100	3	M	M
			[E.21]	Errores de mantenimiento / actualización de programas (software)	Instalación de complementos innecesarios que pueden permitir captura de información sensible	M	3	M	10	2	B	M

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
		A	**[A.22]**	Manipulación de Programas	Instalación de complementos innecesarios que pueden permitir captura de información sensible	M	2	B	100	3	M	B
[mid]	Equipo Host - (Aplicaciones)	I	**[I.3]**	Contaminación mecánica	No existe un plan de mantenimiento preventivo y correctivo para evitar el deterioro o corrosión de los componentes físicos por polvo.	M	3	M	10	2	B	M
			[I.5]	Avería de origen físico o lógico	No se realiza una limpieza periódica de los componentes físicos de los equipos	M	3	M	10	2	B	M
			[I.6]	Corte del suministro eléctrico	No se identifica fuentes de alimentación regulada y alterna	M	3	M	100	3	M	M
		E	**[E.23]**	Errores de mantenimiento / actualización de Equipos (hardware)	No existe un plan de mantenimiento preventivo y correctivo para evitar el deterioro o corrosión de los componentes físicos	M	1	MB	100	3	M	MB
		A	**[A.25]**	Robo	No hay restricción de personal a las oficinas donde están los equipos computacionales de la organización, por mecanismo alguno.	M	2	B	100	3	M	B

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
[mobile]	Computadores Portátiles	I	**[I.3]**	Contaminación mecánica	No existe un plan de mantenimiento preventivo y correctivo para evitar el deterioro o corrosión de los componentes físicos por polvo.	B	3	M	10	1	MB	B
			[I.5]	Avería de origen físico o lógico	No se realiza una limpieza periódica de los componentes físicos de los equipos	B	3	M	10	1	MB	B
			[I.6]	Corte del suministro eléctrico	No se identifica fuentes de alimentación regulada y alterna	B	3	M	100	2	B	M
		E	**[E.23]**	Errores de mantenimiento / actualización de Equipos (hardware)	No existe un plan de mantenimiento preventivo y correctivo para evitar el deterioro o corrosión de los componentes físicos	B	1	MB	100	2	B	MB
		A	**[A.25]**	Robo	No existe restricción de personal a las oficinas donde están los equipos computacionales de la organización.	B	2	B	100	2	B	B
[router]	Router	A	**[A.11]**	Acceso no autorizado	No existen mecanismos de restricción a los dispositivos de comunicación o rejillas de protección.	A	4	A	100	4	A	MA

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
			[A.25]	Robo	No existe restricción de personal a las oficinas donde están los equipos computacionales de la organización.	A	2	B	100	4	A	M
		E	**[E.2]**	Errores del administrador	Bajo conocimiento o equivocación en el manejo del dispositivo por parte del administrador	A	3	M	10	3	M	M
			[E.4]	Errores de configuración	Falta de conocimiento en los procesos de administración y configuración del dispositivo por el personal administrador	A	3	M	10	3	M	M
		I	**[I.5]**	Avería de origen físico o lógico	No se realiza una limpieza periódica de los componentes físicos de los equipos por deterioro o corrosión de los componentes por uso y tiempo de vida	A	3	M	10	3	M	M
			[I.6]	Corte del suministro eléctrico	No se identifica fuentes de alimentación regulada y alterna	A	3	M	100	4	A	A
[switch]	Switch	A	**[A.25]**	Robo	No existe restricción de personal a las oficinas donde están los equipos computacionales de la organización.	M	2	B	100	3	M	B

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
		I	**[I.6]**	Corte del suministro eléctrico	No se identifica fuentes de alimentación regulada y alterna	M	3	M	100	3	M	M
[printer]	Impresora Multifuncional	I	**[I.3]**	Contaminación mecánica	No existe un plan de mantenimiento preventivo y correctivo para evitar el deterioro o corrosión de los componentes físicos por polvo.	B	3	M	10	1	MB	B
			[I.5]	Avería de origen físico o lógico	Deterioro o corrosión de los componentes por uso y tiempo de vida	B	3	M	10	1	MB	B
		E	**[E.23]**	Errores de mantenimiento / actualización de Equipos (hardware)	No existe un plan de mantenimiento preventivo y correctivo para evitar el deterioro o corrosión de los componentes físicos	B	1	MB	100	2	B	MB
		A	**[A.25]**	Robo	No existe restricción de personal a las oficinas donde están los equipos computacionales de la organización.	B	2	B	100	2	B	B
[lan]	Red Local – LAN	I	**[I.8]**	Fallo de servicios de comunicaciones	Falta de protección del cableado estructurado.	A	2	B	10	3	M	B
		E	**[E.2]**	Errores del administrador	Bajo conocimiento o equivocación en la administración de la RED parte del administrador	A	3	M	10	3	M	M

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
			[E.24]	Caída del sistema por agotamiento de recursos	Utilización indebida de los recursos del sistema necesarios para atender la demanda de los usuarios de la red. Juegos, shopping, videos, descargas aplicaciones, etc. Falta de un plan de recuperación del servicio	A	3	M	10	3	M	M
		A	**[A.7]**	Uso no previsto	Utilización indebida de los recursos del sistema necesarios para atender la demanda de los usuarios de la red. Juegos, shopping, videos, descargas aplicaciones, etc.	A	2	B	100	4	A	M
			[A.11]	Acceso no autorizado	No existen control de ingreso a los equipos informáticos para personal externo	A	4	A	100	4	A	MA
			[A.24]	Denegación de servicio	Utilización indebida de los recursos del sistema necesarios para atender la demanda de los usuarios de la red. Juegos, shopping, videos, descargas aplicaciones, etc.	A	2	B	10	3	M	B

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
[Internet]	Internet	I	**[I.8]**	Fallo de servicios de comunicaciones	Falta de protección del cableado estructurado.	B	2	B	10	1	MB	MB
		E	**[E.24]**	Caída del sistema por agotamiento de recursos	Utilización indebida de los recursos del sistema necesarios para atender la demanda de los usuarios de la red. Juegos, shopping, videos, descargas aplicaciones, etc.	B	3	M	10	1	MB	B
		A	**[A.7]**	Uso no previsto	Utilización indebida de los recursos del sistema necesarios para atender la demanda de los usuarios de la red. Juegos, shopping, videos, descargas aplicaciones, etc.	B	2	B	100	2	B	B
			[A.11]	Acceso no autorizado	No existen control de ingreso a los equipos informáticos para personal externo	B	4	A	100	2	B	A
			[A.24]	Denegación de servicio	Utilización indebida de los recursos del sistema necesarios para atender la demanda de los usuarios de la red. Juegos, shopping, videos, descargas aplicaciones, etc.	B	2	B	10	1	MB	MB

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
[san_cld]	Servicio Respaldo (Drive)	E	**[E.1]**	Errores de los usuarios	Baja operatividad y conocimiento de los procesos de respaldo	MA	2	B	1	3	M	B
			[E.2]	Errores del administrador	Falta de conocimiento de los procesos de administración y configuración de los procesos de respaldo de la información por el personal administrador.	MA	3	M	10	4	A	A
		A	**[A.18]**	Destrucción de información	Manejo inadecuado y creación de contraseñas débiles por parte del personal administrativo	MA	2	B	100	5	MA	M
			[A.24]	Denegación de servicio	Personal con bajo compromiso institucional y falta de ética en el manejo de la información reservada	MA	2	B	10	4	A	M
[usb]	Dispositivos USB.	A	**[A.15]**	Modificación deliberada de la información	Uso inadecuado de los dispositivos extraíbles por parte del personal	A	2	B	1	2	B	B
		I	**[I.5]**	Avería de origen físico o lógico	Deterioro o corrosión de los componentes por uso y tiempo de vida	A	3	M	10	3	M	M
		A	**[A.25]**	Robo	No existen políticas de manejo y control de los dispositivos extraíbles	A	2	B	100	4	A	M

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
[printed]	Historias Clínicas	I	**[I.1]**	Fuego	Se identifica en la sala de espera de la institución un único extintor de Químico Seco no apto para equipos electrónicos.	MA	1	MB	100	5	MA	B
			[I.7]	Condiciones inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.	MA	3	M	10	4	A	A
			[I.10]	Degradación de los soportes de almacenamiento de la información	No existe un manejo técnico y adecuado del archivo de historias clínicas, en cuanto a almacenamiento, custodia y disposición final.	MA	3	M	100	5	MA	A
		N	**[N.7]**	Desastres naturales	La organización se encuentra en zona de riesgo medio por estar rodeado de volcanes: Galeras, Cumbal, Chiles.	MA	1	MB	100	5	MA	B
[power]	Fuentes de alimentación	I	**[I.6]**	Corte del suministro eléctrico	No se identifica fuentes de alimentación regulada y alterna	M	3	M	100	3	M	M
[cabling]	Cableado de datos.	I	**[I.1]**	Fuego	Se identifica en la sala de espera de la institución un único extintor de Químico Seco no apto para equipos electrónicos.	A	1	MB	100	4	A	B
			[I.7]	Condiciones inadecuadas de	No existe sistema de alarma de control de	A	3	M	10	3	M	M

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
				temperatura o humedad	temperatura y humedad.							
[ups]	UPS (Sistemas de Poder Ininterrumpido)	I	**[I.1]**	Fuego	Se identifica en la sala de espera de la institución un único extintor de Químico Seco no apto para equipos electrónicos.	M	1	MB	100	3	M	MB
		N	**[N.7]**	Desastres naturales	La organización se encuentra en zona de riesgo medio por estar rodeado de volcanes: Galeras, Cumbal, Chiles.	M	1	MB	100	3	M	MB
[Edificio Principal]	Edificio Principal	I	**[I.1]**	Fuego	Se identifica en la sala de espera de la institución un único extintor de Químico Seco no apto para equipos electrónicos.	A	1	MB	100	4	A	B
		N	**[N.7]**	Desastres naturales	La organización se encuentra en zona de riesgo medio por estar rodeado de volcanes: Galeras, Cumbal, Chiles.	A	1	MB	100	4	A	B
		I	**[I.*]**	Desastres Industriales	No se identifica fuentes de alimentación regulada y alterna. Posibles fluctuación eléctrica	A	3	M	100	4	A	A
[op]	Ingeniero en Sistemas	E	**[E.28]**	Indisponibilidad del personal	Delegación del control de los procesos a una	A	3	M	10	3	M	M

CODIGO	NOMBRE DEL ACTIVO	CLASIFICACION DE LA AMENAZA	COD	AMENAZAS	VULNERABILIDADES	VALOR DEL ACTIVO	FRECUENCIA		DEGRADACION	IMPACTO		RIESGO
					sola persona o administrador							
		A	**[A.30]**	Ingeniería Social (Picaresca)	No se evidencia capacitación al personal sobre prevención y manejo de la información y el riesgo a que está expuesta.	A	3	M	10	3	M	M

Fuente: El Autor

Anexo F Lista de Chequeo Controles y Dominios ISO 27002:2013.

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	5. POLÍTICAS DE SEGURIDAD.		**0**	**2**	**2**	**0**					
Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.	**5.1 Directrices de la Dirección en seguridad de la información.**										
	5.1.1 Conjunto de políticas para la seguridad de la información.	¿La empresa cuenta con políticas para la seguridad de la información, conocida por los empleados?		X			Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes.			X	X
	5.1.2 Revisión de las políticas para la seguridad de la información.	¿Las políticas de seguridad de la información son revisadas con regularidad?		X			Este control aplica desde el momento que se definan y formalicen las políticas de seguridad.			X	X
	6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.		**2**	**5**	**7**	**29**					
Establecer un esquema directivo de gestión para iniciar y controlar la implementación y operativa de la seguridad de la información en la organización.	**6.1 Organización interna.**										
	6.1.1 Asignación de responsabilidades para la seguridad de la información.	¿Los empleados cuentan con responsabilidades sobre la seguridad de la información?		X			Se deberían definir y asignar claramente todas las responsabilidades para la seguridad de la información.			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	6.1.2 Segregación de tareas.	¿Los empleados tienen funciones definidas, con sus respectivas responsabilidades y activos a cargo?	X				En los acuerdos contractuales se establece roles y funciones específicas a los funcionarios en relación a la protección y custodia de los bienes asignados.		X	X	
	6.1.3 Contacto con las autoridades.	¿Se tiene actualizado los contactos de las entidades?	X				La entidad mantiene actualizada la lista de contactos con las autoridades para los casos que se requieran su actuación,			X	X
	6.1.4 Contacto con grupos de interés especial.	¿En la empresa existen contactos hacia otros grupos o foros de seguridad?		X			La entidad no mantiene relación con grupos o foros especializados sobre seguridad.				
	6.1.5 Seguridad de la información en la gestión de proyectos.	¿Se tiene garantía y seguridad de los proyectos a ejecutarse en la organización?		X			En la entidad no se han formalizado proyectos independientes para su desarrollo, por tal razón el control no es aplicable.				
Garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.	**6.2 Dispositivos para movilidad y teletrabajo.**										
	6.2.1 Política de uso de dispositivos para movilidad.	¿Existen políticas para el uso de dispositivos móviles?		X			La entidad no cuenta con políticas sobre los dispositivos móviles.			X	X
	6.2.2 Teletrabajo.	¿Existen políticas de seguridad de acceso para el teletrabajo?		X			La entidad no ha definido otras alternativas laborales como el teletrabajo, por lo tanto este control no aplica.				

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.		**4**	**2**	**6**	**67**					
Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.	**7.1 Antes de la contratación.**										
	7.1.1 Investigación de antecedentes.	¿La empresa verifica los antecedentes de los empleados nuevos?	X				La entidad verifica los antecedentes de los trabajadores que ingresan por primera vez.		X	X	
	7.1.2 Términos y condiciones de contratación.	¿La organización realiza contratos con sus empleados determinando los términos y condiciones del trabajo?	X				La entidad formaliza los términos y condiciones laborales en las minutas contractuales entre cada trabajador y la entidad.		X	X	
Asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.	**7.2 Durante la contratación.**										
	7.2.1 Responsabilidades de gestión.	¿La organización verifica el cumplimiento de políticas de seguridad para con sus empleados?		X			Este control aplica desde el momento que se definan y formalicen las políticas de seguridad.				
	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	¿La organización capacita, entrena y actualiza a sus empleados?		X			La entidad debe realizar capacitaciones a los trabajadores en los cambios normativos, además se enfatice en la sensibilidad de la información que se maneja.			X	X
	7.2.3 Proceso disciplinario.	¿La organización abre procesos disciplinarios en caso que un empleado incumpla los términos o condiciones?	X				La entidad aborda las faltas cometidas por los funcionarios según las cláusulas contractuales establecidas.		X		

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
Proteger los intereses de la organización durante el proceso de cambio o finalización de empleo por parte de empleados y contratistas.	**7.3 Cese o cambio de puesto de trabajo.**										
	7.3.1 Cese o cambio de puesto de trabajo.	¿La empresa tiene un proceso para cesar las actividades de un empleado o contrato?	X				La entidad aborda la terminación contractual de los funcionarios según las cláusulas contractuales establecidas.			X	X
	8. GESTIÓN DE ACTIVOS.		**8**	**2**	**10**	**80**					
Identificar los activos en la organización y definir las responsabilidades para una protección adecuada.	**8.1 Responsabilidad sobre los activos.**										
	8.1.1 Inventario de activos.	¿La organización clasifica todos sus activos en un inventario?	X				La entidad si lleva registro actualizado de sus activos en un inventario.			X	X
	8.1.2 Propiedad de los activos.	¿La organización asigna un responsable a cada uno de los activos?	X				La entidad asigna la responsabilidad de sus activos considerando la responsabilidad de las actividades desempeñadas por el trabajador en su respectiva área.		X	X	
	8.1.3 Uso aceptable de los activos.	¿En la organización se realiza un adecuado manejo de cada activo?	X				La entidad realiza un control sobre el uso y manejo de los activos asignados a cada trabajador.			X	X
	8.1.4 Devolución de activos.	¿Una vez un empleado deja su cargo devuelve los activos en su poder?	X				La entidad solicita el trámite de un paz y salvo para validar la entrega los activos en custodia del trabajador saliente.			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
Asegurar que se aplica un nivel de protección adecuado a la información.	**8.2 Clasificación de la información.**										
	8.2.1 Directrices de clasificación.	¿En la organización se clasifica la información de acuerdo a su sensibilidad, requisitos legales y criticidad?	X				La entidad clasifica la información teniendo las normatividad del orden nacional, contractual y directriz institucional.	X		X	
	8.2.2 Etiquetado y manipulado de la información.	¿La organización clasifica, identifica y etiqueta la información, de acuerdo a sus directrices?	X				La entidad clasifica la información de acuerdo a la normatividad del orden nacional, contractual y directriz institucional.	X		X	
	8.2.3 Manipulación de activos.	¿Los procesos desarrollados para la manipulación y uso de la información se realizan en base a la clasificados adoptaba por la entidad?	X				La entidad desarrolla sus procesos con base a las directrices institucionales.			X	X
Evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento	**8.3 Manejo de los soportes de almacenamiento.**										
	8.3.1 Gestión de soportes extraíbles.	¿La organización tiene procedimientos para la gestión de medios extraíbles?		X			Generar políticas para el manejo y uso de hardware.			X	X
	8.3.2 Eliminación de soportes.	¿La organización desecha de forma adecuada los medios extraíbles que ya no se usaran?		X			Generar políticas para el manejo y uso de hardware.			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	8.3.3 Soportes físicos en tránsito.	¿La organización protege la información que se encuentra en tránsito por fuera de los límites físicos?	X				La entidad protege la información que es requerida externamente, el envió se realiza mediante procesos criptográficos o si es física su custodia la realiza el personal autorizado.			X	X
	9. CONTROL DE ACCESOS.		**9**	**5**	**14**	**64**					
Controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.	**9.1 Requisitos de negocio para el control de accesos.**										
	9.1.1 Política de control de accesos.	¿La organización cuenta con políticas de acceso a los activos e información?		X			Generar políticas sobre sistemas de información e infraestructura tecnológica.			X	X
	9.1.2 Control de acceso a las redes y servicios asociados.	¿Los empleados y personas externas de la organización tienen restricciones para el acceso a la red?	X				La entidad tiene control al acceso a la red sobre personal externo. Esto por directiva gerencial es exclusiva del encargado de soporte tecnológico.			X	X
Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.	**9.2 Gestión de acceso de usuario.**										
	9.2.1 Gestión de altas/bajas en el registro de usuarios.	¿La organización cuenta con procedimientos formales cuando un empleado es dado de baja?	X				La entidad administra la información y acceso de acuerdo a las estipulaciones contractuales y durante el tiempo que el trabajador se encuentre activo en la organización.		X		X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	¿Existen procedimientos para verificar la asignación de derechos de acceso a usuarios?		X			Generar políticas sobre sistemas de información e infraestructura tecnológica.			X	X
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	¿La organización controla el acceso con privilegios especiales (administradores, usuarios root, entre otros) de los empleados?	X				Lo realiza mediante directriz gerencial, autorizando exclusivamente al personal de soporte tecnológico.			X	X
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	¿La organización corrobora la autenticidad de información confidencial?	X				La entidad mediante el Uso de Medios criptográficos verifica la información confidencial y que es solicitada por las entidades de control.	X		X	
	9.2.5 Revisión de los derechos de acceso de los usuarios.	¿Los empleados verifican el acceso de sus activos?	X				Lo realiza mediante directriz gerencial, autorizando exclusivamente al personal de soporte tecnológico.			X	X
	9.2.6 Retirada o adaptación de los derechos de acceso	¿La organización retira los accesos de empleados externos al terminar los contratos?	X				La entidad administra la información y acceso de acuerdo a las estipulaciones contractuales y durante el tiempo que el trabajador se encuentre activo en la organización.		X	X	
Hacer que los usuarios sean responsables de	**9.3 Responsabilidades del usuario.**										

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
la protección de la información para su identificación.	9.3.1 Uso de información confidencial para la autenticación.	¿La organización exige a los empleados la protección de la información confidencial?	X				La entidad formaliza los requisitos de protección y confidencialidad de la información en sus acuerdos contractuales.		X		X
Impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.	**9.4 Control de acceso a sistemas y aplicaciones.**										
	9.4.1 Restricción del acceso a la información.	¿La organización restringe el acceso a información confidencial de los empleados de mantenimiento?	X				La entidad formaliza los requisitos de protección y confidencialidad de la información en sus acuerdos contractuales.		X		X
	9.4.2 Procedimientos seguros de inicio de sesión.	¿La organización implementa procesos de inicio de sesión seguro a los sistemas?		X			Generar políticas sobre sistemas de información e infraestructura tecnológica.			X	X
	9.4.3 Gestión de contraseñas de usuario.	¿La organización cuenta con políticas para el manejo de contraseñas de calidad?		X			Generar políticas sobre sistemas de información e infraestructura tecnológica.			X	X
	9.4.4 Uso de herramientas de administración de sistemas.	¿La organización controla el uso de software no autorizado?		X			Generar políticas sobre sistemas de información e infraestructura tecnológica.			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	9.4.5 Control de acceso al código fuente de los programas.	¿La organización controla el acceso al código fuente de los sistemas?	X				En la entidad no se realiza desarrollo de software, por lo tanto el control no es aplicable.				
	10. CIFRADO.		**0**	**2**	**2**	**0**					
Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.	10.1 Controles criptográficos.										
	10.1.1 Política de uso de los controles criptográficos.	¿La organización cuenta con políticas para el uso de controles criptográficos?		X			Generar políticas sobre sistemas de información e infraestructura tecnológica.			X	X
	10.1.2 Gestión de claves.	¿La organización cuenta con políticas para el uso de claves criptográficas a través de su ciclo de vida?		X			Generar políticas sobre sistemas de información e infraestructura tecnológica.			X	X
	11. SEGURIDAD FÍSICA Y AMBIENTAL.		**8**	**7**	**15**	**53**					
Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de	**11.1 Áreas seguras.**										
	11.1.1 Perímetro de seguridad física.	¿La organización restringe el acceso a las instalaciones que manejan información crítica?	X				Actualmente, la información crítica solo es de conocimiento del gerente y el personal de soporte tecnológico.			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
procesamiento de la información.	11.1.2 Controles físicos de entrada.	¿Las entradas a los lugares prohibidos se encuentran con algún mecanismo de seguridad, por ejemplo biométricos?		X			Únicamente hay guardias y cerraduras de seguridad. No existe otro mecanismo tecnológico para su custodia y protección.			X	X
	11.1.3 Seguridad de oficinas, despachos y recursos.	¿Las oficinas, recintos e instalaciones cuentan con algún tipo de seguridad? Por ejemplo Vigilantes, cámaras?		X			Únicamente hay guardias y cerraduras de seguridad. No existe otro mecanismo tecnológico para su custodia y protección.			X	X
	11.1.4 Protección contra las amenazas externas y ambientales.	¿La organización cuenta con protecciones para desastres naturales?		X			Generar un plan de contingencia contra amenazas externas y ambientales			X	X
	11.1.5 El trabajo en áreas seguras.	¿La organización cuenta con áreas de trabajo seguras para sus empleados?	X				La entidad asegura las áreas de trabajo, las que son producto de la revisión y habilitación de la IPS por norma legal.	X		X	
	11.1.6 Áreas de acceso público, carga y descarga.	¿La organización cuenta con control en áreas de carga/descarga?	X				La entidad controla el ingreso y salida del personal.			X	X
Evitar la pérdida, los daños, el robo o el	**11.2 Seguridad de los equipos.**										

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
compromiso de activos y la interrupción a las operaciones de la organización..	11.2.1 Emplazamiento y protección de equipos.	¿La organización protege los equipos de amenazas y peligros ambientales así como de acceso no autorizado?	X				La entidad controla los equipos existentes mediante la vigilancia y observación, además cada trabajador debe custodiar el bien asignado.			X	X
	11.2.2 Instalaciones de suministro.	¿Los equipos de la organización están protegidos contra cortes de energías y fallos en los suministros básicos?		X			No se cuenta con UPS de Respaldo en caso de cortes de energía eléctrica.			X	X
	11.2.3 Seguridad del cableado.	¿Existe protección para el cableado por parte de la organización ?	X				La entidad controla el cableado estructurado que enlaza los diferente puntos de la red informática			X	X
	11.2.4 Mantenimiento de los equipos.	¿Los equipos de la organización reciben mantenimiento preventivo constante?		X			Se debe crear un plan de mantenimiento preventivo y correctivo de los equipos de la organización.			X	X
	11.2.5 Salida de activos fuera de las dependencias de la empresa.	¿La organización protege la salida de equipos, información y software de su lugar de trabajo?	X				La entidad controla los equipos que salen de la dependencia, mediante formatos que registran su trazabilidad.			X	X
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	¿Se aplica seguridad a los equipos que salen de las instalaciones, considerando los distintos riegos?		X			La entidad no hace uso de sus equipos externamente, por lo tanto este control no aplica.			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	¿La organización supervisa la reutilización o retirada de equipos?	X				La entidad realiza control sobre los dispositivos que necesiten ser retirados.			X	X
	11.2.8 Equipo informático de usuario desatendido.	¿La organización exige a los empleados verificar la seguridad de sus equipos de trabajo?	X				La entidad controla los equipos que no estén activos, existe un lugar para su custodia y protección.			X	X
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	¿En la organización se a adoptado una política de trabajo despejado y bloqueo de pantallas, para proteger la información?		X			Generar políticas sobre sistemas de información e infraestructura tecnológica.			X	X
	12. SEGURIDAD OPERATIVA.		**4**	**10**	**14**	**29**					
Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.	**12.1 Responsabilidades y procedimientos de operación.**										
	12.1.1 Documentación de procedimientos de operación.	¿La organización documenta todos los procedimientos operativos?		X			La entidad está en proceso de implementación de los procesos operativos			X	X
	12.1.2 Gestión de cambios.	¿La organización lleva un control de los cambios sobre los activos que alteran la seguridad de la información?		X			La entidad actualmente realiza el control mediante actas de entrega del activo.			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	12.1.3 Gestión de capacidades.	¿La organización garantiza el rendimiento adecuado en los sistemas?	X				La entidad cuenta con equipos informáticos que cumplen con las características necesarias para la operación de las actividades.			X	X
	12.1.4 Separación de entornos de desarrollo, prueba y producción.	¿la organización separa los entornos de desarrollo, pruebas y producción?	X				La entidad no tiene como objeto el desarrollo de software, por lo tanto no aplica este control.			X	X
Garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware.	**12.2 Protección contra código malicioso.**										
	12.2.1 Controles contra el código malicioso.	¿La organización controla la propagación de software malicioso, así como la recuperación en caso de ser infectado los equipos, además capacita a los usuarios en la prevención de estos?	X				La entidad cuenta con herramientas de protección gratuitas, que para mayor efectividad debería hacer uso de herramientas de detección y protección de mejor alcance y operación.			X	X
Alcanzar un grado de protección deseado contra la pérdida de datos	**12.3 Copias de seguridad.**										
	12.3.1 Copias de seguridad de la información.	¿La organización realiza copias de seguridad con sus respectivas pruebas regulares?	X				Se realiza copias de seguridad de las bases de datos de los aplicativos misionales			X	X
Registrar los eventos relacionados con la	**12.4 Registro de actividad y supervisión.**										

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
seguridad de la información y generar evidencias.	12.4.1 Registro y gestión de eventos de actividad.	¿La organización revisa constantemente los eventos log de fallos, excepciones, accesos?		X			Por intermedio de la oficina de soporte tecnológico, se realiza monitoreo esporádico cuando se presenta alguna actividad inusual.			X	X
	12.4.2 Protección de los registros de información.	¿La organización protege de alteración y accesos no autorizado, los registros de eventos?		X			No se realiza una protección de los registros de eventos, pero la persona encargada del soporte es el responsable.			X	X
	12.4.3 Registros de actividad del administrador y operador del sistema.	¿La organización protege los registros de los administradores y operadores de los sistemas realizando un revisión regular?		X			No se realiza una protección de los registros de eventos, pero la persona encargada del soporte es el responsable.			X	X
	12.4.4 Sincronización de relojes.	¿La organización sincroniza los relojes de los sistemas con una única fuente de referencia?		X			Teniendo en cuenta la baja complejidad de la entidad no es necesario este procedimiento.			X	X
Garantizar la integridad de los sistemas operacionales para la organización.	**12.5 Control del software en explotación.**										
	12.5.1 Instalación del software en sistemas en producción.	¿La organización implementa procesos para la instalación segura de software en sistemas en producción?		X			Se debe generar procesos que permitan garantizar instalaciones seguras dentro de los equipos.			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
Evitar la explotación de vulnerabilidades técnicas.	**12.6 Gestión de la vulnerabilidad técnica.**									X	X
	12.6.1 Gestión de las vulnerabilidades técnicas.	¿La organización gestiona las vulnerabilidades técnicas de los sistemas de manera oportuna?		X			La entidad debe asegura la protección de algunos de los eventos o vulnerabilidades que puedan generar riesgo para la entidad.			X	X
	12.6.2 Restricciones en la instalación de software.	¿La organización controla la instalación de software por parte de los empleados?		X			No existe control del software que puede ser instalado por los trabajadores de la entidad.			X	X
Minimizar el impacto de actividades de auditoría en los sistemas operacionales.	**12.7 Consideraciones de las auditorías de los sistemas de información.**										
	12.7.1 Controles de auditoría de los sistemas de información.	¿La organización realiza y planea auditoria regulares a los sistemas de operación?		X			La organización no realiza auditorias de sistemas y de información.			X	X
	13. SEGURIDAD EN LAS TELECOMUNICACIONES.		**3**	**4**	**7**	**43**					
Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.	**13.1 Gestión de la seguridad en las redes.**										
	13.1.1 Controles de red.	¿La organización controla y administra la red?	X				La entidad controla la red sin detalle mayor.			X	X
	13.1.2 Mecanismos de seguridad asociados a servicios en red.	¿La organización identifica los mecanismos de seguridad para los servicios de red?	X				La empresa controla la red de forma parcial, no se lleva un control de segmentación ni de monitoreo			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	13.1.3 Segregación de redes.	¿La organización segrega la red en funciona los empleados y servicios?		X			La entidad no segmenta la red, lo anterior teniendo en cuenta que es una IPS pequeña.			X	X
Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.	**13.2 Intercambio de información con partes externas.**										
	13.2.1 Políticas y procedimientos de intercambio de información.	¿La organización gestiona políticas para el intercambio de información?		X			Generar políticas sobre sistemas de información e infraestructura tecnológica.			X	X
	13.2.2 Acuerdos de intercambio.	La organización garantiza la transferencia de información entre las ¿entidades externas a ella?		X			La entidad realiza el control de transferencia y envió de información a entidades de control, mediante la utilización de medios criptográficos para proteger la integridad y veracidad de la información.			X	X
	13.2.3 Mensajería electrónica.	¿La organización tiene control sobre la mensajería electrónica e-mail?	X				La entidad utiliza mensajería gratuita, y no hay un control adecuado sobre este servicio.			X	X
	13.2.4 Acuerdos de confidencialidad y secreto.	¿La organización identifica, revisa y documenta las restricciones para que los empleados no divulguen información confidencial?		X			La entidad lo estable en los acuerdos contractuales.		X	X	X
	14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.		**4**	**9**	**13**	**31**					

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
Garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para aquellos que proporcionan servicios en redes públicas.	**14.1 Requisitos de seguridad de los sistemas de información.**										
	14.1.1 Análisis y especificación de los requisitos de seguridad.	¿La organización revisa requisitos de seguridad antiguos, para mejorar y obtener nuevos?		X			Debería La entidad y con propiedad la oficina de soporte tecnológico analizar eventos ocurridos por situaciones de riesgo para implementar mejoras a la seguridad.			X	X
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	¿La organización protege las comunicaciones y servicios tercerizados con redes públicas?		X			La entidad solo hace uso del servicio tercerizado - internet, pero no un control exclusivo.		X		X
	14.1.3 Protección de las transacciones por redes telemáticas.	¿La organización protege las transacciones en las redes, para evitar accesos no autorizados, divulgación y enrutamiento incorrecto?		X			La entidad solo hace uso del servicio tercerizado - internet, pero no un control exclusivo.		X		X
Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información.	**14.2 Seguridad en los procesos de desarrollo y soporte.**										
	14.2.1 Política de desarrollo seguro de software.	¿La organización tiene políticas para el desarrollo de sistemas seguros?		X			El objeto de la entidad no hace referencia al desarrollo de software			X	X
	14.2.2 Procedimientos de control de cambios en los sistemas.	¿La organización tiene control sobre los cambios en los sistemas?	X				La entidad controla el cambio del software que necesite su actualización.		X		X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	¿La organización revisa las aplicaciones críticas, posterior a cambios en el sistema?	X				La entidad verifica los cambios y actualizaciones realizadas al sistema.		X		X
	14.2.4 Restricciones a los cambios en los paquetes de software.	¿La organización verifica y controla los cambios en paquetes de software?	X				La entidad verifica los cambios y actualizaciones realizadas al sistema.		X		X
	14.2.5 Uso de principios de ingeniería en protección de sistemas.	¿Se aplican los principios de ingeniería para la protección de sistemas?		X			La entidad no hace uso de métodos de ingeniería inversa para la protección de los sistemas			X	X
	14.2.6 Seguridad en entornos de desarrollo.	¿La organización asegura los entornos de desarrollo de sistemas?		X			El objeto de la entidad no hace referencia al desarrollo de software			X	X
	14.2.7 Externalización del desarrollo de software.	¿La organización verifica y supervisa el desarrollo de sistemas externalizados?		X			El objeto de la entidad no hace referencia al desarrollo de software			X	X
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	¿La organización realiza pruebas constantes durante el desarrollo de sistemas?		X			El objeto de la entidad no hace referencia al desarrollo de software			X	X
	14.2.9 Pruebas de aceptación.	¿La organización realiza pruebas de aceptación una vez se termina un desarrollo?	X				El objeto de la entidad no hace referencia al desarrollo de software. Solo se realiza la verificación cuando hay compra de software u actualización.		X		X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
Garantizar la protección de los datos que se utilizan para procesos de pruebas.	**14.3 Datos de prueba.**										
	14.3.1 Protección de los datos utilizados en pruebas.	¿La organización protege los datos usados durante las pruebas de los desarrollas de sistemas?		X			La entidad realiza el control al momento de realizar las pruebas en los sistemas desarrollados.		X		X
	15. RELACIONES CON SUMINISTRADORES.		**4**	**1**	**5**	**80**					
Garantizar la protección de los activos de la organización que son accesibles a proveedores.	**15.1 Seguridad de la información en las relaciones con suministradores.**										
	15.1.1 Política de seguridad de la información para suministradores.	¿Se lleva un control de acceso a la información para terceros?	X				Generar políticas sobre sistemas de información e infraestructura tecnológica.		X		X
	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	¿la organización cuenta con un pan de tratamiento para los servicios contratados a terceros?		X			La entidad no cuenta con un plan de tratamiento de riesgos para los servicios que contrata			X	X
	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	¿La organización exige garantías de seguridad al momento de contratar o comprar suministros de terceros?	X				La entidad realiza las exigencia a los terceros en los acuerdos contractuales que se establezcan		X		X
Mantener el nivel en la prestación de servicios conforme a los acuerdos con el proveedor en materia	**15.2 Gestión de la prestación del servicio por suministradores.**										
	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	¿La organización verifica regularmente los	X				La entidad verifica las aplicaciones o software suministrado por tercero,		X		X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
de seguridad de información.		servicios contratados a terceros?					especialmente las actualizaciones.				
	15.2.2 Gestión de cambios en los servicios prestados por terceros.	¿La organización supervisa los cambios de términos y uso de servicios a terceros'	X				La entidad controla las aplicaciones o software suministrado por tercero, especialmente las actualizaciones.		X		X
	16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.		**2**	**5**	**7**	**29**					
Garantizar una administración de incidentes de seguridad de la información coherente y eficaz en base a un enfoque de comunicación de los eventos y las debilidades de seguridad.	**16.1 Gestión de incidentes de seguridad de la información y mejoras.**										
	16.1.1 Responsabilidades y procedimientos.	¿En la organización se maneja un protocolo de respuesta rápida al momento de sucesos que relacionan la seguridad de la información?		X			La entidad no cuenta con un plan de contingencia y continuidad del negocio			X	X
	16.1.2 Notificación de los eventos de seguridad de la información.	¿En la organización se notifica los eventos de seguridad, mediante los canales de administración?		X			La entidad no cuenta con un plan de contingencia y continuidad del negocio			X	X
	16.1.3 Notificación de puntos débiles de la seguridad.	¿Se notifica debilidades sospechosas que involucran la seguridad de la información		X			La oficina de soporte tecnológico comunica al gerente las posibles sospechas que pueden involucrar la seguridad de la información.			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	¿Se realiza una valoración de los eventos que involucran la seguridad de la información?		X			La entidad no cuenta con un plan de contingencia y continuidad del negocio			X	X
	16.1.5 Respuesta a los incidentes de seguridad.	¿Se da respuesta a los incidentes presentados de seguridad de la información?	X				Por intermedio de la oficina de soporte tecnológico se comunica el incidente de seguridad a la alta dirección para su gestión			X	X
	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	¿Se hace uso del conocimiento obtenido en la solución de un incidente de seguridad de la información, para reducir la probabilidad e impacto?	X				Por intermedio de la oficina de soporte tecnológico se da trámite y gestión al incidente de seguridad ocurrido, y con base de sucesos similares ocurridos.			X	X
	16.1.7 Recopilación de evidencias.	¿Se realiza un procedimiento adecuado para recopilar evidencia de incidentes con el fin de preservar la información?		X			La entidad no lleva un control de la información que puede servir como evidencia en un caso de incidente.			X	X
	17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.		**1**	**3**	**4**	**25**					
Mantener la seguridad de la información integrada en los	**17.1 Continuidad de la seguridad de la información.**										

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
sistemas de gestión de continuidad del negocio de la organización.	17.1.1 Planificación de la continuidad de la seguridad de la información.	¿La empresa tiene determinado los requisitos para dar continuidad de la seguridad informática en un momento de situaciones adversas?		X			La entidad no cuenta con un plan de contingencia y continuidad del negocio			X	X
	17.1.2 Implantación de la continuidad de la seguridad de la información.	¿La empresa tiene implementado y documentado, tanto los procesos como procedimientos y controles de la seguridad de la información?		X			La entidad no cuenta con controles de continuidad de la información			X	X
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	¿La empresa verifica, revisa y evalúa los controles de continuidad de la información?		X			La entidad no cuenta con controles de continuidad de la información			X	X
Garantizar la disponibilidad de las instalaciones de procesamiento de información.	**17.2 Redundancias.**										
	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	¿La organización garantiza el procesamiento y disponibilidad de la información?	X				La entidad garantiza el procesamiento de información a pesar de no tener plan de continuidad de la información			X	X
	18. CUMPLIMIENTO.		**1**	**7**	**8**	**13**					

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
Evitar incumplimientos a requisitos relacionados con la seguridad de la información de cualquier tipo especialmente a las obligaciones legales, estatutarias, normativas o contractuales.	**18.1 Cumplimiento de los requisitos legales y contractuales.**										
	18.1.1 Identificación de la legislación aplicable.	¿La organización garantiza los requisitos estatutarios para los sistemas de información?		X			El objeto de la entidad no hace referencia al desarrollo de software. Solo se realiza la verificación cuando hay compra de software u actualización.	X			X
	18.1.2 Derechos de propiedad intelectual (DPI).	¿En la organización se garantiza el cumplimiento de derechos de propiedad intelectual?	X				La entidad por ser controlada públicamente, necesariamente hace uso exclusivo de software licenciado	X			X
	18.1.3 Protección de los registros de la organización.	¿Cada uno de los registros que se realizan en la organización está debidamente protegidos contra perdida, falsificación, acceso, destrucción y publicación?		X			La entidad no cuenta con procedimientos que permitan proteger y administrar de manera adecuada la información, con base en la normatividad que los regula.			X	X
	18.1.4 Protección de datos y privacidad de la información personal.	¿Se realiza un proceso de protección de datos y privacidad de la información personal?		X			La entidad tiene en cuenta la normatividad que a esta la regula.	X			X
	18.1.5 Regulación de los controles criptográficos.	¿En la organización se utiliza controles de cifrado de la información?		X			La entidad utiliza métodos criptográficos en los casos de envió de información hacia las entidades externas.			X	X

Objetivo de Control	Dominio	Pregunta Existencia Control	SI	NO	Numero Controles	Nivel Cumplimiento (%)	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones Selección Control			
								L	C	N	R
Garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos organizacionales.	**18.2 Revisiones de la seguridad de la información.**										
	18.2.1 Revisión independiente de la seguridad de la información.	¿Se realiza un revisión independiente de la seguridad de la información?		X			La entidad no ha realizado auditorias de sistemas que permitan identificar no conformidades en el sistema de información.			X	X
	18.2.2 Cumplimiento de las políticas y normas de seguridad.	¿Se revisa por parte del gerente el cumplimiento de las políticas y normas de seguridad?		X			Las políticas enfocadas a la seguridad de información aún se encuentran en proceso de desarrollo.			X	X
	18.2.3 Comprobación del cumplimiento.	¿El sistema de información se revisa regularmente para verificar su cumplimiento?		X			La entidad no ha realizado auditorias de sistemas que permitan identificar no conformidades en el sistema de información y además verificar la eficacia del cumplimiento			X	X

Fuente: El Autor.

RESUMEN ANÁLITICO ESPECIALIZADO - RAE	
1. INFORMACION GENERAL	
Tema	Gestión de riesgos en los sistemas de información de la IPS Solidarios del municipio de Cuaspud Carlosama.
Titulo	Realizar el análisis para gestión de riesgos en los sistemas de información de la IPS Solidarios Salud del municipio de Cuaspud Carlosama a partir de la norma ISO 27001 aplicando la metodología Magerit.
Autor(es)	Fabio Adalberto Arellano Montenegro
Director	Ing. Martin Camilo Cancelado Ruiz
Fuente Bibliográfica	Se referencian las bibliografías que refieren los temas principales del proyecto: Ministerio de Hacienda y Administraciones públicas, MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, octubre 2012. {En línea}. {Consultado Marzo 2017}. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WNxY_G81_IU **AMAYA**, Camilo. "MAGERIT: metodología práctica para gestionar riesgos". {En línea}. {Consultado Marzo 2017}. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/ SGSI-Blog especializado en Sistemas de Gestión de Seguridad de la Información. "ISO 27001: El método MAGERIT". {En línea}. {Consultado Marzo 2017}. Disponible en: http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/ EAR. EAR/PILAR-documentación Magerit. {En línea}. {Consultado Marzo 2017}. Disponible en: http://www.ar-tools.com/magerit/index.html Dirección de Estándares y Arquitectura de TI del Ministerio de las Tecnologías de Información y las Comunicaciones de la República de Colombia. (2014). Generalidades del Marco de Referencia – versión 1.0. {En línea}. {Consultado Marzo 2017}. Disponible en: http://www.mintic.gov.co/marcodereferencia/624/articles-8102_generalidades.pdf Ley 1273 de 2009. Delitos informáticos en Colombia. {En línea}. {Consultado Marzo 2017}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html Ministerio de la Tecnologías de Información y Comunicación-Tic. Ley 1341 de 2009. Principios y conceptos sobre la sociedad de la

	información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-. {En línea}. {Consultado Marzo 2017}. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3707.html Gobierno de España. Agencia Estatal Boletín Oficial del Estado. {Consultado Marzo 2017}. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-9741 BOCANEGRA, Yamilet. Análisis y Gestión de Riesgos de los Sistemas de Información de la Alcaldía Municipal de Tuluá aplicando la metodología MAGERIT. {En línea}. {Consultado Marzo 2017}. Disponible en: http://repository.unad.edu.co/handle/10596/3632. IPS SOLIDARIOS SALUD. Portafolio de Servicios. {Consultado Marzo 2017}. 2008
Año	2018
Resumen	El proyecto de investigación tratará aspectos relativos a la IPS Solidarios Salud del municipio de Cuaspud Carlosama, como es, la reseña histórica, el tipo de entidad dentro del sector salud y la formalización de la plataforma estratégica, además, se tratará los conceptos referentes de la Metodología MAGERIT v 3.0, como es la identificación de activos, su valoración, determinación de vulnerabilidades, amenazas y el impacto que causarían en los activos si llegaran a materializar el riesgo. También, se efectuará el análisis e identificación de los riesgos como aporte central del presente proyecto, determinando el plan de tratamiento de riesgos, la evaluación de los controles de la norma ISO 27001 y 27002, y se culminará el trabajo con la Gestión de Riesgos.
Palabras Claves	Activos, vulnerabilidades, amenazas, impacto, riesgo, Magerit, ISO 27001, ISO 27002, IPS, Seguridad Información, disponibilidad, confidencialidad, integridad, gestión del riesgo, controles, declaración de aplicabilidad, políticas de seguridad,
Contenidos	Descripción del problema Planteamiento del problema Formulación del problema Objetivos Objetivo general Objetivos específicos Justificación Alcance y delimitación del proyecto Metodología Marco referencial Marco de antecedentes Marco contextual Marco conceptual

	Marco teórico Marco legal Producto resultado a entregar Recursos necesarios para el desarrollo Recursos humanos Recursos tecnológicos Recursos materiales Recursos financieros o presupuesto Desarrollo del proyecto Conclusiones

2. DESCRIPCION DEL PROBLEMA DE INVESTIGRACION

La IPS Solidarios es una institución que presta servicios de salud a la población de Cuaspud Carlosama, enfocando su quehacer en la recuperación de pacientes, a través de terapias proporcionadas en localidad. La IPS Solidarios cuenta con una red de computadoras e informática, que permite realizar sus actividades operativas y de administración, como es el caso de la facturación, generación de RIPS y presentación de informes a las diferentes entidades públicas, privadas y Entes de Control. De esta manera, ésta red de datos, se convierte en el medio indispensable y relevante para la realización, procesamiento y gestión de las actividades diarias que la institución oferta.

Desafortunadamente, la IPS Solidarios, carece de una debida protección y administración de sus recursos informáticos, el fácil acceso a sus equipos computacionales, pueden convertirlos en sistemas informáticos vulnerables por no contar con los debidos controles. También, el acceso no restringido de internet al personal de la institución, puede convertirse en un medio visible a posibles atacantes, generando consecuencias catastróficas como el robo de información, secuestro o encriptación por ransomware, e incluso su perdida.

De esta manera, se pretende como tema de investigación considerar la aplicación de la Metodología MAGERIT, para realizar un estudio del análisis y gestión de riesgos en los sistemas de información de la IPS Solidarios Salud del municipio de Cuaspud Carlosama. Cabe resaltar que por el momento no existe una valoración de los activos en la institución, de igual manera no se ha identificado las amenazas a que está expuesta, y no se cuenta con un documento o política institucional que tenga en cuenta la protección de la información y su custodia. Además el desconocimiento de como salvaguardar la información que se procesa en la institución por parte del personal que ahí labora.

3. OBJETIVOS

Objetivo general

Realizar el análisis para gestión de riesgos en los sistemas de información de la IPS Solidarios Salud del municipio de Cuaspud Carlosama a partir de la norma ISO 27001 aplicando la Metodología MAGERIT.

Objetivos específicos

-Describir la institución objeto de estudio para determinar sus antecedentes, plataforma estratégica, portafolio de servicios y activos.
-Aplicar la metodología MAGERIT para el análisis de los riesgos, identificando los activos, las amenazas, vulnerabilidades, controles, impacto y riesgo.
-Aplicar la metodología MAGERIT para la gestión de riesgos estableciendo la interpretación de los valores de impacto y riesgo.
-Verificar los controles existentes en la norma ISO 27002 que mejor se adecuen a la IPS Solidarios Salud.

4. METODOLOGIA

Las actividades requeridas para el proceso de análisis y gestión de riesgos de la IPS Solidarios Salud, van a estar definidas por la metodología de gestión de riesgos MAGERIT, y son las siguientes:

a) Actividades preliminares
   - ✓ Visita y reconocimiento de la empresa
   - ✓ Identificar la información y procesos de la empresa
   - ✓ Entrevistas directas a socios y gerente
   - ✓ Entrevistas al personal.

b) Análisis de riesgos
   - ✓ Realizar el inventario de activos de información
   - ✓ Identificar y valorar las amenazas a las que están expuesta los activos.
   - ✓ Determinación del impacto potencial
   - ✓ Determinación del riesgo potencial
   - ✓ Estimar el estado del riesgo.
   - ✓ Gestión del Riesgo.
   - ✓ Determinar los controles según ISO 27001 y 27002

5. REFERENTES TEORICOS

Para el desarrollo de éste proyecto se consultaron diferentes fuentes que centran su investigación en temas relacionados con el análisis e identificación de riesgos informáticos a través de la metodología Magerit y las normas ISO 27001, 27002, en instituciones de salud, entidades territoriales y centros educativos entre otros.

6. REFERENTES CONCEPTUALES

Se presenta temas y definiciones que ayudan a conceptualizar y referenciar las etapas desde el reconocimiento de la organización, como la misión, visión el tipo de entidad en el sector y su localización; también, lo correspondiente al análisis e identificación de riesgos, como, los conceptos para la aplicación de la metodología Magerit y la verificación de controles según la norma ISO 27001 y 27002.

7. RESULTADOS

Realizada la correspondiente evaluación de los activos de la IPS Solidarios, la identificación de vulnerabilidades, la valoración de las amenazas, la determinación del impacto y los riegos a que está expuesta la institución, como parte fundamental del análisis de riesgos que conlleva la metodología Magerit, se pretende dar a conocer a la IPS Solidarios, el plan de tratamiento de riesgos, la identificación de los controles según la ISO 27001, el nivel de madurez en que se encuentra el sistema de información de la entidad y la generación de políticas de seguridad y procedimientos para su implementación para materializar las decisiones adoptadas para el tratamiento de los riesgos.

8. CONCLUSIONES

-La IPS Solidarios Salud no cuenta con un proceso metodológico para el análisis y tratamiento de riesgos en seguridad informática, siendo el presente proyecto aplicado un apoyo para la identificación de posibles riesgos y su gestión.

-Con la identificación y el tratamiento que se den a los riesgos, fortalecerá la seguridad de la información de la IPS Solidarios.

-La utilización de la metodología Magerit, contribuye a identificar de manera estructurada las dificultades existentes por la escasa seguridad informática de la entidad.

-Se constató la ausencia de capacitaciones al personal de la IPS Solidarios en seguridad y protección de la información, siendo el recurso humano el medio más vulnerable en temas de seguridad.

-El proceso desarrollado en las diferentes fases de identificación de riesgos ha despertado mayor interés en la gerencia de la IPS Solidarios por propender al mejoramiento de la seguridad de la información y la protección de los datos en esta entidad.