DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (SGSI) EN LA INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD CENTRO DE TERAPIAS INTEGRALES MISALUD S.A.S.

HARRY MÁRQUEZ LEAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2020

DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (SGSI) EN LA INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD CENTRO DE TERAPIAS INTEGRALES MISALUD S.A.S.

HARRY MÁRQUEZ LEAL

Proyecto de grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA.

CHRISTIAN REYNALDO ANGULO RIVERA
Director del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2020

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedico este proyecto a mi madre Olga Rosa Leal Serpa mi gran apoyo para conseguir mis sueños a lo largo de mi vida, a mi Esposa Lucia Estrada Coronado mi gran apoyo incondicional y a mis Hijos Juan Pablo Márquez Estrada y Noah José Márquez Estrada las personas que hacen especial mi vida.

AGRADECIMIENTOS

A Dios todo poderoso, mi familia que siempre encontré apoyo en ellos durante mi proceso de formación académica y las largas jornadas nocturnas que se tuvieron que aguantar, y sobre todo los buenos momentos que hemos pasado juntos.

Estoy muy agradecido con la UNAD a los Ingenieros Juan José Cruz, Christian Reynaldo Angulo Rivera y Luis Fernando Zambrano Hernández, por servir todos sus conocimientos para esta formación académica y progresar como profesional.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

Este proyecto aplicado permite conocer el contexto de la empresa Centro de Terapias Integrales Misalud S.A.S., en sus proceso y áreas con el objetivo de diseñar un SGSI que apoye en un futuro los distintos procesos y actividades allí efectuados, minimizando los riesgos de la información y controlar las vulnerabilidades que puedan estar presentes en el sistema de información, mediante el uso de políticas de seguridad documentados y que sean actualizados constantemente.

El diseño de un SGSI en la empresa Centro de Terapias Integrales Misalud S.A.S. involucra una labor de responsabilidad por parte de la alta gerencia, ya que son ellos los encargados de aprobar y suministrar los recursos precisos para desarrollar mejoras futuras.

El desarrollo del proyecto se basó en ISO 27001:2013 la cual establece los métodos adecuados y una despejada tesis de compromisos basada en una sucesión de procedimientos, instrucciones e implementación que deben constituir como se documenta la información. La metodología utilizada fue MAGERIT, esta metodología permite lograr un mejor nivel de calidad administrativa y procesos de mejora continua.

PALABRAS CLAVES: Diseño de SGSI, PHVA, MAGERIT, políticas, amenazas, activos, seguridad de la información.

ABSTRACT

This applied project allows knowing the context of the company Integral Therapies Center Misalud SAS, in its different areas and processes with the objective of designing an ISMS that supports in the future the different processes and activities carried out there, minimizing the risks of the information and control the threats that may be present in the computer system, through the use of documented security policies that are constantly updated.

The design of an ISMS in the company Centro de Terapias Integrales Misalud S.A.S. It involves a responsibility task on the part of the top management, since they are in charge of approving and providing the precise resources for the development and its future improvement.

The development of the project was based on ISO 27001: 2013, which establishes the appropriate methods and a clear thesis of commitments based on a succession of procedure, instructions and implementation that should constitute how the information is documented. The methodology used was MAGERIT, this methodology allows to achieve a better level of administrative quality and continuous improvement processes.

KEYWORDS: Design of ISMS, PHVA, MAGERIT, policies, threats, assets, information security.

INTRODUCCIÓN

Actualmente en el sector salud se maneja mucha información confidencial, lo cual nos lleva a que este sector debe buscar preservar la confidencial, integridad y disponibilidad de la información. Las instituciones prestadoras de salud son blancos fáciles para los Hackers porque poseen muchas vulnerabilidades, dichas vulnerabilidades o amenazas deben ser evaluadas y detectadas para así poder evitar la afectación del negocio.

Diseñar un SGSI a las empresas del sector salud debe relacionarse con los objetivos actuales que necesita la empresa, para garantizar los tres pilares de la seguridad de la información.

El Centro de Terapias Integrales Misalud S.A.S. es una empresa que pertenece al sector salud, entre sus servicios esta: prestar a los pacientes fisioterapia, terapia ocupacional, psicología y fonoaudiología, como manejan muchos pacientes poseen historias Clínicas con datos importantes.

El Centro de Terapias Integrales Misalud S.A.S. no se encuentra certificado en ningún sistema de gestión, la política de seguridad que posee es copia de otra y su departamento de TI está desorganizado.

Como prestador de servicios de salud, la IPS se encarga de recibir usuarios de las diferentes EPS con las que tiene un convenido, ingresando en el sistema las autorizaciones respectivas, con las que se dan apertura a las historias clínicas y de esta forma iniciar la atención de los pacientes. Todo es proceso se debe cumplir garantizando los pilares de la seguridad de la información, con el fin de certificar a las EPS y a los usuarios que su información se encuentra bien protegida.

Como se ha dicho anteriormente en la IPS existen muchos procesos que no tienen las mínimas medidas o controles de seguridad y estos deberían estar implementados en las áreas más fundamentales de la IPS, es por esto que para el diseño del SGSI del Centro de Terapias Integrales Misalud S.A.S., se implementaron algunos controles y requerimientos de la Norma Técnica Colombiana ISO 27001:2013.

1. TITULO

DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (SGSI) EN LA INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD CENTRO DE TERAPIAS INTEGRALES MISALUD S.A.S.

AREA DEL CONOCIMIENTO: Seguridad Informática.

LINEA DE INVESTIGACIÓN: Sistema de Gestión de Seguridad Informática

TEMA PROBLEMÁTICA: La institución prestadora de servicios de salud con nombre Centro de Terapias Integrales Misalud S.A.S. posee pocas políticas de seguridad de las cuales no existen controles sobre ellas los procesos internos para salvaguardar los datos son escasos o nulos y el plan de acción no está documentado, no existe un plan de capacitación a los empleados para comprender que los activos son de suma importancia.

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

En la IPS Centro de Terapias Integrales Misalud S.A.S. posee pocas políticas y no se ejercen los controles efectivos sobre la información en la organización.

¿Cuál es la información más valiosa que manejamos?

- La información asociada a nuestros clientes
- La información asociada a nuestros servicios
- La información asociada a nuestros empleados y colaboradores
- La información asociada a nuestros pacientes
- La información asociada a nuestras operaciones

¿Qué amenazas y vulnerabilidades pueden existir en la organización?

- La organización necesita y es necesario tener las políticas de seguridad para implementar los controles y así poder tomar decisiones para mejorar los controles.
- La información se tiene que proteger para evitar daños o pérdidas de la información y capacitar o evaluar el personal contestemente para que tenga conocimiento de los activos informáticos de la Empresa.

Con un SGSI, las empresas pueden conocer las inseguridades de sus activos e información, permitiéndoles organizar un plan para minimizarlos y controlarlos por medio de una excelente gestión que cumpla con los requisitos normativos existentes, los cuales se actualizarán periódicamente. A través del SGSI se proporciona una serie de actividades como: políticas, procedimientos, directrices todo esto en conjunto son necesarios para mejorar la seguridad y proteger sus activos esenciales. El alcance de un SGSI resalta la ubicación de los activos más críticos de la organización, como también los riesgos internos y externos asociados, por lo tanto, un SGSI ayuda a solucionar problemas técnicos de seguridad, tanto legales como en la organización, analizando los riesgos, aumentando la mejora de la información dentro de la organización y con este se garantiza la continuidad del negocio. [1]

[1] NUÑEZ ALAVAREZ Yenny Stella, diseño de un sgsi para el área de automatización del proceso de báscula, de la empresa minera sanoha ltda ubicada en nobsa –Boyacá. {En Línea}, {2015} disponible en http://repository.unad.edu.co:8080/bitstream/10596/3649/1/23810642.pdf

2.2 FORMULACIÓN DEL PROBLEMA

¿De qué manera se puede salvaguardar la información de una forma efectiva y que permita proteger los datos sensibles de los pacientes en la IPS Centro de Terapias Integrales MISALUD S.A.S.?

2.3 DESCRIPCIÓN DEL PROBLEMA

La IPS Centro de Terapias Integrales MISALUD S.A.S es una entidad privada que se encargar de atender pacientes de las diferentes EPS del Departamento del Atlántico, en la actualidad el volumen de información es muy alto, la Base de Datos contiene alrededor 10.000 datos de pacientes y en cada registro se almacenan datos sensibles.

La IPS Centro de Terapias Integrales MISALUD S.A.S actualmente cuenta con 4 oficinas y 8 computadores o estaciones de trabajo, acopladas sobre una red local e inalámbrica. La información de los pacientes, informes y bases de datos se acceden, consultan y modifican desde los equipos de cómputo de cada uno de los empleados de la IPS y es importante destacar que todos tienen habilitados privilegios administrativos, debido a que desde el servidor principal no se han establecido unas políticas que permitan instaurar bloqueos para acceder a herramientas administrativas en los equipos, al igual que se permite el uso de memorias USB, grabar archivo en CDs y acceder a páginas de uso común como: Facebook, YouTube, entre otras, sin ninguna restricción. Esto podría ocasionar diferentes vulnerabilidades que ponen en riesgo la información confidencial de los pacientes.

Debido a lo anterior, es importante que la empresa realice una inversión que permita realizar un SGSI y destine algunos recursos para garantizar la seguridad de la información en los datos que almacena. Para esto, se debe contar con un inventario de toda la información que maneja la organización, así como, las necesidades de seguridad de acuerdo con su actividad primaria y campo de acción, verificando en todo momento las normatividades a las que pueda estar sujeta su actividad. Con esto podemos contrarrestar las vulnerabilidades y amenazas que están presentes dentro del entorno de la organización. [2]

El SGSI debe contar con el protocolo necesario en el cual se va a justificar las

[2] AGUIRRE, Juan, ARISTIZABAL Catalina, diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda. {En Línea}, {2013} disponible en http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

decisiones de la alta gerencia, las acciones, así como políticas que se van a ejecutar y en la cual se demostrara que dichos controles que se seleccionaron han sido resultados de las disposiciones y análisis de vulnerabilidades. Lo que significa, que debemos llevar una trazabilidad y seguimiento de las políticas y objetivos hasta la implementación de este.

3. JUSTIFICACIÓN

El proyecto representa el progreso del diseño de un SGSI, para el Centro de Terapias Integrales MISALUD S.A.S con sede principal en la ciudad de Barranquilla se puede estructurar en 9 grandes bloques, que alcanzan una serie de etapas y acciones.

Las actividades principales para crear un SGSI según la ISO/IEC 27001:2013 son:

- Definir objetivos, políticas de seguridad y eficacia del SGSI.
- Implementación del MSPI (Herramienta realizada para identificar los niveles de madurez durante la implementación del MSPI).
- Realizar la relación de activos.
- Desarrollar el estudio de riesgos.
- Seleccionar de acuerdo con los objetivos de la Entidad las políticas de seguridad que se debe de implementar.
- Evaluar los riesgos residuales.
- Documentar los procedimientos necesarios para implementar las medidas seleccionadas.
- Implementación de los controles y los procedimientos.
- Formar y concienciar al personal.
- Ejecutar la auditoría interna y la revisión del SGSI por la Gerencia.

La norma ISO/IEC 27001:2013 nos indica que en un SGSI no es necesario poseer un manual de seguridad como si lo muestran otras normas de proceso y gestión, en las cuales se hace referencia a la necesidad de contar con un manual de gestión. Pero, la norma ISO/IEC 27001:2013 enseña y es muy precisa que toda información debe de estar documentada. Entonces, el SGSI estará conformado por una serie de documentos que mínimo son los siguientes:[3]

- Realizar las políticas de seguridad de la información.
- Desarrollar un inventario de activos de la información.
- Realizar un estudio de riesgos.
- Gestión de riesgos.
- Socializar los documentos de aplicabilidad.
- Instrucciones para implementar los controles.
- Instrucciones para la gestión del SGSI.

[3] Fuente: Sin autor. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html

Desarrollando la Metodología es de suma importancia el MSPI (Herramienta realizada para identificar los niveles de madurez durante la implementación del MSPI) tiene series de guías en donde nos dan instrucciones a la entidad de elaborar los documentos, en los cuales serán de mucha ayuda ya que con esto se cumplirá los solicitado de cada una de las fases del modelo, con estos resultados se analizará y posteriormente se desarrollarán de una mejor manera.

El MSPI nos ayudara en la implementación del SGSI, donde se debe tener claro los objetivos y sus necesidades, mirar la seguridad de sus de todos sus procesos, tipo y tamaño de la empresa, esto sirve para garantizar, la confidencialidad, integridad y disponibilidad de la información que son los tres principios pilares de la seguridad de información, esto con el fin de certificar el buen uso y datos privados.

Implementado el MSPI dentro de la organización sirve para favorecer el aumento de la gestión pública mediante la transparencia, esto promueve mejores prácticas de los activos de seguridad información con base a esta implementación.[4]

MINTIC nos indica que la seguridad de información es muy importante en la organización por eso nos brinda el MSPI basado en las buenas prácticas de la NTC-ISO 27001:2013, cuyo propósito es servir como guía para la mejora de los estándares de Seguridad de la Información de las organizaciones.

Como trabajador del sector salud he vivido en carne propia ataques informáticos dentro de la organización, esto con el paso de los años ha ido en aumento específicamente en este sector, estos ataques pueden ser tanto externos como internos. Los riesgos de sufrir ataques por personal de la organización son muy altos debido a la falta de protocolos estos ataques pueden ser voluntaria o involuntariamente también se pueden presentar eventos adversos, catastróficos o fallas técnicas.[5]

Por todo lo ilustrado anteriormente dentro de la organización es importante diseñar un SGSI bajo la norma ISO/IEC 27001:2013 ya que esta ayuda potencialmente reducir riesgos la perdida de datos sensibles, y sirve para descubrir vulnerabilidades del sistema y cómo reaccionar cuando se presenta un ataque.

---

[4] MINISTERIO DE COMUNICACIONES. Sistemas de Gestión de la Seguridad de la Información (SGSI) disponible en http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

[5] MINISTERIO DE COMUNICACIONES. informe final –modelo de seguridad de la información – sistema sansi – sgsi -modelo de seguridad de la información para la estrategia de gobierno en línea Versión 3, 26 diciembre 2008 disponible en http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un SGSI que permita minimizar los riesgos y amenazas de las diferentes áreas del Centro de Terapias Integrales MISALUD S.A.S, teniendo como base ISO 27001:2013 y en futuro lograr su implementación.

4.2 OBJETIVO ESPECÍFICOS

- Describir las complicaciones vitales de seguridad que presenta la organización en su departamento TI.

- Determinar las vulnerabilidades existentes en el Centro de Terapias Integrales MISALUD S.A.S, referentes al manejo de la información.

- Verificar si el Centro de Terapias Integrales MISALUD S.A.S. posee políticas o manuales de seguridad de la información, si es así realizar estudio sobre dichos manuales y si es su caso actualizar y/o crearlas.

- Proponer un SGSI para el área TI del Centro de Terapias Integrales MISALUD S.A.S, que garantice los tres pilares de la información que son confidencialidad, integridad y disponibilidad.

5. MARCOS DE REFERENCIA

5.1 MARCO TEÓRICO

5.1.1. Definición de un SGSI

Hay muchas definiciones de lo que es un Sistema de Gestión de Seguridad de la Información (SGSI), pero se va a mencionar la que contempla la ISO/IEC 27001, que hace referencia a la base de un sistema general de gestión, donde se concentra en el riesgo de las organizaciones, en la cual se crea, implementa, se hace operaciones, se vigila, revisa periódicamente, se mantiene y se perfecciona la seguridad de la información. Todo esto dicho anteriormente significa para la organización deja de operar intuitivamente y se empieza a tomar del control sobre lo que sucede alrededor de los sistemas de información y la información que maneja la organización. Esto permite revisar la estructura de la organización y mirar puntos débiles para mejorar. (ver Figura 1).

En los sistemas de gestión, el SGSI se implementa y con ellos se obtiene políticas, planificación, responsabilidades, mejores prácticas, procedimientos, procesos y recursos. Todo esto siempre va a estar documentado así lo define las normas ISO, así se formaliza normas y procedimientos y son más fáciles de explicar y transmitir, ya que pasar una información verbal no siempre es confiable. (ver Figura 2).

Se tiene que garantizar que toda la información sea segura y tramitada exitosamente, haciendo un proceso documentado y sistematizarlo. Esto debe ser conocido por toda la organización, basándose de un riesgo organizacional. Todo esto compone un SGSI.

Figura 1: Seguridad de la Información

Fuente: Sin autor. Figura 1 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html

Figura 2: Procesamiento de la Información

Fuente: Sin autor. Figura 2 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html

5.1.2 Para qué sirve un SGSI

El motivo verdadero para lo que sirve un SGSI para una organización son sus activos. Los tres pilares fundamentales confidencialidad, integridad y disponibilidad de la información que contiene datos sensibles que son esenciales para conservar la competitividad, ser rentables, legales y tener una imagen empresarial esenciales para los objetivos de la organización y aumentar sus ingresos económicos.

Una de cada 4 empresas está expuestos a millones de amenaza, no existe sistema seguro, pero si existe proteger de la mejor manera esos sistemas de información, para que sus activos estén protegidos y reducir las distintas formas de amenazas. (ver Figura 3).

La normatividad, el miedo al cambio y adaptarse de la mejor manera a las condiciones del sector, preservar y efectuar los objetivos de la organización para nuevos caminos de negocio, lo dicho anteriormente es muy fundamental para una organización y un SGSI es la mejor herramienta para la gestión del riesgo de la organización. El nivel que se tiene que alcanzar en materia de seguridad debe ser óptimo, la alta gerencia se debe de comprometer con los objetivos incluyendo a sus clientes y proveedores. La implementación de la seguridad debe ser planificada, con procedimientos e implementar controles de seguridad, no olvidando la evaluación de riesgos y el control de la eficiencia de estos.

Figura 3:Cuadro de Riesgos

Fuente: Sin autor. Figura 3 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html

5.1.3 Que incluye un SGSI

La norma ISO 9001 en sus versiones, se muestran la documentación en forma de pirámide de cuatro niveles (ver Figura 4). Existe el anexo SL en la cual nos ayuda para que todas las normas ISO tenga la misma estructura, dicho esto podemos trasladar el modelo a un SGSI basado en la ISO 27001. Dichos niveles se explican a continuación.

Figura 4: Que incluye un SGSI

Fuente: Sin autor. Figura 4 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html

Documentos de Nivel 1: Manual de seguridad: el documento más importante ya que es el que dirige todo el sistema de un SGIS, en él se encontrara políticas y directrices, objetivos y alcances, e intenciones y responsabilidades.

Documentos de Nivel 2: Procedimientos: documentos netamente operativos, aquí comprobamos que se desarrollen de la mejor forma la planificación, control y operación de la seguridad de la información.

Documentos de Nivel 3: Instrucciones, checklists y formularios: aquí vemos como se describen las actividades relacionadas con la seguridad de la información.

Documentos de Nivel 4 Registros: vemos las evidencias del cumplimiento del SGSI, según lo visto en los niveles anterior y se tiene que mostrar que se ha cumplido con los mismos.

De manera específica, ISO 27001:2013 indica que un SGSI debe estar desarrollado por los siguientes documentos (en cualquier formato o tipo de medio):

- Alcance del SGSI: Se tiene que observar cómo está organizada la empresa identificando las áreas, relaciones de estas y mirar los límites que existe entre ellas, observar que áreas no son consideradas (si estas quedan afuera de la influencia del SGSI se considera las demás áreas con tareas concretas).

- Política y objetivos de seguridad: En este documento vemos el compromiso de la alta gerencia, y como la organización se enfocó en la gestión de la seguridad de la información. Este documento regula todos los procedimientos del funcionamiento del SGSI.

- Enfoque de evaluación de riesgos: Representación de la metodología a utilizar (ejecución de cómo se evaluará las vulnerabilidades, y el impacto de estas a los activos de información siempre y cuando estén contenidos dentro del alcance), se observará la aceptación del riesgo y los límites de estos.

- Informe de evaluación de riesgos: Investigación que resulta de aplicar el enfoque de evaluación de riesgos a los activos de información de la organización.

- Plan de tratamiento de riesgos: Este documento nos identifica que acciones de la dirección, sus recursos, responsabilidades y prioridades para la gestión del riesgo de la seguridad de la información, observando las conclusiones conseguidas de la evaluación de riesgos, objetivos de control detallados, y recursos disponibles.

- Procedimientos documentados: Aquí se encontrará todos los documentos para asegurar los procesos en planificación control y operación de la seguridad de la información, y medir la eficacia de los controles implementados.

- Registros: Este documento suministra las evidencias y el funcionamiento correcto de los requisitos del SGSI.

- Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); el SGSI viene contemplados los objetivos de control y controles basados en lo desarrollado en los procesos de evaluación de riesgos. Donde se evidencia inclusiones y exclusiones. Todo este lo vemos en este documento.

- Control de la documentación Después de haber implementado lo descrito anteriormente, se debe instaurar, formalizar, mantener los procedimientos de gestión necesarias para:

  - Antes de su emisión se debe de apropiar los documentos para su aprobación.
  - Solo cuando sea necesario se debe de revisar y actualizar documentos para verificar su validez.
  - El estado actual de la revisión de los documentos se debe de garantizar y los cambios se deben de identificar.
  - Documentos relevantes se deben de garantizar las versiones para que estén vigentes y disponibles en la organización.
  - Se deben de mantener los documentos legibles e identificables.
  - Documentos disponibles y de fácil acceso a las personas, y llevar procedimientos acordes a la clasificación de estos.
  - Documentos del exterior plenamente identificados.
  - Controlas los documentos obsoletos para su no utilización.
  - Identificar de manera eficaz los documentos retenidos con un propósito específico.

5.1.4 Implementación de un SGSI

Implementar un SGSI basado en ISO 27001, utilizamos el ciclo PHVA muy utilizado en los sistemas de gestión de calidad, con el anexo SL nos ayuda a implementar toda las ISO de manera similar. (ver Figura 5).

Figura 5: Como se implementan un SGSI

- ***Plan (planificar):*** establecer el SGSI.
- ***Do (hacer):*** implementar y utilizar el SGSI.
- ***Check (verificar):*** monitorizar y revisar el SGSI.
- ***Act (actuar):*** mantener y mejorar el SGSI.

Plan: Establecer el SGSI

Fuente: Sin autor. Figura 5 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html

- Definimos el alcance del SGSI dentro de la organización según su actividad principal, detallando todos sus componentes dentro del negocio y realizando justificación de alguna exclusión.

- Concretar la política de seguridad de la organización que:
  - Defina marco general, objetivos de seguridad de la información de la organización.
  - Requerimientos legales y contratos referentes a la seguridad de la información.
  - Gestión de riesgo en la organización donde se mantendrá el SGSI.
  - Aprobado por la dirección.
  - Criterios para la evaluación del riesgo,

- Se define la mejor metodología para evaluar los riesgos convenientes para el SGSI y obligaciones del negocio, se establece criterios para aceptar los riesgos y niveles especificados de los riesgos aceptables. Lo principal de la metodología son los resultados conseguidos se comparen y se pueden repetir (se aconseja definir una metodología propia tomando como ejemplo las metodologías estandarizadas.)

- Como identificar los riesgos:
  - Activos dentro del SGSI, responsables, propietarios, todos directamente dentro del activo.
  - Amenazas relacionadas con los activos.
  - Revisar las vulnerabilidades que se estén aprovechando por las amenazas.
  - Activos impactados por la confidencialidad, integridad y disponibilidad de los activos.

- Evaluación y análisis de los riesgos:
  - De un fallo de seguridad donde se pierde la confidencialidad, integridad y disponibilidad de los activos, justipreciar el impacto que ocurre en el negocio.
  - De la manera más realista hacer la probabilidad de un fallo de seguridad relacionando amenazas, vulnerabilidades, que impacto tiene con los activos y los controles que se encuentre implementados.
  - Tasar los niveles de riesgos. (ver Figura 6)
  - Establece previamente según criterios de aceptación de riesgo. Si dicho riesgo se puede aceptar o se puede tratar.

- Tratamientos de los riesgos y las distintas opciones:

  - Controles adecuados
  - Revisar políticas de aceptación de riesgos si es así aceptar el riesgo.
  - Impedir el riesgo, por ejemplo, dejar de hacer las actividades pertinentes que originan ese riesgo.
  - Trasladar el riesgo a compañías terceras.

Figura 6:Gestión de riesgos

Fuente: Sin autor. Figura 6 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html

- Verificar y seleccionar dentro del Anexo A de la norma ISO 27001:2013, los controles para trata el riesgo que son cumplidos dentro de los requerimientos identificados durante el proceso de evaluar los riesgos.
- La dirección debe aprobar los tipos de riesgos residuales y la implementación y buen uso del SGSI.
- Precisar la declaración de aplicabilidad que incluya:

    - Elección de los objetivos de control y porque se seleccionaron esos motivos.
    - Controles actualmente implementados.
    - Controles excluidos del Anexo A sus motivos de exclusión y revisión de posibles controles omitidos.

5.1.5 Modelo de Seguridad y Privacidad de la información

El ciclo de cinco fases que contempla el modelo de seguridad y privacidad de la información permite que las organizaciones gestionen sus activos de información para adecuar la seguridad y la privacidad.

Los seis niveles de madurez que contempla el modelo de seguridad y privacidad de la información. Es la evolución de dicha implementación de un modelo de operación. La estrategia del Gobierno en línea es que la seguridad y privacidad de la información sea un componente transversal. Donde el componente TIC se complementa para la gestión y el uso de las tecnologías de información, implementando adecuadamente el modelo de seguridad y privacidad de la información enfocándose a salvaguardar la confidencialidad, integridad y disponibilidad de la información. Lo que ayuda a cumplir la misión y la estrategia de una entidad.

El componente TIC se alinea y así se apoya el tratamiento de la información que se utiliza en los trámites ofrecidos por la organización. Verificando las normas de protección de datos personales, y las demás normas donde se garantiza el proceso de excepción al acceso público de dicha información.

El componente de Seguridad y Privacidad de la Información se alinea con el componente TIC el cual accede a la construcción de un país transparente, participativo y colaborativo donde se garantiza tenga los mejores controles de seguridad y privacidad, para que el ciudadano, empresas estén seguros y tenga confianza de que la información está segura. [6]

[6] Ministerio de Tecnologías de la Información y las Comunicaciones. tecnología de la información. Modelo de seguridad y privacidad de la información). 29 de julio 2016 Bogota. disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

5.2 MARCO CONCEPTUAL

Los miembros de las organizaciones se tienen que concientizar en las políticas y procedimientos de seguridad basados en una herramienta importante para la organización donde es significativo y sensible que la información favorece al desarrollo y la mejora del funcionamiento de la organización. Las reglas se deben de cumplir para evitar que surjan problemas y establece un soporte a los mecanismos de seguridad efectuados en la parte informática de la organización.[7]

Se debe de tener un plan de seguridad soportado con sus políticas, procedimientos y controles, esto con el fin de proteger el recurso. Esto se debe de lograr con un procedimiento claro y preciso.

Según lo explicado en el marco de referencia, un SGSI debe estar formado por los siguientes documentos:

- Alcance del SGSI
- Política y objetivos de seguridad
- Enfoque de evaluación de riesgos
- Informe de evaluación de riesgos
- Plan de tratamiento de riesgos
- Procedimientos documentados
- Registros
- Declaración de aplicabilidad
- Control de la documentación.[8]

El SGSI debe tener una política que recoja y transmita un compromiso de la dirección bajo una declaración de aplicabilidad del más alto nivel que suministre los objetivos definidos con el fin de delimitar responsabilidades para las diferentes actuaciones básicas y técnicas en la organización, las cuales se requieren para llevar a cabo la misión de seguridad en la organización. Se tiene que considerar los siguientes aspectos los cuales son:

---

[7] Gómez, V. Á. (2014). Gestión de incidentes de seguridad informática. España: RA-MA Editorial.

[8] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información (sgsi). requisitos 22 de marzo 2006 Bogota. Incontec disponible en **http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf**

- Instrucciones de las organizaciones y prioridades en todo lo referente a seguridad de la información, en las cuales se puede establecer los objetivos prioritarios de seguridad.
- Instrucciones legales, contratos y reglamentos de aplicación.
- La gestión de la seguridad de la información debe tener una responsabilidad del más alto nivel.
- Confidencialidad, integridad y disponibilidad, debe ser las propiedades básicas de la seguridad de la información, esto se debe definir como política.[9]

Basado en lo anterior nos podemos cuestionar que los directivos de las organizaciones deben de tomar iniciativas de TI ya que estas pueden multiplicarse de una manera rápida. Hay muchas empresas con proyectos emprendedores de TI algunos están en marchas otros en proyección. Pero se ha descubierto que estos proyectos cuando son presentados a los directivos suelen mostrar cierto amargo a dar ese paso fundamental para iniciar el proyecto, el cual más adelante puede tener un resultado importante y caso de éxito dentro de la empresa y los cuales pueden simplificar procesos dentro de la compañía. Estas decisiones no se pueden dejar al área de TI los directivos tiene que dar todo su apoyo para establecer prioridades de lo que es importante o problemático. Se debe de tener financiación para estos proyectos, el departamento de TI se esforzará al máximo para cumplir con el objetivo.

El desapego de los directivos a la hora de elegir proyectos TI puede ser perjudicial para una compañía, ya que se debe de tener una iniciativa de mejora en los sistemas, un ejemplo tangible puede ser las malas decisiones tomadas por la empresa Hershey Foods, la cual en 1999 realizo la puesta en marcha de dos sistemas simultáneamente, entre ellos, relación con el cliente, planificación de recursos y cadena de suministro, lo que finalmente tuvo la consecuencia de que la empresa no pudiera surtir de caramelos a sus clientes durante las fiesta de Halloween una de la más importante.

Podemos comparar lo anterior con la empresa Delta Airlines utilizando inversiones TI. En el año 1997, la empresa está en una crisis tecnológica, en años anteriores, el departamento de TI había sido subcontratado, lo que se logró con esto fue que varias unidades del negocio estaban insatisfechas con el servicio prestado. Esto se veía reflejado que los trabajadores no podían brindar un servicio óptimo al cliente ya que había varios sistemas en las distintas unidades, no se sabía con exactitud en que puerta de embarque estaba un pasajero debido que había muchos sistemas de consulta.

[9] Modelo para el gobierno de las TIC basado en las normas ISO. (2012). España: AENOR - Asociación Española de Normalización y Certificación

Estos sistemas estaban basados en tecnología antiguas y en ese momento dichos sistemas serian obsoletos por la llega del nuevo milenio. Esto llevo a que Delta aprovechara el efecto del nuevo milenio para realizar la potente plataforma llamada Delta Nervous System (DNS, Sistema Nervioso de Delta), con este sistema se mejoraría de manera inmediata el servicio al cliente del pasajero, dicho proyecto con un tiempo de tres años y de inversión de 1.000 millones de dólares, era la solución para los empleados de mejorar la capacidad de respuestas en los estados de vuelo de cualquier pasajero.

Al momento de realizar la visión del sistema los directivos de la compañía tomaron otra importante decisión, las inversiones simultáneas no las iban hacer. Por el contrario, decidieron mejorar el sistema y actualizar constantemente para brindar un mejor servicio a los pasajeros.

Pero, Delta era sensata que sus necesidades tecnológicas no se podían hacer inmediatamente, porque había limitaciones del departamento de TI, y los demás recursos estaban destinado a proyectos de otras áreas. Dichos proyectos habían puesto en peligro el sistema Delta Nervous System.[10]

5.3 MARCO LEGAL

Las estrategias de seguridad se requieren implementar en las organizaciones esto con el fin de proteger la información cumpliendo los estándares internacionales esto sirve para desarrollo de un SGSI (sistema de gestión de seguridad de la información). Basado en la norma ISO27001/ BS-7799-2.

BS 7799-2 es un estándar británico el cual determina los requisitos donde se establecen y administra un SGSI. La historia nos dice que su primera versión fue en el año 1995 basándose en mejores prácticas para la seguridad. Luego se hace actualizaciones y modificaciones en los años 1998,1999, 2001 y en el año 2002 es corregida para convertirse en estándar certificable, el ICONTEC es la única entidad en Colombia donde es aceptado, en la actualidad no se conoce alguna empresa que este certificada bajo este estándar.

[10] Ross, J. W., & Weill, P. (2004). Seis decisiones de TI que no debe dejar en manos del departamento de TI. España: Ediciones Deusto - Planeta de Agostini Profesional y Formación S.L.

Hablemos un poco de la Ley 1581 del 2012, protección de datos personales, el objeto es que las personas conozcan sus derechos de actualizar, rectificar su información recogidas en diferentes bases de datos, además garantiza libertades constitucionales el cual indica en el artículo 15 de la Constitución Política; así como el derecho de conocer su información indicado en el artículo 20 de la misma.

Ahora la Ley 1273 de 2009 protección de la información de datos delitos informáticos en Colombia, esta Ley nos indica 10 delitos dividido en dos capítulos donde nos enseñan las penas y multas vigentes. A continuaciones daremos el listado de los delitos:

Artículo 269A: Acceso abusivo a un sistema informático: no entras a sistemas sin autorización sin lo permitido o en contra de su voluntad, penas de 48 a 96 meses multa de 100 a 1000 Salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: obstaculizar el acceso a un sistema informático, bloquear datos del sistema o la red de esta, penas de 48 a 96 meses multa de 100 a 1000 Salarios mínimos legales mensuales vigentes.

Artículo 269C: Interceptación de datos informáticos: Bloquear datos desde el origen o interior. Penas de 36 a 72 meses.

Artículo 269D: Daño Informático: sin tener los permisos entra al sistema de información y a sus componentes lógicos y destruya, formatear dichos datos. Penas 48 a 96 meses multa 100 a 1000 Salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso: el que produce o venda sin tener la facultad software malicioso en el territorio nacional. Penas 48 a 96 meses multa 100 a 1000 Salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales: podemos ver más detallado este artículo en la Ley 1581 del 2012. Penas 48 a 96 meses multa 100 a 1000 Salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales: duplique páginas web para su beneficio propio. Penas 48 a 96 meses multa 100 a 1000 Salarios mínimos legales mensuales vigentes. La misma sanción para el que duplique dominios, IP, páginas de bancos, sitios de confianzas. Estas penas pueden subir dependiendo al caso.

Artículo 269H: Circunstancias de agravación punitiva: aumentos de las penas a las tres cuartas partes dependiendo de la conducta:

1. Redes o sistemas informáticos del sector estatal, financiero o extranjero

2. Servidores públicos.
3. Confianza en proveedores que tiene información confidencial
4. Revelar datos sin tener permiso de la persona.
5. Provecho para sí mismo u otra persona.
6. Terrorismo o riesgo para la seguridad de la defensa nacional.
7. Instrumento utilizado de buena fe.

Si se comete alguna de estos numerales, inhabilitación profesional, penas de tres años y no utilizar equipos informáticos.[11]

[11] LEY 1273 DE 2009 Nivel Nacional enero 2009 disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

6. DISEÑO METODOLÓGICO

El diseño metodológico que se va a utilizar y se definió es descriptivo, debido a que el problema sobresale en la organización, en el cual se inicia con un análisis y evaluación mediante variables para así poder diseñar y analizar un SGSI bajo la norma ISO/IEC 27001:2013.

De la siguiente manera se tomarán las instrucciones a seguir:

- Investigación de riesgos y amenazas, con el fin de asegurar la documentación pertinente. Con esto se desarrolla y se realiza la implementación del SGSI.
- Encuesta y entrevista diseñadas de la mejor manera para el personal con procesos importantes dentro de la organización, con el fin de implementar el SGSI.
- Bosquejo del SGSI.
- Tentativas y desarrollo del SGSI.

La distribución de los requisitos, controles y mejores prácticas servirán para una implementación del SGSI bajo la norma ISO/IEC 27001:2013, los controles que se van a utilizar se definen a continuación:

Bajo una capacitación al personal de la Empresa Centro de Terapias Integrales MISALUD S.A.S se manifestarán los dominios de seguridad de la norma ISO/IEC 27001:2013.

- Políticas de seguridad: la política de seguridad de la información de la empresa Centro de Terapias Integrales MISALUD S.A.S. tiene que estar estipulada en un documento.
- Organización de la seguridad: el personal tiene que estar comprometido, asegurar sus roles, acuerdos, el manejo con clientes terceros, compromisos, entre otros, esto bajo una estructura del departamento de seguridad.
- Gestión de activos: confidencialidad, integridad y disponibilidad tienen que estar identificados mediante sus activos.
- Seguridad del Recurso Humano: los empleados, contratista, terceros deben de entender sus responsabilidades y sean idóneos para cumplir roles esto debe estar asegurado mediante procedimientos para minimizar los riesgos con el personal.
- Seguridad física y del entorno: la información, accesos físicos no autorizados, daños, deben de estar asegurado mediante procedimientos y controles esto es para prevenir lo dicho anteriormente en la organización.
- Gestión de comunicaciones y operaciones: la operación de los departamentos donde la información procesada debe de estar asegurada

mediante procedimientos y controles esto con el fin de garantizar la correcta operación dentro del organización.

- Control de acceso: los activos deben de estar protegidos para que el personal no autorizado no tenga acceso a estos, deben de estar asegurado mediante procedimientos y controles.
- Adquisición, desarrollo y mantenimiento de sistemas de información: los nuevos sistemas de información o los cambios que se hagan se deben de incluir en los controles y su procedimiento.
- Gestión de incidentes de seguridad: las debilidades del sistema de información y los eventos que ocurran se tiene que comunicar inmediatamente para que se tome una acción correcta en el momento justo, esto debe de estar asegurado mediante procedimientos y controles.
- Gestión de la continuidad del negocio: las interrupciones del negocio deben de protegerse para no tener fallas críticas en los sistemas de información, ya que esto se puede convertir en un desastre y no se puedan recupera a tiempo, por esto deben de estar asegurado mediante procedimientos y controles.
- Cumplimiento: documento que busca avisar si se incumple total o parcialmente las normas enfocadas en controles de seguridad.[12]

Posteriormente se realizarán las siguientes actividades de tratamiento de las BD con la información de los pacientes, personal a cargo de estas, se clasificarán en medio físico y electrónico. Con esto se adquiere la información importante que se relaciona a continuación:

- Números de bases de datos con información de los pacientes.
- Numero de titulares distribuidos en las bases de datos
- Por donde se atiende a los pacientes
- Que datos se utilizan de los pacientes: ID, donde vive, estado, o historia clínica que es un dato sensible.
- Donde se encuentra las bases de datos, si en medios propios en archivos carpetas, dentro del lugar o en otro lugar y electrónicamente.
- Si hay uno o más encargados de las bases de datos, que medidas de seguridad o controles tienen implementado esto con el fin de que el riesgo sea mínimo.
- Quien tiene las bases de datos y que hace con ese contenido.
- Como se obtuvieron estos datos. Autorizado por el titular o mediante la compra u obtención por parte de terceros.
- Si las bases de datos se obtuvieron por medio de una transacción internacional.

[12] SALCEDO, Robin, plan de implementación del sgsi basado en la norma ISO 27001:2013. {En Línea}, {19 diciembre 2014} disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf

- Si fueron cedidas, quien la cedió con su información básica.
- personales tratados.
- Información acerca de la tenencia de datos contenidos de titulares (autorización)
- Como se obtuvieron estos datos (directamente del titular o mediante terceros).
- Si realizo transferencia internacional de la información.
- Si se cedió las bases de datos, quien la cedió y como. Datos básicos.

La entidad tiene que definir los límites para garantizar que todos los activos importantes tengan una alta relevancia para la valoración del riesgo. Al momento en que la organización defina esto se debe de tener en cuenta la información que se detalla a continuación:

- Estrategias del negocio, detallado mediante políticas
- Dentro del negocio cuál es su proceso.
- Las funciones y organigrama de la organización.
- Normatividad del sector dentro de la organización.
- La organización debe de tener la política de seguridad de la información.
- El riesgo a donde se ve reflejado mediante un enfoque global.
- Los activos de TI
- Donde está ubicado la organización con sus características.
- Que amenazas tiene la organización y sus efectos.
- Expectativas de todos los interesados.
- Su entorno
- Transacciones con otras entidades.[13]

Existen varios modelos que podemos tomar como bases para este proyecto el MSPI se puede implementar en cuatro fases, donde las entidades gestionan la seguridad y sobre todo la privacidad de la información, esto con el fin de fortificar a las personas sus datos de forma protegida y cumplir con la normatividad vigente. También se adoptan las estrategias del Gobierno, dando cabalidad a todos sus componentes. Toda esta gestión va aplicada a todos los procesos de la implementación del modelo, con esto se conserva las perspectivas del personal de la organización, y también aplicar para los clientes. Los costos para la implementación de esta gestión se verán reflejados al momento de implementar cada fase. Esto se puede observar en MSPI (Ver Figura 7).[14]

[13] MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES. Guía de Gestion de riesgos Versión 3.0 01 de abril 2016 disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

[14] MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES .guía para la preparación de las TIC para la continuidad del negocio Versión 1.0 15 diciembre 2010 disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

Implementación de las medidas de autodiagnóstico

Fase de desarrollo donde se ejecutan las fases dentro de la organización:

Figura 7:Fase de desarrollo

Fuente: Sin autor. Figura 7 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html

6.1 TIPO DE INVESTIGACIÓN

Para el diseño metodológico se utilizará del tipo aplicado, ya que el resultado de este proyecto nos orientará a lograr un nuevo conocimiento destinado a solucionar problemas.

Investigación descriptiva: Se hace uso de la investigación descriptiva con la cual podemos concretar, analizar y ordenar los resultados de lo que se observó tanto como conductas y característica de la población y sus posibles fenómenos y hechos.

6.2 METODOLOGÍA

Para el análisis de riesgos del Centro de Terapias Integrales Misalud S.A.S. Se utilizará una metodología MAGERIT, esto con el fin de mirar las medidas para adoptar y posteriormente tratar de manera adecuada los activos de la empresa.

6.3 DISEÑO DE HIPÓTESIS

El diseño de un SGSI para el Centro de Terapias Integrales Misalud S.A.S. en donde se va a desarrollar unas series de acciones en las cuales solucionaran problemas de seguridad de la información a nivel de la empresa y legal todo esto mediante el análisis de riesgo, corrigiendo y actualizando la seguridad de la información corporativa y garantizar que la empresa tenga una continuidad de negocio.

6.4 VARIABLES

Vulnerabilidades, activos, Incidentes, riesgos, personal de la empresa, controles existentes, Sistemas informáticos.

6.5 UNIVERSO O POBLACIÓN

Trabajadores de la IPS Centro de Terapias Integrales Misalud S.A.S.

6.6 TÉCNICAS PARA LA RECOLECCIÓN DE LA INFORMACIÓN

En el presente proyecto se utilizarán técnicas de análisis de datos en investigación de campo los cuales permitirán realizar un análisis sistemático del problema de tal manera que se pueda identificar e interpretar de manera adecuada, a partir de los datos obtenidos.

6.7 ESQUEMA TEMÁTICO

Capítulo 1 Describir los principales problemas de seguridad y Establecer los riesgos que se presentan con la información.

Capítulo 2 Verificar si el Centro de Terapias Integrales MISALUD S.A.S. posee políticas o manuales de seguridad de la información y Proponer un SGSI para el departamento TI.

7. INVESTIGADORES

7.1 PROPONENTE PRIMARIO

Harry Marquez Leal Magister en Calidad en Servicios de Salud, Ingeniero de Sistemas, experiencia sector salud liderando proyectos de este sector

7.2 PROPONENTES SECUNDARIOS

Dra. Rosario de la Rosa, Abogada especialista en derecho penal, cargo en la empresa gerente.
Ing. Lucia Estrada, Ingeniera Industrial, especialista en seguridad y salud en el trabajo cargo en la empresa coordinadora de salud y trabajo.
Ing. Juan Jose Cruz Tutor del Proyecto
Ing. Christian Reynaldo Angulo director del Proyecto

8. DESARROLLO DE LA INVESTIGACIÓN

8.1 COMPLICACIONES VITALES DE SEGURIDAD QUE PRESENTA LA ORGANIZACIÓN EN SU DEPARTAMENTO TI.

La seguridad de la información es velar por la integridad, disponibilidad y confidencialidad de los activos de información esto basados sobre tres pilares (Procesos, Personas y Tecnología).

En el Centro de Terapias Integrales Misalud S.A.S. en su departamento de TI se pudo observar lo siguiente a través de entrevistas con el personal encargado y visitas técnicas realizadas, que afecta a la seguridad de la información:

8.1.1 Procesos

- Copias de otra empresa de las políticas de la seguridad de la información, lo que significa que estas políticas no fueron aprobadas ni revisadas por la Dirección, ni fueron comunicadas a los empleados de la empresa o terceros.

- Organización de la seguridad de información, no se tienen roles ni responsabilidades de la seguridad de la información. Existe conflicto en la asignación de tareas lo cual trae inconvenientes para los activos de la empresa.

- Seguridad de los recursos humanos, los empleados o contratistas no saben cuáles son sus responsabilidades respecto a la seguridad de la información. No realizan capacitaciones en forma apropiada y por ende no hay actualizaciones sobre las políticas de seguridad de la empresa.

- Gestión de activos, no se tiene identificado los activos de la empresa y por ende no hay responsabilidades de estos, el inventario de los activos no está actualizado, y no se tiene implementado reglas para el uso aceptable de la información, el etiquetado de los activos no está implementado. No se encuentra desarrollado el proceso de manejos de activos.

- Control de acceso, no se tiene una política de control de acceso con base a los requerimientos del negocio y seguridad de la información, el acceso a redes y sus servicios está permitido a todos los usuarios. No se tiene implementado un proceso de registro para la asignación de derechos, todos los usuarios tienen derechos privilegiados los cuales no se revisan por el departamento de TI, al momento de terminar el empleo no se cancela los usuarios por ende sus privilegios tampoco.

- Seguridad física y ambiental, los empleados pueden entrar al área de TI y esto puede ocasionar daño o interferencia a la información de la organización, no se tiene definido un perímetro de seguridad, los controles de entradas físicas no son los apropiados, las amenazas externas o ambientales no se encuentra diseñadas.

- Los equipos no están protegidos para riesgos de amenazas, peligros ambientales y lo puede utilizar cualquier usuario o paciente.

- Las copias de respaldo no están documentadas no se lleva registro ni evidencias y solo se hacen al sistema de información, relojes no se encuentra sincronizados.

- Los acuerdos de confidencialidad no se encuentran documentados.

- Relación con los proveedores no se tiene una política de seguridad respecto a los proveedores.

- Gestión de incidentes de seguridad de información, las responsabilidades no están establecidas por lo tanto no se puede gestionar de manera eficaz los incidentes de seguridad. Por lo tanto, los informes de eventos, debilidades, evaluación, respuestas, recolección no están definidas ni implementados.

- No se encuentra implementado la continuidad de la seguridad de la información, por lo tanto, ante una situación adversa esto puede ser crítico para la empresa.

- Para concluir no se está cumpliendo con las políticas o normas de seguridad, lo que significa que la gerencia no está revisando el cumplimiento de estas, por lo tanto, esto trae complicaciones vitales de seguridad.

- La inversión en seguridad es mínima digamos que nula, los equipos están instalados sin cumplir algún criterio de norma internacional, se da a entender que los instaron a groso modo, se puede entender que en el sector salud no invierte en seguridad informática, un 10% de las entidades son las que invierten en este sector, en Colombia se está entrando al mundo de la seguridad informática en el sector salud, en la cual se puede simplificar procesos, mejorar datos de los paciente, y realizar interoperabilidad de registros en el sector, también podemos realizar procesos de blockchain y bigdata, pero para mejorar y aplicar a estos procesos se necesita una inversión de dinero y personal capacitado con competencias en el tema.

8.1.2 Personas

- No existe responsabilidades a los usuarios lo cuales no rinden custodia de la información.

- Los equipos no están protegidos para riesgos de amenazas, peligros ambientales y lo puede utilizar cualquier usuario o paciente.

- Se necesita más personal con las competencias suficientes para mejorar el proceso de seguridad informática.

- Sensibilizar al personal y capacitar en los criterios establecidos en la ISO 27001:2013.

- Presupuesto para contratar personal capacitado para asesorar el proceso de seguridad informática.

- Relaciones con proveedores no existe control en los contratos y hacer seguimientos de los mismo.

- La gerencia no demuestra liderazgo y compromisos por mejorar el departamento de sistemas.

8.1.3 Tecnología:

- El proceso de conexiones seguras esta implementado en un 20% lo cual la calidad de las contraseñas no se encuentra implementadas.

- Se pueden utilizar programas de cualquier clase, se puede instalar con privilegios de administrador. No tiene documentado un proceso de restricción de instalación de software a los usuarios.

- Seguridad de las operaciones, los equipos están protegidos por antivirus actualizados, pero no tiene implementadas políticas de acceso a páginas web maliciosas, por lo tanto, los controles contra estos códigos no están implementado de la mejor manera.

- No se realizan pruebas de penetración lo que significa que las vulnerabilidades que poseen no están documentadas y por lo tanto no se pueden evaluar y con esto tomar medidas pertinentes para trata dicho riesgo en la empresa.

- Seguridad de la comunicación, no se tiene identificado cuales son los mecanismos de seguridad en los servicios de red, no se tiene establecidos las políticas de transferencia de la información.

- Seguridad perimetral con el fin de proteger de los perímetros físicos, instrucciones, instalaciones sensibles esto es importante para evitar robo o desaparición de la red de la empresa.

- En el punto anterior se indicó que los equipos poseen antivirus NOD32 con licencia de un año, pero dichos equipos no tienen los protocolos y políticas para proteger los equipos como por ejemplo las USB no están bloqueadas.

- Gestión de recursos la calificación de la información es visible para todos no existe un inventario de recursos y su respectiva calificación.

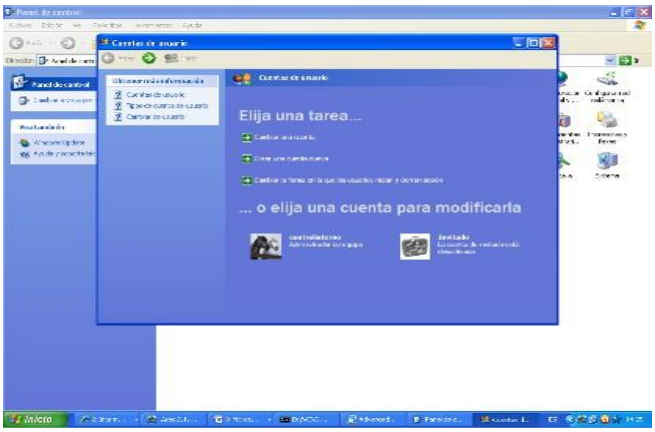
- No existe un protocolo de cifrado de claves, se puede colocar cualquier clave sin distinguir mayúsculas minúsculas y carácter especial.

A las presentes complicaciones se adjunta las siguientes evidencias encontradas en la entidad:

Figura 8: Identificación departamento de informática

Fuente: El autor

Figura 9: Perfil Administrador



Fuente: El autor

Figura 10: Cables Sueltos

Fuente: El autor

Figura 11: Suministro ininterrumpido de energía

Fuente: El autor

8.2 VULNERABILIDADES EXISTENTES EN EL CENTRO DE TERAPIAS INTEGRALES MISALUD S.A.S. REFERENTE AL MANEJO DE LA INFORMACIÓN.

Para el siguiente objetivo utilizaremos un método para encontrar la vulnerabilidad existente en la IPS, se utilizará el programa llamado Nessus el cual sirve para realizar escaneos de vulnerabilidades en diferentes sistemas operativos e informa al cliente sobre sus vulnerabilidades.

Nessus es un software que permite escanear puertos y vulnerabilidades, con lo cual obtenemos una bigdata con distintas vulnerabilidades de diferentes sistemas operativos y software comerciales. Nessus se puede trabajar de diferentes maneras. Una opción es trabajar con demon o componente principal, el cual realiza chequeos en el host y encuentra vulnerabilidades, la segunda opción es un servidor cliente que se conecta al demon o servicio en Nessus, se le indica distintos escaneos de directrices o políticas para hallar vulnerabilidades, el cual nos genera reportes. La tercera opción son Script lo cual se lleva a un lenguaje llamado NALS. Al final luego de haber hecho el análisis de vulnerabilidades se utilizará un proceso de gestión.

El primer paso es definir la importancia del escáner, planear e iniciar el escaneo de vulnerabilidad, este paso lo llamamos descubrimiento de la vulnerabilidad.

Segundo paso se tiene que evaluar si la vulnerabilidad no es eliminada y fuera explotada, se debe priorizar las vulnerabilidades de acuerdo con el nivel crítico del negocio, este paso lo llamamos evaluación de la vulnerabilidad.

Tercer paso realizar las correcciones de los sistemas operativos afectados, como acciones correctivas y compensatorios, en base de eso realizamos recomendaciones del riesgo, este paso lo llamamos determinar las acciones de remediación.

En base al tercer paso lo dividimos en dos acciones correctivas y acciones compensatorias, en las correctivas son controles aplicados directamente en el sistema vulnerable y las acciones compensatorias son controles aplicados indirectamente a través de sistemas seguridad externos.

Cuarto paso es generar un plan de acción que indique cuando deben ser aplicadas las acciones de remediación del paso 3. Este paso lo llamamos planeación y priorización de las acciones de remediación.

Quinto paso las recomendaciones planeadas deben ser ejecutadas en los tiempos establecidos. En su debido caso si ocurre problemas con la implementación de las acciones se deben implementar diferentes acciones de remediación. Este paso lo llamamos implementación de acciones de remediación.

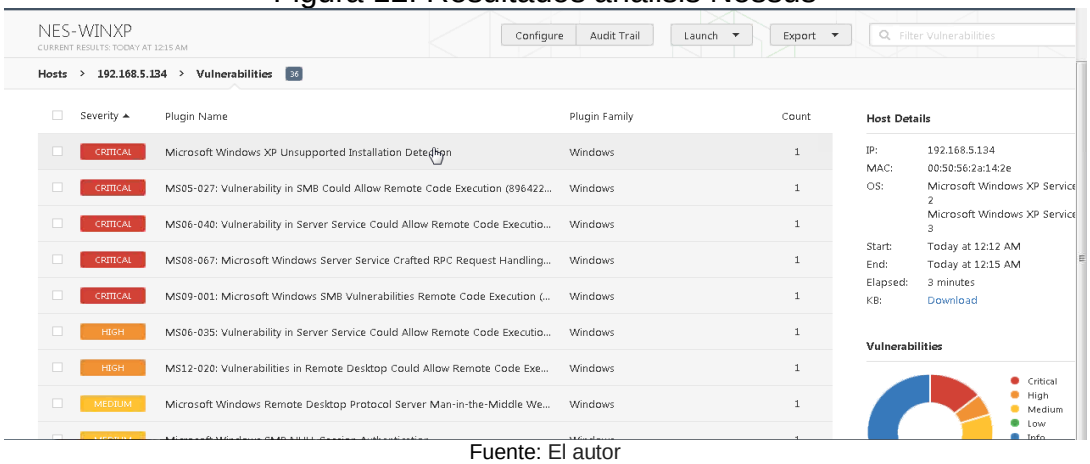
Sexto paso es verificar que las acciones hayan sido implementadas y hayan remediado o mitigado las vulnerabilidades, esta verificación se debe usar las mismas herramientas de escaneos y los procesos que el análisis inicial. Este paso lo llamamos verificación de efectividad.

El séptimo paso se establece una adecuada gestión de vulnerabilidades se deben monitorear continuamente las vulnerabilidades y amenazas, la ejecución del proceso deben ser usadas para reevaluar y mejorar la gestión de vulnerabilidades, este paso lo llamamos lecciones aprendidas y mejora.

Después de haber descrito los pasos a utilizar en este objetivo procederemos a mostrar la evaluación de las vulnerabilidades.

Paso 1:

Figura 12: Resultados análisis Nessus



Fuente: El autor

Paso 2: en este paso se debe priorizar las vulnerabilidades de acuerdo con el nivel crítico del negocio, en este paso utilizaremos el llamado Modelo de Seguridad y Privacidad de la información, el cual está contemplado en cinco fases en este caso se utilizará las tablas del MSPI suministrada por gobierno en línea en donde se abordará las vulnerabilidades encontradas, con el fin de determinar el nivel de cumplimiento y madurez.

Tabla 1: Definición de los niveles de madurez

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. tecnología de la información. Modelo de seguridad y privacidad de la información). 29 de julio 2016 Bogota. disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Luego de haber definido el nivel de madurez, en la matriz del MSPI se adjuntará las evidencias encontradas dentro de la IPS (Ver anexo N° 5 y 6), se calificará de 0 a 100 de acuerdo con la siguiente tabla:

Tabla 2: Escala de Valoración de Controles

Tabla de Escala de Valoración de Controles		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. tecnología de la información. Modelo de seguridad y privacidad de la información). 29 de julio 2016 Bogota. disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

En el tercer paso utilizaremos un formato para realizar las correcciones sistema operativo afectado, sus respectivas correcciones y recomendaciones del riesgo. (Ver anexo N° 7)

Cuarto paso es genera el plan de acción el cual nos va a permitir donde se encuentra las vulnerabilidades con el fin de que sean detectadas y posterior prevenir estos problemas y aplicar las acciones de recomendación. (Ver anexo N° 8)

Quinto Paso de acuerdo con la recomendación planeadas verificar que sean ejecutadas en los tiempos establecidos para eso utilizaremos como ayuda la tabla de identificación de la línea base de seguridad hoja de levantamiento de información MSPI suministrada por gobierno en línea (Ver anexo N° 9).

Implementamos el sexto paso en donde ejecutamos las acciones planeadas se hayan implementados de la mejor manera y haya mitigado las vulnerabilidades. Volveremos a utilizar la herramienta Nessus para realizar la verificación de la efectividad.

El último paso se establece una gestión de vulnerabilidades se deben monitorear continuamente las vulnerabilidades y amenazas, la ejecución del proceso deben ser usadas para reevaluar y mejorar la gestión de vulnerabilidades para esto utilizaremos el formato. (Ver anexo N° 10)

8.3 ANÁLISIS DE POLÍTICAS O MANUALES DE SEGURIDAD DE LA INFORMACIÓN EXISTENTES EN EL CENTRO DE TERAPIAS INTEGRALES MISALUD S.A.S.

El primer paso es realizar el listado de maestro de documentos, utilizaremos el instrumento de identificación del MSPI que hemos venido trabajando en puntos anteriores. (Ver anexo N° 11)

En base a la evaluación de riesgos se diseñan las políticas de seguridad según la norma ISO/IEC 27002:2013, con el objetivo de utilizar los controles cada dominio como apoyo a la gestión de la información se realiza evaluación de las políticas actuales de la entidad con su porcentaje de cumplimiento.

Implementando la norma ISO 27001:2013 se explora la posibilidad de certificar los tres pilares de la información, para disminuir amenazas y estar preparado para un ataque como externas y de los mismos empleados, con controles seguros, monitoreando la información y haciendo seguimiento a los riesgos.

La Empresa se responsabiliza a desempeñar las practicas legales, contractuales, legales y reglamentarias basadas en la seguridad de la información, esto siempre se tiene que ver como una mejora continua del proceso de la seguridad de la información, para lograr objetivos y los compromisos de la empresa con el adecuado uso de la información.

La Gerencia debe tener el compromiso de brindar todo su apoyo consiguiendo los recursos óptimos para que los trabajadores y proveedores efectúen el adecuado uso de la información.

La empresa se responsabiliza a practicar las exigencias especificada en la norma ISO 27001:2013, y las buenas prácticas de estas para la mejora del SGSI.

Objetivos

- Capacitar a los trabajadores de la empresa en buenas prácticas de seguridad de la información para prevenir casos de ataques que puedan afectar las operaciones de la empresa.
- Proteger en los mayores de los casos los documentos confidenciales de tipo electrónico y papel.
- Tratar de priorizar las atenciones cuando se tenga novedades que afecte la operación de la empresa mediante la seguridad de la información.
- Garantizar que las políticas se cumplan de la mejor manera y que los registros este protegido y que no sean utilizados para modificaciones o accesos inoportunos y estén disponibles para cuando se requieran.

8.3.1 Cumplimiento de dominios

Tabla 3 Porcentajes y cumplimientos de dominios

Norma	Dominios	Estado
5	Políticas de seguridad	20%
8	Gestión de activos	13%
9	Control de acceso	9%
11	Seguridad física y ambiental	10%
12	Seguridad en la operativa	20%
13	Seguridad en las telecomunicaciones	3%
14	Adquisición, desarrollo y mantenimiento de los sistemas de información	0%

Cumplimiento General	11%

Dominios	Bajo	Medio	Alto
Políticas de seguridad	20%	0%	0%
Gestión de activos	13%	0%	0%
Control de acceso	9%	0%	0%
Seguridad física y ambiental	10%	0%	0%
Seguridad en la operativa	20%	0%	0%
Seguridad en las telecomunicaciones	3%	0%	0%
Adquisición, desarrollo y mantenimiento de los sistemas de información	0%	0%	0%

Fuente: el autor

8.3.2 Cumplimiento de objetivos de control

Tabla 4: Porcentaje de cumplimiento de objetivos de control

Norma	Objetivos de Control	Estado
5.1	Directrices de la Dirección en seguridad de la información	20%
8.1	Responsabilidad sobre los Activos	20%
8.2	Clasificación de la Información	20%
8.3	Manejo de los soportes de almacenamiento	0%
9.1	Requisitos de negocio para el control de accesos	10%
9.2	Gestión de acceso de usuario.	0%
9.4	Control de acceso a sistemas y aplicaciones	16%
11.1	Áreas Seguras	13%
11.2	Seguridad de los Equipos	7%
12.2	Protección contra código malicioso	20%
12.3	Copias de seguridad	20%
13.1	Gestión de la seguridad en las redes.	0%
13.2	Intercambio de información con partes externas.	5%
14.2	Seguridad en los procesos de desarrollo y soporte	0%
	Cumplimiento	11%

Objetivos de Control	Bajo	Medio	Alto
Directrices de la Dirección en seguridad de la información	20%	0%	0%
Responsabilidad sobre los Activos	20%	0%	0%
Clasificación de la Información	20%	0%	0%
Manejo de los soportes de almacenamiento	0%	0%	0%
Requisitos de negocio para el control de accesos	10%	0%	0%
Gestión de acceso de usuario.	0%	0%	0%
Control de acceso a sistemas y aplicaciones	16%	0%	0%
Áreas Seguras	13%	0%	0%
Seguridad de los Equipos	7%	0%	0%
Protección contra código malicioso	20%	0%	0%
Copias de seguridad	20%	0%	0%
Gestión de la seguridad en las redes.	0%	0%	0%
Intercambio de información con partes externas.	5%	0%	0%
Seguridad en los procesos de desarrollo y soporte	0%	0%	0%

Fuente: el autor

8.3.3 Madurez de los controles

Tabla 5: Número de controles

Nivel	N° controles

No realizado	33
Realizado informalmente	13
Planificado	5
Bien definido	0
Cuantitativamente controlado	0
Mejora continua	0

Total, de Controles	**51**

Fuente: el autor

8.3.4 Informe ejecutivo estado de las políticas

Como se puede observar en el punto 9.3.2, el porcentaje de las políticas esta es del 20%, lo cual es un porcentaje muy bajo debido a la información delicada que se maneja en un centro de salud. Hablando de seguridad informática en el sector salud en Colombia, vemos que las entidades de salud no implementan herramientas para proteger información delicada de los pacientes, mirando estadísticas vemos lo siguientes:

Estudios hechos por compañías reconocidas en el sector en especial ESET nos indica que hay un gran camino que transitar en el sector salud. La importancia de la seguridad de la información todavía no ha tocado de fondo a los directivos de la organización del sector salud, lo que sí ha sucedido en otras industrias que desde hace mucho más tiempo trabajan en la reducción de riesgos, por eso es importante contar con un plan de seguridad integral de la información.

Este estudio nos arroja sorprendentemente que un 39% del personal TIC del sector salud no comprenden de cómo protegerse de ataques cibernéticos. Y otro 50% no tiene la respuesta mediante un plan a los incidentes ocurridos. Dentro de esto encontramos que 1 de cada 4 ingenieros de TI que trabaja en el sector salud no puede asegurar lo siguiente:

- Estadísticas de ataques cibernéticos ocurridos en la organización durante el último año
- Pérdida o exhibición de datos, de pacientes, mediante incidentes de seguridad.
- Si los ataques evadieron el firewall, antivirus, IPS, u otros controles de seguridad.

La dimensión de proteger los datos en el sector salud es muy importante. Hay muchas compañías que han trabajado en asesorar cuales son los riesgos dentro de este sector, de cómo afrontarlos si en caso de ocurrir un ataque esto con el fin de proteger al paciente y garantizar la seguridad. Por eso hay que tomar medidas preventivas como las copias de seguridad periódicas definidas en la política de seguridad. Doble autenticación, cifrar los datos y pentesting caja blanca para que detecten posibles ataques y con estos corregir las vulnerabilidades presentadas, todo esto permite a las empresas del sector salud brindar un excelente servicio a sus pacientes.[15]

Como podemos observar, las instituciones prestadoras de salud incluidos Clínicas privadas, hospitales públicos, laboratorios clínicos, son blanco fácil y atractivos para Hackers ya que estas entidades manejan información delicada como datos personales, datos financieros y las historias Clínicas donde hay información de medicamentos e incluso datos de los médicos. Como se puede observar ya los Hacker no están interesados en los datos como nombre, dirección, número de documento o teléfono del paciente o afiliado, sino que están más interesados en los medicamentos quien lo distribuye o las necesidades de los tratamientos.

Con lo observado anteriormente vemos que es importante un Sistema De Gestión de la Seguridad de la Información (SGSI), especialmente en el Sector Salud.

Con el proyecto que se está desarrollando observamos que las políticas de seguridad de la empresa están en un 20%, se encontró una carpeta de 37 hojas en donde se desarrollan unas políticas de información, pero no están implementadas en la empresa y dichas políticas se ven que son copiadas de otra empresa, y las políticas se elaboraron para cumplir con lo estipulado en la Ley 1581 del 2012 para el informe correspondiente a la Superintendencia de Industria y comercio.

De los 51 controles vemos que 33 no están implementados lo que equivale a un porcentaje del 64%, lo cual es muy alto, se tienen 13 controles realizado informalmente lo cual es un porcentaje del 25% y solo 5 controles que están planificados lo cual es un porcentaje del 9%.

[15] Sector salud lejos de adoptar medidas de ciberseguridad: Por Corporación Colombia Digital mayo 27 2016, en línea https://colombiadigital.net/actualidad/noticias/item/8963-sector-salud-lejos-de-adoptar-medidas-de-ciberseguridad.html

En general se tiene implementando un 11% de los objetivos de control, en el cual se verifican cada objetivo de control y el porcentaje máximo de implementación es de 20%.

Estos porcentajes es la realidad que vive el sector salud en materia de Seguridad Informática. Las instituciones prestadoras de salud incluidas Clínicas privadas, hospitales públicos, laboratorios clínicos archivan datos muy confidenciales de muchos pacientes, para esto se necesitan buenas prácticas de seguridad por este motivo es importante implementarlos. Capacitar al personal y clientes sobre la información que manejan dentro del sector salud. Los estudios no demuestran que un 90% de las entidades del sector salud han sido objetivos de violación de datos.

Todo lo dicho anteriormente podemos deducir que todas las empresas del sector salud son especialmente amenazadas por ataques ya que son vulnerables. Todas estas organizaciones de manera inmediata y de la forma más rentable necesitan prevalecer sus protocolos de seguridad porque, con esto protegen la información de sus afiliados y/o pacientes. Los estudios nos demuestran que un 60% de las entidades que sufrieron un ataque tuvieron que cerrar la organización durante los siguientes seis meses de haberse presentado el ataque.[16]

8.3.5 Calificación estado de las políticas

La calificación que se le da a estas políticas del 1 al 5, siendo 1 Malo y 5 excelente, es de 1, se da esta calificación debido a la copia que realizaron de la política y a la no implementación de esta en la entidad.

NOMBRE DE POLÍTICA	CALIFICACIÓN DE POLÍTICA
Política de Seguridad	1
Política de Confidencialidad	1

Porque se da esta calificación, debido a que las políticas son copia de otra empresa lo cual es grave, y no se encuentra implementado en la empresa, solo están por cumplimiento de la Ley 1581 del 2012.

[16] Ciberseguridad en el Sector Salud Susan Biddle, 2016 en línea https://revistaempresarial.com/salud/salud-ocupacional/ciberseguridad-sector-salud/

8.4 MODELO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PROPUESTO PARA EL CENTRO DE TERAPIAS INTEGRALES MISALUD S.A.S.

8.4.1 Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información

Para llevar a cabo una implementación de en una organización de un SGSI hay varias formas, pero pueden existir varias maneras, pero para lograr el éxito y no tener resultados de incertidumbre, se tiene que implementar un enfoque que permita cumplir con los elementos del SGSI. Por eso se utilizará la norma ISO 27003.
Se utilizará estas cinco fases combinadas con la ISO 27001 a continuación se describirá en detalle estas fases y detalles prácticos para la implementación de UN SGSI.

- Fase 1: aprobación de la dirección para iniciar el proyecto

La primera fase es la menos comprendida en un proyecto de SGSI, ya que este no es un proyecto del área TI, es un proyecto de la organización y por lo tanto requiere que la dirección apruebe y apoye el proyecto para su correcta implementación.

Para implementar la primera fase hay que llevar ciertas actividades que son:

- Tener claro cuáles son las prioridades de la organización para el desarrollo de un SGSI, se recomienda estos elementos para dichas prioridades:
  - ✓ La organización cuenta con objetivos estratégicos: primero hay que determinar cuáles son los objetivos estratégicos de la empresa y de estos cuales pueden aportar para la implementación del SGSI.
  - ✓ Normatividad de la seguridad de la información: describir los requerimientos normativos que tenga la empresa, de terceros de los cuales cumplan los criterios de confidencialidad, integridad y disponibilidad de la información. Esto es fundamental para justificar la implementación de un SGSI.
  - ✓ Sistemas de gestión existentes: si ya la empresa tiene implementada otras normas de sistemas de gestión podemos utilizar estas bases para la implementación del SGSI aprovechando que la norma ISO cuenta con la estructura del ANEXO SL. Y podemos utilizar ciertos elementos en nuestra implementación.
- Alcance preliminar del SGSI: inicio de un SGSI, nos preguntamos el SGSI que quiere proteger y con esto definimos el alcance. La ISO 27003 indica que

se debe realizar un resumen de los requisitos impuestos por la dirección y obligación realizadas por terceros a la empresa.

- Plan de proyecto para aprobación de la dirección: el SGSI es una tarea permanente, primer paso es promover su diseño e implementación, tiempo, personal, recursos y dinero. Es importante utilizar herramientas, software de gestión de proyectos.

  Después de esto es poner en cintura a la alta dirección que se involucren en el proyecto, por son ellos que autorización el plan y su operación y sobre todo el presupuesto para mitigar los riesgos resultantes del análisis de riesgos.

  La dirección debe proporcionar evidencias donde se ve comprometidos con la implementación del SGSI invocando a la norma ISO 27001:2013; deben establecer la política de seguridad de la información, establecer objetivos, asignar personal, documentación, responsabilidades, tener buena comunicación, recursos y nivel bajo de riesgos.

- Fase 2: alcance, limites, y políticas del SGSI

  - Que es el alcance: podemos definir que el alcance es lo que delimita el proceso de gestión de riesgos y es el foco de la implementación del SGSI.

    Esto establece la función del negocio y sirve para las entidades que tengan varias sedes y esto reduce tiempo y recursos.

    Es importante establecer el alcance, se recomienda utilizar matrices que permitan cruzar información con los procesos y dominios establecidos en la norma ISO 27001:2013 en el anexo A y cuales son aplicables a la organización.

    Finalmente, el resultado del alcance es una sentencia que resume lo que se va a proteger en la organización y es una parte del documento de certificación que se entregan aquellas entidades que puedan cumplir con este requisito.

  - Como podemos definir las políticas y objetivos de seguridad: existen muchas definiciones sobre esto, pero revisando diferentes autores la definición más exacta es el reflejo de lo que presenta la organización y que quiere hacer sobre la seguridad de la información en base a la normatividad vigente y su reglamentación apoyado por el compromiso de la dirección.

    La política es una directriz que nos ayuda con los objetivos, esto se encuentra contemplado en la norma ISO 27002. Lo más importante es que la política es una sola y de esa política podemos especificar distintos niveles como por

ejemplo política de backups, de accesos, de uso de dispositivos móviles, entre otros.

Hablemos de los objetivos de seguridad, se tiene que aclarar los tipos de objetivos que contempla un SGSI: generales del sistema y de control de los cuales son resultados de la valoración de riesgo. Se debe definir inicialmente el objetivo general de la implementación del SGSI.

- Aprobación de la dirección: el numeral 5.1 de la norma ISO 27001:2013 dice que la dirección debe tener compromiso y el apoyo que hace para establecer las políticas y objetivos de seguridad de la información acorde con la dirección estratégica de la empresa.

- Fase 3: observación de los requisitos de la seguridad de la información

La norma ISO 27003 establece requisitos de la seguridad de la información los cuales son cinco elementos:

- ✓ Identificación de los activos más importantes
- ✓ Visión de la organización y sus efectos futuros en base al procesamiento de la información
- ✓ Formas actuales de procesamiento de información
- ✓ Normatividad vigente, clientes proveedores
- ✓ Toma de conciencia, capacitaciones, formación

Esto justifica la necesidad de implementar un SGSI en la empresa

- Activos identificados dentro del alcance del SGSI: la mayoría de las empresas cuentan con muchas cantidades, variedades y estrategias de activos tecnológicos. Por esto se hace difícil la tarea de identificar y clasificar dichos activos. La norma ISO 27005 nos indica que hay dos tipos de activos: primarios y soportes.

  Por eso se clasifican los activos de acuerdo con niveles de seguridad y criticidad, e identificar quien es el dueño de ese activo y el responsable de su seguridad.

- Fase 4: gestión de riesgos y planificación del tratamiento de riesgos

  El eje principal del SGSI, referente en la norma ISO 27005, pero existen otros modelos que se pueden utilizar para esto que son MAGERIT hablado anteriormente, MEHARI, OCTAVE, CRAMM.

- Establecer el contexto: primera fase que prepara los elementos del proceso de gestión de riesgos de seguridad de la información, iniciando desde el alcance, políticas, objetivos y parametrización de la evaluación del riesgo.

  Esta actividad se lleva a cabo se requiere establecer parámetros de evaluación, que deben ser fáciles de utilizar para la implementación del SGSI, estos parámetros de referencia son los siguientes:

  - ✓ Parámetros de probabilidad: tabla de frecuencias de las posibles amenazas con sus respectivos niveles de tres a cinco rangos. Con su valor de referencia, escala lineal y respectivo nombre con el fin de establecer valoraciones de cuantas veces ocurre o llegase a ocurrir en un determinado periodo.

  - ✓ Parámetros de impacto: las amenazas pueden ser graves que la cantidad de dinero que se pierde puede llegar a ser un evento menor, ya que de estos surgen diferentes eventos y puede afectar a toda la empresa.

  - ✓ Determinación de la vulnerabilidad: se establecen medidas para estimar el impacto de la amenaza para la empresa. Que pasaría y afectaría la información en los términos de confidencialidad, integridad y disponibilidad.

  - ✓ Criterios del riesgo: este punto permite establecer el deseo que tiene la empresa y define los parámetros para determinar si un riesgo es aceptable. La empresa determina lo que ese suficientemente seguro esto es lo que delimita el nivel de seguridad y sus recursos principales y esfuerzo para mantenerse. Los parámetros de aceptabilidad del riesgo es la mayor dificultad para determinar condiciones de seguridad, hay muchos intereses del personal por eso el equipo de SGSI con la alta dirección, acepte el riesgo en forma razonable.

  - ✓ Valoración del riesgo: de acuerdo con la norma ISO 27005 contempla tres escenarios:

    - Identificación de escenarios de riesgo.
    - Estimación de riesgo.
    - Evaluación de riesgo.

- Fase 5: diseño del SGSI

  - Documentación del sistema: El SGSI debe tener una información documentada que cumpla con lo establecido en la norma ISO/IEC 27001,

esto surge a partir de la implementación de las distintas fases. A continuación, se detalla un resumen de la información a documentar según lo estipulado en el SGSI.

Implementación del tratamiento de riesgo: la alta dirección aprueba el tratamiento de riesgo asignando los recursos pertinentes, con su respectivo mantenimiento de los controles. Esto permite garantizar niveles de seguridad aceptables dentro de la organización.

Por eso se tiene que llevar un permanente seguimiento y monitoreo de los controles y escenarios que puedan ocurrir con el fin de mantener el SGSI con las realidades de la organización.

Seguimiento y monitoreo de la información: el manual establece es su numeral 9, de la norma ISO/IEC 27001:2013, por medio de una supervisión, análisis y medición el desempeño se realiza por medio de una evaluación del sistema con sus respectivas auditorias y aprobación de la dirección.

Todo esto se realiza mediante indicadores definidos desarrollados por el SGSI a nivel general, esto permite evaluar la eficacia, la gestión de riesgos de los diferentes controles de la aplicabilidad definida por el sistema.

Se debe tener en cuenta tres normas de suma importancia con el fin de tener un proceso de auditoria:

- ✓ ISO 19011:2011
- ✓ ISO/IEC 27007:2011
- ✓ ISO/IEC TR-27008

Para finalizar la revisión es pertinencia de la alta dirección. Esto se realiza cada año con el fin de dar suficiencia a los objetivos y eficacia de la ejecución. Estos resultados se obtienen mediante auditorias realizada durante el periodo.

8.5 DISEÑO DE UN SGSI PARA EL CENTRO DE TERAPIAS INTEGRALES MISALUD S.A.S

8.5.1 Inventarios de Activos

Toda empresa debe proteger los tres pilares de la información con el fin de asegurar la continuidad del negocio no importa la actividad social de la empresa. Para esto vamos a realizar un inventario de los activos implementando MAGERIT la cual pueden observar a continuación:

Tabla 6: Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013

No.	DATOS DEL ACTIVO DE INFORMACION			TIPO									
	Nombre del activo de información	Proceso propietario del activo	Responsable	[D] DATOS	[K] CLAVES CRIPTOGRAFICAS	[S] SERVICIOS	[SW] SOFTWARE	[HW] EQUIPAMENTO INFORMÁTICO	[COM] REDES DE COMUNICACIONES	[Media] SOPORTE DE INFORMACIÓN	[AUX] EQUIPAMENTO AUXILIAR	[L] INSTALACIONES	[P] PERSONAL
1	[SA_HEALTH SYSTEM CONTABILIDAD]	Contabilidad	Olga Serpa				X						
2	[HW_ROUTER]	Sistemas	Jose vila					X					
3	[HW] SERVIDORES	Sistemas	Jose vila			X							
4	[HW] COMPUTADORES	Sistemas	Jose vila					X					
5	[HW] PORTATILES	Sistemas	Jose vila					X					
6	[HW] IMPRESORAS Epson L375	Sistemas	Jose vila					X					
7	[HW] ESCANERES	Sistemas	Jose vila					X					
8	[SW] SISTEMAS OPERATIVOS	Sistemas	Jose vila				X						
9	[SW] OFFICE	Sistemas	Jose vila				X						
10	[COM] SWITCHES	Sistemas	Jose vila						X				
11	[COM] ROUTERS	Sistemas	Jose vila						X				
12	[L] CENTRO DE DATOS Y CABLEADO	Sistemas	Jose vila						X				
13	[COM]PUNTOS DE ACCESO A LA RED	Sistemas	Jose vila						X				
14	[P] EMPLEADOS	Sistemas	Jose vila										X
15	[SW] BASES DE DATOS	Sistemas	Jose vila				X						
16	[AUX] UPS	Sistemas	Jose vila								X		
17	[MEDIA] INFORMACION DIGITAL	Sistemas	Jose vila							X			
18	[MEDIA] ADMINISTRADOR DBA	Sistemas	Jose vila							X			
19	[D] DOCUMENTOS	Sistemas	Jose vila	X									
20	[MEDIA]CORREOS ELECTRONICOS	Sistemas	Jose vila							X			

21	[SW] SOFTWARE HEALTH SYSTEM	Sistemas	Jose vila				X						
22	[HW] DISCO DUROS	Sistemas	Jose vila					X					
23	[HW] MEMORIAS	Sistemas	Jose vila					X					

Fuente: Matriz de análisis de riesgos

8.5.2 Valoración

Tabla 7: Valoración del Riesgo

	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Matriz de análisis de riesgo

8.5.3 Valoración de los activos cualitativa

Observar Anexo 2: Levantamiento de la Información en donde está el inventario de activos y la clasificación de estos.

8.5.4 Valoración de los activos cuantitativa

De acuerdo con el inventario realizado realizamos una valoración de los activos cuantitativo con el fin de observar el riesgo según la escala de la Tabla 8 con el fin de determinar su fuerza e impacto dentro de la organización.

Tabla 8: Valoración cuantitativa

Resumen de Valoración de Riesgos de los Activos							
Nombre	**Riesgo**	**AUTENTICIDAD**	**TRAZABILIDAD**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**VALOR**
[SA_HEALTH SYSTEM CONTABILIDAD]	APRECIABLE	9	20	15	9	9	12

[HW_ROUTER]	BAJO	4	4	4	4	25	8
[HW] SERVIDORES	IMPORTANTE	9	4	25	15	25	16
[HW] COMPUTADORES	APRECIABLE	4	20	4	20	9	11
[HW] PORTATILES	APRECIABLE	9	9	9	20	9	11
[HW] IMPRESORAS Epson L375	APRECIABLE	9	9	9	20	9	11
[HW] ESCANERES	APRECIABLE	9	9	9	20	9	11
[SW] SISTEMAS OPERATIVOS	APRECIABLE	4	20	4	20	9	11
[SW] OFFICE	BAJO	4	4	4	4	25	8
[COM] SWITCHES	BAJO	4	4	4	4	25	8
[COM] ROUTERS	BAJO	4	4	4	4	25	8
[L] CENTRO DE DATOS Y CABLEADO	IMPORTANTE	15	15	15	15	25	17
[COM]PUNTOS DE ACCESO A LA RED	IMPORTANTE	20	15	15	20	25	19
[P] EMPLEADOS	APRECIABLE	15	15	9	15	4	12
[SW] BASES DE DATOS	IMPORTANTE	20	20	20	20	20	20
[AUX] UPS	APRECIABLE	15	15	15	15	15	15
[MEDIA] INFORMACION DIGITAL	IMPORTANTE	20	20	20	20	20	20
[MEDIA] ADMINISTRADOR DBA	IMPORTANTE	20	20	20	20	20	20
[D] DOCUMENTOS	IMPORTANTE	20	15	9	9	25	16
[MEDIA]CORREOS ELECTRONICOS	APRECIABLE	9	9	9	15	20	12
[SW] SOFTWARE HEALTH SYSTEM	IMPORTANTE	20	20	20	20	20	20
[HW] DISCO DUROS	APRECIABLE	9	9	9	15	20	12

[HW] MEMORIAS	APRECIABLE	9	9	9	15	20	12

Fuente: Matriz de análisis de riesgo

8.5.5 Análisis de Riesgos y tratamiento de los riesgos

En el Anexo 3 de este proyecto observamos las amenazas, vulnerabilidades presentadas, la probabilidad de dicha vulnerabilidad, el cálculo del riesgo, su nivel de criticidad, clasificación de la gestión, riesgo residual, criticad residual y los niveles de aceptación.

8.5.6 Informe de Riesgos

Realizado el análisis de riesgos del Anexo 3 podemos observar que existen activos del Centro de Terapias Integrales MISALUD S.A.S. que son calificados con riesgos importantes y tienen una gran probabilidad de ser críticos como en el caso de los servidores, punto de accesos a la red, bases de datos, documentos. Esto puede generar perdida de la información, divulgar los datos confidenciales, daños en el servidor, bases de datos manipuladas, virus y cierre de la empresa.

Los activos de redes también están calificados como un riesgo importante y pasar a critico se pudo observar que hay cables sueltos en los pisos, estos son más por negligencia del personal de la empresa. El software de la empresa está en un servidor de poca confianza y descontinuado. Por eso es necesario implementar las políticas de seguridad con el fin de proteger los activos, cero riesgos e impacto mínimo.

Equipos en condiciones precarias sin la temperatura correspondiente, expuesto a humedad, UPS está en buen estado, pero no es lo recomendable cables sueltos de energía, equipos con permiso de administrador, servidor manipulables por el personal lo cual puede ocasionar perdida de la información.

La empresa es deficiente en su personal poco capacitado tanto en la parte administrativa como la de sistemas ya que tienen que ser conscientes de la información que manejan que es muy delicada y estos puede ocasionar grandes pérdidas para la empresa.

Los activos por proteger son:
[HW] SERVIDORES
[L] CENTRO DE DATOS Y CABLEADO
[COM]PUNTOS DE ACCESO A LA RED

[SW] BASES DE DATOS
[MEDIA] INFORMACION DIGITAL
[MEDIA] ADMINISTRADOR DBA
[D] DOCUMENTOS
[SW] SOFTWARE HEALTH SYSTEM

Se tiene que proteger de: abuso de privilegios, fallos en las comunicaciones, usuarios de la empresa con errores de sistemas, condiciones inadecuadas, contaminación.
Como se protegen: implementando políticas de seguridad para capacitar al personal de la empresa en todos los puntos referentes de la Norma ISO 27001:2013

A continuación, hacemos un resumen de los riesgos encontrados dentro de la empresa:

Tabla 9: Tipo de amenazas

TIPO AMENAZA	AMENAZA
[N] Desastres naturales	[N1] Fuego
[N] Desastres naturales	[N2] Daños por agua
[N] Desastres naturales	[N*] Desastres naturales
[I] De origen industrial	[I1] Fuego
[I] De origen industrial	[I2] Daños por agua
[I] De origen industrial	[I*] Desastres industriales
[I] De origen industrial	[I3] Contaminación mecánica
[I] De origen industrial	[I4] Contaminación electromagnética
[I] De origen industrial	[I5] Avería de origen físico o lógico
[I] De origen industrial	[I6] Corte del suministro eléctrico
[I] De origen industrial	[I7] Condiciones inadecuadas de temperatura o humedad
[I] De origen industrial	[I8] Fallo de servicios de comunicaciones
[I] De origen industrial	[I9] Interrupción de otros servicios y suministros esenciales
[I] De origen industrial	[I10] Degradación de los soportes de almacenamiento de la información
[I] De origen industrial	[I11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	[E1] Errores de los usuarios
[E] Errores y fallos no intencionados	[E2] Errores del administrador
[E] Errores y fallos no intencionados	[E3] Errores de monitorización (log)
[E] Errores y fallos no intencionados	[E4] Errores de configuración
[E] Errores y fallos no intencionados	[E7] Deficiencias en la organización

[E] Errores y fallos no intencionados	[E8] Difusión de software dañino
[E] Errores y fallos no intencionados	[E9] Errores de [re-]encaminamiento
[E] Errores y fallos no intencionados	[E10] Errores de secuencia
[E] Errores y fallos no intencionados	[E14] Escapes de información
[E] Errores y fallos no intencionados	[E15] Alteración accidental de la información
[E] Errores y fallos no intencionados	[E18] Destrucción de información
[E] Errores y fallos no intencionados	[E19] Fugas de información
[E] Errores y fallos no intencionados	[E20] Vulnerabilidades de los programas (software)
[E] Errores y fallos no intencionados	[E21] Errores de mantenimiento / actualización de programas (software)
[E] Errores y fallos no intencionados	[E23] Errores de mantenimiento / actualización de equipos (hardware)
[E] Errores y fallos no intencionados	[E24] Caída del sistema por agotamiento de recursos
[E] Errores y fallos no intencionados	[E25] Pérdida de equipos
[E] Errores y fallos no intencionados	[E28] Indisponibilidad del personal
[A] Ataques intencionados	[A3] Manipulación de los registros de actividad (log)
[A] Ataques intencionados	[A4] Manipulación de la configuración
[A] Ataques intencionados	[A5] Suplantación de la identidad del usuario
[A] Ataques intencionados	[A6] Abuso de privilegios de acceso
[A] Ataques intencionados	[A7] Uso no previsto
[A] Ataques intencionados	[A8] Difusión de software dañino
[A] Ataques intencionados	[A9] [Re-]encaminamiento de mensajes
[A] Ataques intencionados	[A10] Alteración de secuencia
[A] Ataques intencionados	[A11] Acceso no autorizado
[A] Ataques intencionados	[A12] Análisis de tráfico
[A] Ataques intencionados	[A13] Repudio

Fuente matriz de riesgos.

8.5.7 Área TIC seguridad, objetivos y políticas

En este punto se elaborarán las políticas del Centro de Terapias Integrales MISALUD.

Generalidades: Los datos al presente es el activo más importante de una empresa eso equivale a la seguridad de dichos datos es fundamentalmente las pilas con el qué se logra los objetivos establecidos para el caso del Centro de Terapias Integrales MISALUD es prestar un servicio de salud con calidad y protección de datos personales en sus pacientes.

Objetivos: Elaborar y definir políticas basada en seguridad para el área TIC del Centro de Terapias Integrales MISALUD, las cuales van a servir como apoyo para controlar y disminuir los riesgos, impedir incidentes, mantener protección y confidencialidad, entregar un servicio eficaz en los servicios de salud y siendo una IPS pionera en SGSI.

Alcance: todas las áreas del Centro de Terapias Integrales MISALUD deben implementar las políticas de seguridad.

Responsables: el coordinador TIC es el responsable de la seguridad de la información, para implementar esta política se tienen que dar ciertas funciones y responsabilidades como elegir al garante de los sistemas y seguridad de la información, seguridad informática, contratación de personal y proveedores, área jurídica y administrativa. Los cuales organizara los siguientes comités:

- **Seguridad de información:** este comité tiene las siguientes funciones presentar los resultados al coordinador TIC donde se aprueban y modifican políticas de seguridad, las cuales deben ser cumplidas a cabalidad por todos los funcionarios del Centro de Terapias Integrales MISALUD revelar los resultados de las amenazas y riesgos. Se debe escoger un líder el cual vigilará las funciones de este comité, y dicho líder debe solicitar aprobación al coordinador TIC.

- **Control interno:** realizar auditoria bimestrales a las políticas de seguridad y el cumplimiento de estas, con su respectiva documentación en caso dado de encontrar algún hallazgo se sugiere como solucionar y brindar su apoyo al coordinador TIC.

Funciones de los responsables:

- **Sistema y seguridad de la información:** tiene como función definir los permisos a los funcionarios de la IPS, catalogar del nivel más alto al más bajo la información conforme a la privacidad de está, realizar copias de información semanales, todas estas funciones deben ser documentadas de acuerdo con el SGC.
-
- **Seguridad informática:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS todas estas funciones deben ser documentadas de acuerdo con el SGC.

- **Contratación personal y proveedores:** al momento de contratar personal y proveedores se deben de capacitar en las políticas de seguridad las cuales se deben efectuar en un 100%. En caso de actualización realizar la capacitación de estas.

- **Jurídica y administrativa:** incluir en los contratos de prestación de servicios que el personal y proveedor de cumplir las políticas de seguridad.

- **Garante de la información:** cumplir con los tres pilares de la información.

Política: en este punto se definen las muestras en base a la seguridad TIC del Centro de Terapias Integrales MISALUD.

- **Organizar la seguridad:** realizar la guía de la seguridad de la información, con el fin de realizar la implementación de esta.

- **Clasificar y controlar activos:** proteger de la mejor manera los activos de la IPS con un orden jerárquico.

- **Controlar el acceso:** la información de orden confidencial se debe restringir ya que es valiosa para la IPS.

- **Mantenimiento y desarrollo de los sistemas:** en los aspectos TIC de la IPS desarrollar modelos de seguridad y realizar una guía para el mantenimiento de los sistemas.

- **Administrar operaciones:** las fallas que se ocasionen se deben de neutralizar para que no afecte el proceso de producción de la IPS.

- **Seguridad de los funcionarios (usuarios):** el error humano siempre está a la orden del día, mal manejo de la información y daños producidos a los

sistemas, se deben minimizar los riesgos y capacitar a los funcionarios para su buen uso.

- **Seguridad en la organización:** robos, daños y acceso no autorizado tanto virtual como físicamente a la organización deben ser impedidos.

- **Cumplir políticas:** como su misma palabra lo dice cumplir en un 100% lo dicho anteriormente, en caso dado de no cumplir se generarán las sanciones correspondientes

- **Rublo:** el coordinador TIC debe gestionar un rublo en el presupuesto anual para la seguridad de la información.

8.5.8 Organizar la seguridad de la información

Generalidades: Formar que seguridad de información es uno de los objetivos vitales para el Centro de Terapias Integrales MISALUD.

Objetivos: Instituir, registrar y administrar la información dentro de la organización.

Alcance: todas las áreas del Centro de Terapias Integrales MISALUD deben implementar las políticas de seguridad.

Responsables: el coordinador TIC es el responsable de la seguridad de la información, para implementar esta política se tienen que dar ciertas funciones y responsabilidades, el comité de seguridad de la información de cumplir sus respectivas funciones:

- **Seguridad de información:** este comité tiene las siguientes funciones presentar los resultados al coordinador TIC donde se aprueban y modifican políticas de seguridad, las cuales deben ser cumplidas a cabalidad por todos los funcionarios del Centro de Terapias Integrales MISALUD revelar los resultados de las amenazas y riesgos, actualización en normatividad o en la organización deben hacerse conocer por el gerente.

- **Control interno:** realizar auditoria bimestrales a las políticas de seguridad y el cumplimiento de estas, con su respectiva documentación en caso dado de encontrar algún hallazgo se sugiere como solucionar y brindar su apoyo al coordinador TIC.

Funciones de los responsables:

- **Seguridad informática:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS todas estas funciones deben

ser documentadas de acuerdo con el SGC. En caso de solicitar asesoría de profesionales en el tema se debe elaborar un plan de trabajo con el fin de realizar la implementación.

- **Administración del sistema:** el coordinador TIC con el visto bueno de la gerencia debe gestionar los recursos propios para todo lo referente al área TIC y seguridad de la información incluyendo asesoría de expertos sobre el tema.

- **Contratación personal y proveedores:** al momento de contratar personal y proveedores se deben de capacitar en las políticas de seguridad las cuales se deben efectuar en un 100%. En caso de actualización realizar la capacitación de estas.

- **Jurídica y administrativa:** incluir en los contratos de prestación de servicios que el personal y proveedor de cumplir las políticas de seguridad.

Política: en este punto se definen las muestras en base a la seguridad TIC del Centro de Terapias Integrales MISALUD.

- **Coordinaciones internas de la seguridad de la información del Centro de Terapias Integrales MISALUD:** la implementación de las políticas debe estar garantizado por comité el cual brindara su apoyo para tomas las medidas necesarias, dicho comité está conformado por:

Tabla 10: Comité de Seguridad de la Información

Área o Dependencia	Representante
Coordinador TIC	XXXX
Seguridad de la información	XXXX
Contratación personal y proveedores	XXXX
Jurídica y administrativa	XXXX

Fuente: el autor

- **Sus funciones son las siguientes:**

  - ✓ Revisar y proponer políticas de seguridad al gerente de Centro de Terapias Integrales MISALUD.
  - ✓ Identificar los riesgos de la IPS con el fin de mitigar estos y generar los reportes de las vulnerabilidades.
  - ✓ Documentación con el visto bueno del SGC referente a eventualidades de seguridad.
  - ✓ Soluciones de primera clase con el fin de mitigar las vulnerabilidades para favorecer la seguridad.

- ✓ Planificar el proceso y que este sea incluido en los planes de mejora de la IPS.
- ✓ Controlar y garantizar la implementación de la seguridad.

- Establecer responsabilidades del comité de seguridad: La Gerencia establecerá responsabilidades en base a la seguridad de la información en cabeza del Coordinador TIC, el cual es el principal responsable del Centro de Terapias MISALUD, y responsable del cumplimiento de lo tratado en la presente política.

  Asignación de responsabilidades, que deben quedar debidamente documentada por el SGC y aprobadas por el Comité de Seguridad de la información de acuerdo con la siguiente tabla:

Tabla 11: Responsables Seguridad de la Información

PROCESO	**RESPONSABLE**
Seguridad del Software	XXXX
Seguridad de las comunicaciones (red y servidores)	XXXX
Seguridad en el desarrollo y mantenimiento de sistemas	XXXX
Seguridad operacional	XXXX
Control de Acceso	XXXX
Seguridad Física	XXXX
Seguridad de la Información	XXXX
Seguridad de Usuarios (personal)	XXXX

Fuente: El autor

- **Responsables de la seguridad de la información del Centro de Terapias Integrales MISALUD:**

Tabla 12: Encargados seguridad de la Información

Información	Propietario	Recursos Asociados	Procesos Involucrados	Administrador

Fuente: Modelo de política de seguridad para organismo de la administración pública nacional

- **Autorizar para procesar servicios de información:** El responsable de la seguridad de la información debe procesar y autorizar los servicios nuevos con el fin de tener detalle del usuario; se debe implementar todo lo referente a TIC teniendo en cuenta las condiciones del sistema actual, se debe elaborar un protocolo de acceso de cómputos a la IPS a estos se le deben hacer los debidos controles.

- **Acuerdo de privacidad:** al momento de elaborar los contratos a los funcionarios o proveedores estos deben incluir el acuerdo de privacidad con el fin de proteger la información, esto es una manera legal de hacerlo. Capacitar el uso de esta enseñar cual es el responsable, condicionar el buen uso del acuerdo y el tiempo estipulado según la normatividad.

- **Autoridades de seguridad y contacto con ellas:** La IPS debe tener relación con las autoridades en delitos informáticos en caso dado de presentar una amenaza, se debe de identificar el líder de esta autoridad o persona encargada.

- **Intereses con grupos especiales:** asesorías en normatividad vigente, nuevos ataques, empresas de seguridad con el fin de estar actualizado en nuevos ataques se recuerda que los ataques mejorar cada día más.

- **Control interno:** realizar auditoria bimestrales a las políticas de seguridad y el cumplimiento de estas, con su respectiva documentación en caso dado de encontrar algún hallazgo se sugiere como solucionar y brindar su apoyo al coordinador TIC.

  El responsable de control interno puede brindar soluciones al gerente de la IPS en caso dado si se debe contratar un tercero especializado se debe documentar de acuerdo con los formatos del SGC.

- **Seguridad informática equipos externos:** políticas de equipos externos se debe elaborar un formato con el fin de controlar los equipos externos de la siguiente manera:

  - ✓ Acuerdo con la autoridad externa con el fin de compartir información
  - ✓ Lista de chequeo con los controles en caso de pasar toda la Check list generar acceso a las instalaciones.
  - ✓ Que servicios va a utilizar la parte externa.
  - ✓ Funciones a realizar la parte externa en la IPS.
  - ✓ Que documentación utilizar la parte externa y cuanto es su valor.
  - ✓ Proteger dicha documentación.
  - ✓ Elaborar protocolo de cómo utilizar la documentación.
  - ✓ Divulgar la normatividad vigente referente a lo que debe cumplir la parte externa.
  - ✓ Elaborar protocolo de fallos y divulgar.
  - ✓ Elaborar contrato con todo lo referente a seguridad de la información, sus funciones y cumplimiento, en caso de no cumplir indicar cuales son las discrepancias legales.

Todos deben cumplir estos criterios en un 100% incluyendo funcionarios proveedores internos y externos de cualquier clase de índole.

8.5.9 Gestionar activos

Generalidades: ya con el inventario realizado y su respectiva clasificación se elaborará la política.

Objetivos: proteger los activos del Centro de Terapias Integrales MISALUD basado en las políticas con el fin de que sean protegido de la mejor manera.

Alcance: todas las áreas del Centro de Terapias Integrales MISALUD deben implementar las políticas de seguridad.

Responsables: el coordinador TIC es el responsable de la gestión del activo él puede colocar a cargo a un responsable para garantizar los tres pilares de la información y el coordinador TIC debe realizar seguimiento y que sea correcto el uso adecuado de los permisos.

Política: en este punto se definen las muestras en base a la seguridad TIC del Centro de Terapias Integrales MISALUD.

- **Realizar inventarios de activos:** bimestral se debe realizar inventarios con su respectiva clasificados con su respectiva jerarquía, elaborar el formato con el responsable de la información y esta se debe tener documentada.

- **Clasificar la información:** en base a estos criterios de seguridad se debe clasificar la información.

Ver Anexo 2: Análisis de amenazas, vulnerabilidad y nivel de riesgo.

El encargado verificara y clasificara los criterios pertinentes con el fin de identificar los elementos.

- Rotular información: elaborar guías con el fin de rotular la información física y virtual para definir qué tal critico es.

8.5.10 Contratación personal y proveedores

Generalidades: al momento de contratar personal y proveedores se deben de capacitar en las políticas de seguridad las cuales se deben efectuar en un 100%. En caso de actualización realizar la capacitación de estas.

Objetivos: minimizar el error humano siempre está a la orden del día, mal manejo de la información y daños producidos a los sistemas, se deben minimizar los riesgos y capacitar a los funcionarios para su buen uso.

Alcance: todas las áreas del Centro de Terapias Integrales MISALUD deben implementar las políticas de seguridad.

Responsables:

- **Funcionarios de recursos humanos:** los cuales son los encargados de contratar al personal, al momento de realizar la inducción con un funcionario elegido por el coordinador TIC, deben de divulgar el acuerdo de privacidad y cumplir con todas las políticas de seguridad.

- **Jurídica y administrativa:** incluir en los contratos de prestación de servicios que el personal y proveedor de cumplir las políticas de seguridad, el acuerdo de privacidad e indicar cuales son las consecuencias de no cumplirlas.

- **Seguridad informática:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS si es necesario asesorías de personas expertas en el tema con el fin de que se utilicen correctamente las políticas de seguridad de la IPS.

Política: en este punto se definen las muestras en base a la seguridad TIC del Centro de Terapias Integrales MISALUD.

- **Selección del personal a contratar:** realizar el manual de funciones de cada uno de los cargos de la IPS con el fin de verificar que controles informáticos va a utilizar la persona día a día en la IPS.

  Su perfil se revisará siempre y cuando la persona firme el acuerdo de privacidad entre las partes, en caso de ser positivo se revisa redes sociales, su vida crediticia y se verificará actas de grado y referencias personales. Esto se clasifica en una lista de chequeo.

  Al momento de realizar el contrato esto aplica para funcionario y terceros ellos deben conocer detalladamente las condiciones laborales con un funcionario del área TIC el cual debe enseñar las condiciones de seguridad informática de la IPS. Dicho contrato debe ser según lo establece la normatividad vigente y firmado debidamente por todas las partes.

- **Vigencia del contrato:** la gerencia exigirá que sus funcionarios y terceros cumplan con el 100% de las políticas de seguridad de la IPS. Esto se logra mediante capacitaciones presenciales o virtuales, en las cuales se pueden realizar actividades con el fin de motivar al personal. Al final ellos deben de estar de acuerdo con los requisitos y contextos del contrato.

- **Formación y capacitación:** esto parte es muy importante se debe elaborar un plan de trabajo aprobado por la gerencia con el fin de capacitar a los

funcionarios y terceros de la empresa. Puede ser virtual o presencial, elaborar videos mostrando la política de seguridad. En caso de haber cambios esta se notificará a todos los funcionarios y terceros.

Las capacitaciones deben ser realizadas por funcionarios del área TIC con el fin de que resalten la importancia de cumplir las políticas de seguridad dentro de la organización. También debe explicar cómo detectar falas, amenazas y en caso de alguna anomalía comunicar a la autoridad competente.

La IPS verificara el cumplimiento mediante aplicativos de seguridad y también gestionar en cada puesto de trabajo la política de seguridad.

El funcionario debe cumplir la política y el acuerdo de privacidad en un 100%.

Los terceros o proveedor que quebranten las políticas de seguridad se notificaran a la autoridad competente con el fin de abrir un expediente disciplinario de acuerdo con lo estipulado en los estatutos de la IPS.

- **Cambio o terminación del contrato:** al momento de la notificación de recursos humanos por un cambio o terminación del contrato el coordinador TIC suspenderá de manera inmediata todo acceso del funcionario y desactivara todas las cuentas que este tiene con la organización. Se organizará una reunión con acta de entrega por parte del funcionario en donde devuelvo todos los hardware y software que fueron prestados durante sus funciones en buen estado. En caso de alguna anomalía se notificará a la autoridad competente. En caso de cambio de contrato el coordinador TIC gestionara este proceso.

8.5.11 Ambiente físico de la organización

Generalidades: el ambiente físico hay que tener en cuenta varias condiciones: protección física, protección de equipos, protección de daños. Ambiente físico de las instalaciones con su respectiva seguridad y protocolos.

Objetivos: impedir daños en las instalaciones físicas del área TIC con el fin de evitar amenazas para la información de la IPS.

Alcance: todas las áreas del Centro de Terapias Integrales MISALUD deben implementar las políticas de seguridad en sus equipos y periféricos.

Responsables:

- **Seguridad informática:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS todas estas funciones deben

ser documentadas de acuerdo con el SGC. Implementar en los servidores de la IPS los controles necesarios. En caso de solicitar asesoría de profesionales en el tema se debe elaborar un plan de trabajo con el fin de realizar la implementación.

- **Seguridad de información:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS si es necesario asesorías de personas expertas en el tema con el fin de que se utilicen correctamente las políticas de seguridad de la IPS.

Política: en este punto se definen las muestras en base a la seguridad TIC del Centro de Terapias Integrales MISALUD.

- **Contorno físico:** el comité encargado elaborara un protocolo donde definen el contorno de seguridad para el área TIC el cual se accederá con huellas ya que esta es un área critica de la IPS y en las cuales se debe cumplir estos criterios:

  - ✓ Precisar el contorno de seguridad
  - ✓ Barreras de acceso a la información
  - ✓ Personal autorizado puede entrar con huella al área.

- **Acceso físico:** el comité encargado elaborara un protocolo donde definen el cómo es el ingreso al acceso físico del área TIC de la IPS y en las cuales se debe cumplir estos criterios:

  - ✓ Lista de chequeo del personal que entra al área, se aclara que este acceso debe ser limitado.
  - ✓ Carné visible de la IPS y documento en la cual sea catalogado como funcionario autorizado.
  - ✓ Revisar periódicamente la lista de chequeo del personal que entra.
  - ✓ Actualizar la lista de chequeo de la persona que entra.

- **Seguridad en las oficinas e instalaciones:** Seguridad perimetral con el fin de proteger de los perímetros físicos, instrucciones, instalaciones sensibles esto es importante para evitar robo o desaparición de la red de la empresa. Se debe de contratar una empresa de vigilancia mediante la modalidad de licitación en la cual debe cumplir con todos los requisitos pertinentes.

- **Ubicación copias de seguridad, equipos, hardware y software:** los cuales deben de estar protegidos y deben tener acceso único para evitar desastres naturales por lo tanto se deben de cumplir los protocolos de acceso físico a las instalaciones. El aseo se vigilaría para verificar que no se maltrate ningún activo.

- **Planta eléctrica:** garantizar en caso de fallas el suministro de energía una planta eléctrica en cada uno de los puntos de la IPS en caso de tenerlos con el fin de garantizar que los equipos se dañen, si es necesario de implementar redes eléctricas reguladas y UPS para los equipos.

- **Cableado eléctrico:** los cables deben de ser seguros y de acuerdo con lo estipulado en las normas internacionales UNE-EN 50525 e IEC 60227. Además, cumplen con el Reglamento Electrotécnico ITC-BT: 9/20/26/27/30/41 y con la Normativa Europea que se aplica a los cables eléctricos CPR (Construction Product Regulation).[17]

- **Mantenimiento de los activos:** elaborar un plan de trabajo bimestral a los equipos de la IPS. Este mantenimiento debe ser preventivo y firmados por cada uno de los funcionarios de la IPS a los cuales le harán el mantenimiento. Esto debe ser documentado por el SGC y tener inventarios con su respectiva codificación de los dispositivos.

- **Remanufactura de los equipos:** elaborar protocolo de remanufacturacion de equipos para la posible utilización de este más adelante, realizar copia de información del equipo y seguir las condiciones del acceso físico. En caso dado de que un equipo no sirva para ser reutilizada este debe ser destruido inmediatamente.

8.5.12 Comunicaciones y operaciones

Generalidades: gerencia debe garantizar los tres pilares de la información que se reciben por los diferentes medios de comunicación.

Objetivos: elaborar protocolos con el fin de mitigar la propagación de virus, software malicioso, como bien saben son categoría alta para los activos de la IPS, el coordinador TIC designara responsables para esta práctica.

Alcance: todas las áreas del Centro de Terapias Integrales MISALUD deben implementar las políticas de seguridad en sus equipos y periféricos.

Responsables:

- **Seguridad informática:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS he implementar la política en los servidores de la IPS, si es necesario asesorías de personas expertas en el tema con el fin de que se utilicen correctamente las políticas de seguridad de la IPS y seguir las siguientes condiciones:

[17] Cables y concejos eléctricos: Cables para instalaciones domesticas [en línea]. [Consultado: 29 de abril de 2020] Disponible en https://www.topcable.com/blog-electric-cable/tag/instalaciones-domesticas/.

- ✓ Documentación de cambios y mantenimiento.
- ✓ Reporte de incidentes mediante aplicativos de seguridad.
- ✓ Políticas de control de correo electrónico, bloquear redes sociales y páginas de internet mediante el aplicativo de seguridad.
- ✓ Antivirus licenciado con su respectivo seguimiento y capacitación.
- ✓ Definir políticas de contraseña y cambios mensualmente.
- ✓ Copias de seguridad periódicas.
- ✓ Recursos para actualizaciones y software nuevos.
- ✓ Herramienta de seguimiento de actividades.
- ✓ Destrucción de periféricos siempre y cuando ya no sirvan.
- ✓ Documentación por el SGC.

- **Jurídica y administrativa:** incluir en los contratos de prestación de servicios que el personal y proveedor de cumplir las políticas de seguridad, el acuerdo de privacidad e indicar cuales son las consecuencias de no cumplirlas.

- **Área TIC:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS si es necesario asesorías de personas expertas en el tema con el fin de que se utilicen correctamente las políticas de seguridad de la IPS.

Política: en este punto se definen las muestras en base a la seguridad TIC del Centro de Terapias Integrales MISALUD.

- **Protocolos operativos:** debe cumplir con las siguientes condiciones:

  - ✓ **Documentación de los procesos operativos:** al momento de realizar una actualización del Sistema Operativo el aplicativo de seguimiento debe realizar un reporte de cada uno de las actualizaciones y modificaciones del sistema.

  - ✓ **Documentación de cambios de los procesos operativos:** gestionar los cambios operativos, verificar si el proceso fue realizado correctamente, en caso de fallos realizar un informe de lo sucedido.

  - ✓ **Documentación de manejos de los incidentes:** el coordinador TIC elaborar protocolos de incidentes de seguridad: las debilidades del sistema de información y los eventos que ocurran se tiene que comunicar inmediatamente

para que se tome una acción correcta en el momento justo, esto debe de estar asegurado mediante procedimientos y controles.

- **Aprobación de sistemas operativos:** debe cumplir con las siguientes condiciones:

  - ✓ **Documentación de la capacidad:** al momento de realizar una actualización del Sistema Operativo el coordinador TIC debe realizar su evaluación.

  - ✓ **Documentación de aprobación:** gestionar los cambios operativos, verificar si el proceso fue realizado correctamente.

- **Software malicioso protección:** debe cumplir con las siguientes condiciones el coordinador TIC y el responsable de la seguridad:

  - ✓ Políticas de no instalación de software y descargas de programas a los equipos estos deben ser autorizados por la autoridad competente.
  - ✓ Verificar contenido de software.
  - ✓ Pruebas al software antes de ser lanzado a producción y libre de virus.
  - ✓ Mediante aplicativos de seguridad realizar informes de software.
  - ✓ Capacitar al personal sobre el software nuevo a utilizar.

- **Mantenimiento:** debe cumplir con las siguientes condiciones:

  - ✓ **Documentación de la información:** definir protocolos de protección de información referente a copias de seguridad de cómo se realizan donde se almacenan, su ubicación debe ser especial de acuerdo con lo definido en el entorno físico.

  - ✓ **Documentación de las actividades:** gestionar los cambios de las actividades del sistema detalladamente.

  - ✓ **Documentación de fallas:** gestionar los cambios de las actividades del sistema detalladamente, en caso de fallas realizar el informe correspondiente.

- **RED:** elaborar protocolos de seguridad de la red de datos con el fin de mitigar amenazas y debe cumplir con las siguientes condiciones:

- ✓ Documentación del proceso de la administración de la red de la IPS.
- ✓ Controles con el fin de asegurar los tres pilares de la información.
- ✓ Actividades de gestión y supervisión de los controles se estén aplicando correctamente.

- **Periféricos de almacenamiento:** debe cumplir con las siguientes condiciones el coordinador TIC y el responsable de la seguridad deben garantizar que cualquier periférico tenga los controles adecuados en caso dado de que no los cumplan destruir el Periférico para evitar amenazas de la información.

    - ✓ **Documentación de eliminar periféricos**: el coordinador TIC y el responsable de la seguridad deben garantizar que cualquier periférico tenga los controles adecuados en caso dado de que no los cumplan destruir el Periférico para evitar amenazas de la información.

    - ✓ **Documentación de manejo de información**: los funcionarios de la IPS deben seguir la política de seguridad y cumplir el procedimiento de protección de documentos, software, hardware, el coordinador TIC y el responsable de la seguridad deben garantizar que el personal no autorizado no tenga acceso a la información. Al momento de guardar la información esta debe ser conservada de la manera más segura.

    - ✓ **Documentación del sistema:** el documento aprobado por el SGC debe ser conservada de la manera más segura y su acceso restringido.

- **Permutas de software e información:** los funcionares de la IPS deben cumplir con la política de seguridad y condiciones el coordinador TIC y el responsable de la seguridad deben garantizar que el correo electrónico sea seguro. Los funcionarios no abrir mensajes desconocidos, el aplicativo de seguridad de blindar estos mensajes y enviarlos a cuarentena. Los funcionarios deben estar capacitados que por mediante correo electrónico e ingeniera social se pueden robar contraseñas, información valiosa para la IPS.

8.5.13 Control de ingreso a los sistemas de información

Generalidades: documentar la política de control de ingreso a los sistemas de información, BD, y activos vitales de la IPS, los cuales con un ingreso no autorizado pone en peligro a la organización.

Objetivos: controlar el ingreso a los sistemas de información.

Alcance: todas las áreas del Centro de Terapias Integrales MISALUD deben implementar las políticas de seguridad en sus equipos y periféricos.

Responsables:

- **Seguridad informática:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS todas estas funciones deben ser documentadas de acuerdo con el SGC. Implementar en los servidores de la IPS los controles y privilegios necesarios. Definir protocolos de ingreso a los sistemas de información y capacitar a los funcionarios para no divulgar sus contraseñas.

- **Seguridad de información:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS, parametrizar el aplicativo de seguridad con todos sus protocolos de control de ingreso a los sistemas de información realizar las pruebas específicas y realizar un ambiente de ingreso a la información como prueba de control. capacitar a los funcionarios para no divulgar sus contraseñas.

Política: en este punto se definen las muestras en base a la seguridad TIC del Centro de Terapias Integrales MISALUD.

- **Control de ingreso:** el responsable de la seguridad de información seguirá los siguientes controles:

    - ✓ Gestionar técnicas de ingreso y autenticación.
    - ✓ Red segmentada.
    - ✓ Control de puertos seguros y prueba de red.
    - ✓ Auditoria de ingresos a los sistemas.
    - ✓ Protocolos de acceso.
    - ✓ Cambios en el acceso.

- **Ingreso de usuarios administración:**

    - ✓ **Registrar usuarios:** formato de registro de usuarios con el fin de verificar los accesos, en caso de revocación del usuario indicar el motivo, identificar en el formato usuarios únicos y que no se repitan.

- ✓ **Privilegios administrativos:** solo el personal autorizado debe tener privilegios administrativos en la IPS, y se debe llevar un registro del usuario y clave, y quien lo utiliza dentro de la organización.

- ✓ **Contraseñas de acceso críticos:** para cambios en servidores y configuraciones en los aplicativos de seguridad de información. La contraseña tiene un grado más alto de complejidad.

- **Responsabilidad de los funcionarios:** las contraseñas deben de tener un protocolo exigido en el servidor mayúsculas, minúsculas y carácter especial, estas deben ser cambiadas cada mes. El funcionario al momento de no utilizar su equipo este de ser bloqueado, y el sistema cuando no detecta movimiento esté se debe de bloquear automáticamente. El correo electrónico no debe de estar abierto en caso de que no se utilice, en los celulares corporativos tenerlo con contraseña por seguridad y utilizar la doble autenticación.

- **Ingreso de control a la red:** el coordinador TIC y el responsable de la seguridad informática son los encargados de definir los protocolos de ingreso a la red, gestionar los controles autorización, procesos, doble autenticación, para conexiones externas definir el control de acceso, para conexiones remotas definir protocolo de acceso, se recomienda segmentar la red para que el momento de una falla no afectar todo el proceso ni la organización. El acceso al wifi debe ser por red de invitados y con el visto bueno del coordinador TIC. Se debe realizar mantenimiento de la red y el acceso desde afuera debe ser vigilado por un aplicativo de seguridad informática.

- **Ingreso de control al S.O:** el coordinador TIC y el responsable de la seguridad informática son los encargados de definir los protocolos de ingreso al S.O, contraseñas seguras de acceso en caso de colocar la contraseña errónea por más de tres veces esta se debe bloquear automáticamente. Protocolo de conexión segura e implementación en los servidores.

- **Ingreso a las aplicaciones:** el coordinador TIC y el responsable de la seguridad informática son los encargados de definir los protocolos de ingreso a aplicaciones internas y externas, el aplicativo de seguridad informática debe emitir informes sobre el uso de estas.

- **Informe de actividades:** el aplicativo de seguridad informática debe emitir un informe sobre el uso y acceso a los sistemas, en caso de presentar una anomalía corregir inmediatamente. Este informe debe ser revisado periódicamente por el coordinador TIC.

8.5.14 Informe de actividades de la información

Generalidades: realizar un instructivo sobre el aplicativo de seguridad informática, con el fin de verificar las políticas de acceso y seguridad a los diferentes activos para evitar amenazas y en caso de tenerlas mitigarlas inmediatamente.

Objetivos: realizar instructivo de seguridad de la información.

Alcance: todas las áreas del Centro de Terapias Integrales MISALUD deben implementar las políticas de seguridad en sus equipos y software.

Responsables:

- **Seguridad informática:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS he implementar la política en los servidores de la IPS y software, si es necesario asesorías de personas expertas en el tema con el fin de que se utilicen correctamente las políticas de seguridad de la IPS.

- **Jurídica y administrativa:** incluir en los contratos de prestación de servicios que el personal y proveedor de cumplir las políticas de seguridad, el acuerdo de privacidad e indicar cuales son las consecuencias de no cumplirlas. En caso de licenciamiento de software políticas de autor y entregas de implementación.

Política: en este punto se definen las muestras en base a la seguridad TIC del Centro de Terapias Integrales MISALUD.

- Lista de chequeo de seguridad al sistema:

  - ✓ **Requerimientos de controles de seguridad:** definir protocolos de acceso al sistema y realizar su implementación, es importante resaltar que este proceso se debe realizar de manera integral e inmediata para evitar daños futuros.

  - ✓ **Controles de seguridad en las aplicaciones:** al momento de instalar aplicaciones se deben implementar los protocolos necesarios con el fin de realizar el registro para mitigar el riesgo de pérdidas de datos.

  - ✓ **Gestión de control de datos:** reporte de gestión sobre el control de datos de entrada donde se verificará periódicamente su contenido, esto debe se realizado mediante un protocolo de seguridad y su respectivo método, además de las responsabilidades de los funcionarios.

- ✓ **Protocolo de seguridad de control de datos:** el coordinador TIC y el responsable de la seguridad deben implementar el protocolo de gestión de control de datos con el fin de verificar el registro de los datos, aplicativos, registros, mensajes de entrada y salida, esto se puede hacer con el aplicativo de seguridad informática.

- **Criptografía:**

  - ✓ **Política criptográfica:** realizar política sobre los controles de claves, datos, servicios, aplicativos, correos, acceso a sistemas de información, permuta de información, entrada y salidas de datos, el coordinador TIC y el responsable de la seguridad gestionarán el protocolo en base a las ultimas políticas criptográficas.

  - ✓ **Gestión de claves:** realizar política sobre los controles de claves, el coordinador TIC y el responsable de la seguridad gestionarán el protocolo en base a las ultimas políticas criptográficas, capacitación al personal sobre el uso de claves seguras, cambios permanentes.

- **Gestión de seguridad soporte y mantenimiento:**

  - ✓ **Control de cambios activos TIC:** documentar los cambios que se realizan los diferentes activos TIC, estos deben ser autorizados por el coordinador TIC y el responsable de la seguridad.

  - ✓ **Control de cambios S.O:** documentar los cambios que se realizan a los S.O, estos deben ser autorizados por el coordinador TIC y el responsable de la seguridad, verificar el impacto que genera.

  - ✓ **Control de cambios aplicativos:** documentar los cambios que se realizan a los aplicativos verificar las licencias y sus costos, cuando se adquiere un software cliente externos aplicar la política de adquisición de software, estos deben ser autorizados por el coordinador TIC y el responsable de la seguridad, verificar el impacto que genera.

  - ✓ **Control de cambios aplicativo de seguridad:** documentar los cambios que se realiza al aplicativo de seguridad informática, (se recomienda adquirir un aplicativo), estos

deben ser autorizados por el coordinador TIC y el responsable de la seguridad, verificar el impacto que genera.

8.5.15 Protocolo de amenazas

Generalidades: los funcionarios del Centro de Terapias Integrales MISALUD, deben conocer el protocolo de amenazas, en caso de presentar una comunicar inmediatamente al coordinador TIC y el responsable de la seguridad.

Objetivos: comunicar al encargado cualquier amenaza que atente contra la seguridad informática.

Alcance: todas las áreas del Centro de Terapias Integrales MISALUD deben implementar las políticas de seguridad.

Responsables:

- **Seguridad informática:** su principal función es garantizar la política de seguridad en todos los aspectos TIC de la IPS he implementar la política en los servidores de la IPS y software, si es necesario asesorías de personas expertas en el tema con el fin de que se utilicen correctamente las políticas de seguridad de la IPS.

- **Seguridad de información:** realizar capacitación a los funcionarios de la IPS con el fin de que conozcan el protocolo de amenazas y en caso de presentar alguna comunicar inmediatamente.

Política: en este punto se definen las muestras en base a la seguridad TIC del Centro de Terapias Integrales MISALUD.

- **Gestión de reportes sobre amenazas de seguridad:** los funcionarios deben estar atento en caso de que se presente una amenaza, el aplicativo de seguridad emite una alerta sobre una posible amenaza, el funcionario diligencia un formato el cual debe estar firmado y este debe ser enviado a los responsables de la seguridad con el fin de tomar las medidas pertinentes.

- **Gestión de mejoras de amenazas en la seguridad:** los responsables de la seguridad deben actuar inmediatamente seguir el protocolo de seguridad de esta manera:

    - ✓ **Procesos de responsabilidad:** el aplicativo de seguridad informática emitirá un reporte de incidente con el fin de evaluar el tamaño de la falla y de qué manera se violentó los tres pilares de la seguridad, se implementan el protocolo de acciones de mejoras por los responsables de la información.

- ✓ **Mejoras para evitar incidentes futuros:** el aplicativo de seguridad informática emitirá un reporte de incidente con el fin de evaluar el tamaño de la falla y de qué manera se violentó los tres pilares de la seguridad, se implementan el protocolo de acciones de mejoras por los responsables de la información y el costo de este a la IPS. Se debe evitar estos incidentes en un futuro.

- ✓ **Evidencia:** en caso de que la falla se presentó por un funcionario de la IPS se muestra las evidencias correspondientes. Estas evidencias deben ser catalogas solo para tus ojos, realizar copia de la evidencia y guardarlas de manera segura utilizando la metodología de cadena de custodia. Comunicar a Recursos Humanos y evaluar la acción a tomar al funcionario.

9. FORMACIÓN Y CAPACITACIÓN

Las políticas de seguridad son muy importantes para la Empresa ya que estas buscan proteger la información con esto garantizar la continuidad de los sistemas de aquellas vulnerabilidades presente en el día a día. Las políticas tienen que ser una cultura para la empresa un compromiso de la Gerencia para una correcta propagación, fortalecimiento y acatamiento de las políticas.

Las políticas de seguridad tienen que ser eficaces para esto los empleados de la Empresa y proveedores tienen que recibir formación y capacitación sobre ellas sobre sus objetivos y procedimientos. La formación tiene que incluir las responsabilidades, requerimientos de seguridad y enseñar el uso correcto del gobierno TI y recursos de la Empresa en general.

Cada seis meses se deben programar capacitaciones o cuando se presente cambios significativos. El personal nuevo debe recibir capacitación y materiales informativos y realizar un examen sobre el material recibido esto antes de crear perfiles en el sistema.

10. CONCLUSIONES

El Centro de Terapias Integrales MISALUD S.A.S posee problemas de que afecta su seguridad en sus servicios y estructura, por lo cual tiene un alto grado de exposición a nivel general. Se utilizaron herramientas las cuales nos ayudaron a emitir un análisis, dichas herramientas como aplicación de encuestas, observaciones directas y mediante aplicaciones se hizo prueba de análisis de la RED. Con que fin de recolectar información de primera mano, con el fin de tener conocimientos claros para definir en donde se debe de empezar para desplegar una primera fase del SGSI.

Con el análisis de riesgos realizado en estos se evidencia la mayoría de los problemas de seguridad del Centro de Terapias Integrales MISALUD S.A.S, este análisis consiente localizar todos los elementos críticos de la organización, evaluar los riesgos, observar las amenazas, mirar el impacto para cada área de seguridad, tiempos, frecuencias y determinar las acciones de mejora.

La metodología MAGERIT se utilizó para el análisis de riesgos del Centro de Terapias Integrales MISALUD S.A.S, con lo cual se documentó lo siguiente:

- Valoración cualitativa de activos.
- Inventario de activos.
- Identificación de salvaguardas de activos.
- Identificar amenazas.
- Valoración y evaluación del riesgo.

Y finalmente el informe final de calificación de riesgos en donde veremos los activos que están en riesgos y que debe ser ajustados de manera inmediata.

Después de haber realizado el análisis de riesgos el cual nos permitió conocer como se encuentra la organización y lo que está expuesta, se empieza a precisar las políticas de seguridad, se definen los controles de aplicabilidad teniendo como base la Norma ISO/IEC 27002, la cual no indican que para proteger una organización en materia de seguridad informática se deben de abarcar 133 controles, 39 objetivos y 11 dominios.

Se utilizo como base la ISO/IEC 27001 para los procesos y teniendo como objetivo principal los tres pilares de la información:

- Definición de políticas de seguridad.
- Análisis de riesgos.
- Declaración de aplicabilidad.
- Controles.
- Diseño del SGSI.

Después de haber realizado todos los procesos descrito anteriormente se desarrolla la implementación de la primera fase del SGSI el cual contiene lo siguiente:

- Control de riesgos.
- Tratamiento de riesgos.
- Identificación de controles seleccionados.
- Personas responsables.
- Tiempo de ejecución.

Se entrega la carta al gerente de la organización con los resultados del SGSI con el fin de proporcionar la continuidad del negocio y el funcionamiento de la organización.

Se concluye que implementar un SGSI en una empresa del sector salud trae beneficios a largo plazo, con el fin de garantizar altos estándares de protección de la información, sus activos y controles. Esto ayuda a fortificar la organización, la continuidad del negocio, y disminuir los riesgos al máximo.

11. RECOMENDACIONES

Las recomendaciones que se relacionan a continuación son con el fin de realizar un SGSI con resultados aceptables:

- Tomas de decisiones: organizar un comité el cual será responsable de tomar las decisiones al proceso de implementación del SGSI y la gestión de la operación del sistema. Es importante incluir al gerente de la organización el cual nos mostrara la visión del negocio.

- Respaldo y patrocinio: la alta dirección debe respaldar el SGSI, ya que esto refleja un esfuerzo al proyecto y permite la colaboración de diferentes funcionarios con roles relevantes. Esto con el comité responsable de la toma de decisiones es una gran ventaja para la seguridad de la información.

- Análisis de brechas (GAP): este es un análisis corto pero que nos llegara a dar entender cómo está la organización en materia de seguridad informática.

- Recursos, tiempo, dinero y personal: después del análisis de brechas vemos el impacto dentro de la organización, y vemos que el SGSI en una primera fase lleva tiempo, por lo tanto, necesitamos personal idóneo, recursos financieros y tecnológicos.

- Impacto del negocio: esto tiene dos objetivos principales, identificar procesos críticos y priorizar los procesos críticos entre mayor es el impacto debe ser mayor la prioridad.

- Por último revisar los estándares de seguridad: conocer la estructura, contenido de la ISO/IEC 27001, toda la serie 27000. El glosario de términos y un resumen general de los estándares.

12. DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación del mismo; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de Sistemas de Gestión de Seguridad de la Información, puedan acceder al documento.

BIBLIOGRAFÍA

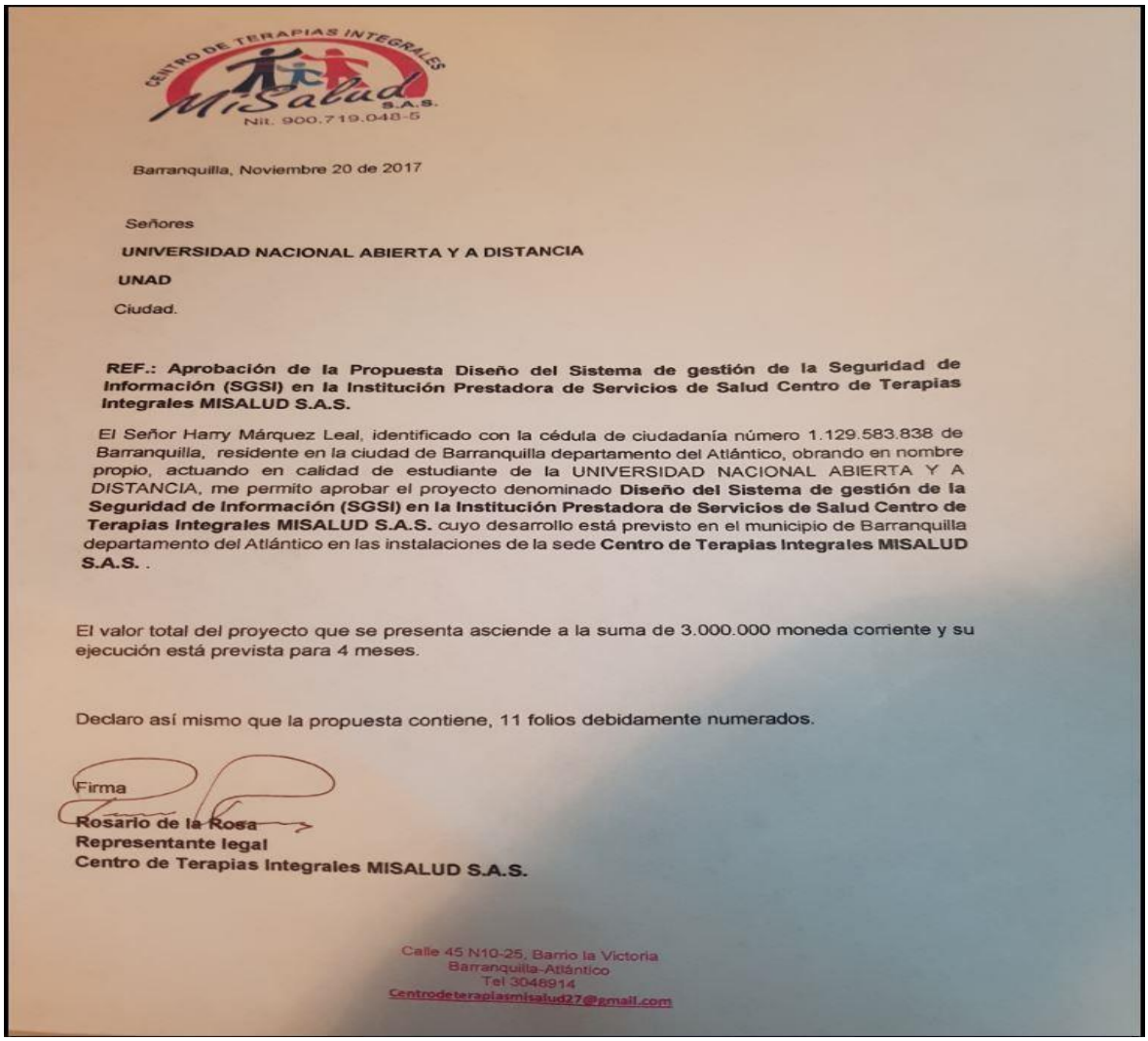
- ✓ AGUIRRE, Juan, ARISTIZABAL Catalina, diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda. {En Línea}, {2013} disponible en http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1
- ✓ AMUTIO, Miguel y CANDAU, Javier. MAGERIT. Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I. Método. Ministerio de Hacienda y Administraciones Pública. España, 2012.
- ✓ Cables y concejos eléctricos: Cables para instalaciones domesticas [en línea]. [Consultado: 29 de abril de 2020] Disponible en https://www.topcable.com/blog-electric-cable/tag/instalaciones-domesticas/.
- ✓ Ciberseguridad en el Sector Salud Susan Biddle, 2016 en línea https://revistaempresarial.com/salud/salud-ocupacional/ciberseguridad-sector-salud/
- ✓ Ciclo PDCA. Sistemas de Gestión de Seguridad de la Información. obtenido de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-14-agosto2013/135_ciclo_pdca_edward_deming.htmll
- ✓ CORDOBA, Alba, diseño e implementación de un sgsi para el área de informática de la Curaduría urbana segunda de pasto bajo la norma iso/iec 27001. {En Línea}, {Mayo 2015} disponible en http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3627/1/59650050.pdf
- ✓ CORLETTI Alejandro, Controles de seguridad. 2006. Obtenido de http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf.
- ✓ EL CONGRESO DE COLOMBIA. Ley estatutaria 1581, 2012 disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981
- ✓ Gómez, V. Á. (2014). Gestión de incidentes de seguridad informática. España: RA-MA Editorial.
- ✓ INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información (sgsi). requisitos 22 de marzo 2006 Bogota. Icontec disponible en http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf
- ✓ ISO27001. Sistemas de Gestión de la Seguridad de la Información (SGSI) disponible en http://www.iso27000.es/download/doc_sgsi_all.pdf
- ✓ LEY 1273 DE 2009 Nivel Nacional enero 2009 disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
- ✓ MINISTERIO DE COMUNICACIONES. informe final –modelo de seguridad de la información – sistema sansi – sgsi -modelo de seguridad de la información para la estrategia de gobierno en línea Versión 3, 26 diciembre 2008 disponible en http://programa.gobiernoenlinea.gov.co/apc-aa-

files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf
- ✓ MINISTERIO DE COMUNICACIONES. Sistemas de Gestión de la Seguridad de la Información (SGSI) disponible en http://www.mintic.gov.co/gestionti/615/w3-article-5482.html
- ✓ MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES .guía para la preparación de las TIC para la continuidad del negocio Versión 1.0 15 diciembre 2010 disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf
- ✓ MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES. Guía de Gestion de riesgos Versión 3.0 01 de abril 2016 disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf
- ✓ MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES. Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información 1.0 09 junio 2017 disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf
- ✓ Modelo para el gobierno de las TIC basado en las normas ISO. (2012). España: AENOR - Asociación Española de Normalización y Certificación
- ✓ Ross, J. W., & Weill, P. (2004). Seis decisiones de TI que no debe dejar en manos del departamento de TI. España: Ediciones Deusto - Planeta de Agostini Profesional y Formación S.L.
- ✓ SALCEDO, Robin, plan de implementación del sgsi basado en la norma ISO 27001:2013. {En Línea}, {19 diciembre 2014} disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf
- ✓ Sector salud lejos de adoptar medidas de ciberseguridad: Por Corporación Colombia Digital mayo 27 2016, en línea https://colombiadigital.net/actualidad/noticias/item/8963-sector-salud-lejos-de-adoptar-medidas-de-ciberseguridad.html
- ✓ Sin autor. Figura 1 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html
- ✓ Sin autor. Figura 2 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html
- ✓ Sin autor. Figura 3 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html
- ✓ Sin autor. Figura 4 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html
- ✓ Sin autor. Figura 5 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html
- ✓ Sin autor. Figura 5 [fotografía]. En: ISO27000. Madrid 2012. [consultado: 12 de abril de 2018]. Disponible en Internet: http://www.iso27000.es/sgsi.html

- ✓ SISTEMAS DE DETENCCION DE INSTRUCIONES (IDS) diciembre 2017 disponible en http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids
- ✓ SUAREZ, Sandra, análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. ltda, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. {En Línea}, {1 de octubre 2015} disponible en http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3777/1/20904541.pdf
- ✓ SUPERITENDENCIA DE INDUSTRIA Y COMERCIO. Manual de usuario del registro nacional de bases de datos-RNDB Versión 5.1, 2017 disponible en http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/RNBD/Manual_de_Usuario_RNBD_5-1_17-08-2017.pdf
- ✓ UNIVERSIDAD DISTRITAL. Seguridad de la Información: Política para la seguridad de la información de la Universidad Distrital Francisco José de Caldas,obtenido en: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf
- ✓ VILLEGAS, Néstor, GAVIRIA, Santiago, importancia de la implementación del sgsi 27001 en la seguridad informática de acceso en {En Línea}, {14 de octubre del 2011} disponible en http://repository.unimilitar.edu.co/bitstream/10654/3215/2/VillegasCortesNestorMauricio2011.pdf

ANEXOS

Anexo 1 Aval Proyecto



CENTRO DE TERAPIAS INTEGRALES
MiSalud S.A.S.
Nit. 900.719.048-5

Barranquilla, Noviembre 20 de 2017

Señores
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
UNAD
Ciudad.

***REF.*: Aprobación de la Propuesta Diseño del Sistema de gestión de la Seguridad de Información (SGSI) en la Institución Prestadora de Servicios de Salud Centro de Terapias Integrales MISALUD S.A.S.**

El Señor Harry Márquez Leal, identificado con la cédula de ciudadanía número 1.129.583.838 de Barranquilla, residente en la ciudad de Barranquilla departamento del Atlántico, obrando en nombre propio, actuando en calidad de estudiante de la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, me permito aprobar el proyecto denominado **Diseño del Sistema de gestión de la Seguridad de Información (SGSI) en la Institución Prestadora de Servicios de Salud Centro de Terapias Integrales MISALUD S.A.S.** *cuyo desarrollo está previsto en el municipio de Barranquilla departamento del Atlántico en las instalaciones de la sede* **Centro de Terapias Integrales MISALUD S.A.S.** .

El valor total del proyecto que se presenta asciende a la suma de 3.000.000 moneda corriente y su ejecución está prevista para 4 meses.

Declaro así mismo que la propuesta contiene, 11 folios debidamente numerados.

Firma
Rosario de la Rosa
Representante legal
Centro de Terapias Integrales MISALUD S.A.S.

Calle 45 N10-25, Barrio la Victoria
Barranquilla-Atlántico
Tel 3048914
Centrodeterapiasmisalud27@gmail.com

Fuente: El autor

Anexo 2 Levantamiento de la Información

MATRIZ DE LEVANTAMIENTO DE INFORMACIÓN DE ACTIVOS
SEGÚN METODOLOGÍA MAGERIT Y NORMA ISO 27001:2013
CENTRO DE TERAPIAS INTEGRALES MISALUD SAS

LEVANTAMIENTO DE INFORMACIÓN, INVENTARIO Y CLASIFICACIÓN DE ACTIVOS - SEGURIDAD DE LA INFORMACIÓN							
1	Nombre Entrevistado 1:	Jose Vila		Cargo	COORDINADOR DE SISTEMAS	Proceso	

INFORMACIÓN DE LOS ACTIVOS

No.	DATOS DEL ACTIVO DE INFORMACION			TIPO										DIMENSION					ATRIBUTOS								UBICACIÓN		
	Nombre del activo de información	Proceso propietario del activo	Responsable	[D] DATOS	[K] CLAVES CRIPTOGRAFICAS	[S] SERVICIOS	[SW] SOFTWARE	[HW] EQUIPAMENTO INFORMÁTICO	[COM] REDES DE COMUNICACIONES	[Media] SOPORTE DE INFORMACIÓN	[AUX] EQUIPAMENTO AUXILIAR	[L] INSTALACIONES	[P] PERSONAL	Dimensión Autenticidad (B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes o	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:		Físico	Electrónico	
																									Leve	Importante	Grave		
1	[SA_HEALTH SYSTEM	Contabilidad	Olga Serpa				X							B	A	M	B	B		x	x	x	x	x			x		x

	CONTABILIDAD]																											
2	[HW_ROUTER]	Sistemas	Jose Vila					X						MB	MB	MB	MB	MA			X	X	X				X	X	
3	[HW] SERVIDORES	Sistemas	Jose Vila			X								B	MB	MA	M	MA		X	X	X	X	X			X	X	X
4	[HW] COMPUTADORES	Sistemas	Jose Vila					X						MB	A	MB	A	B	X	X	X	X	X	X			X	X	X
5	[HW] PORTATILES	Sistemas	Jose Vila					X						B	B	B	A	B	X	X	X	X	X	X			X	X	X
6	[HW] IMPRESORAS Epson L375	Sistemas	Jose Vila					X						B	B	B	A	B		X	X				X			X	
7	[HW] ESCANERES	Sistemas	Jose Vila					X						B	B	B	A	B		X	X				X			X	
8	[SW] SISTEMAS OPERATIVOS	Sistemas	Jose Vila				X							MB	A	MB	A	B		X	X	X	X				X		X
9	[SW] OFFICE	Sistemas	Jose Vila				X							MB	MB	MB	MB	MA	X		X	X	X	X		X			X
10	[COM] SWITCHES	Sistemas	Jose Vila						X					MB	MB	MB	MB	MA		X	X	X		X		X			X
11	[COM] ROUTERS	Sistemas	Jose Vila						X					MB	MB	MB	MB	MA		X	X	X		X		X		X	X
12	[L] CENTRO DE DATOS Y CABLEADO	Sistemas	Jose Vila						X					M	M	M	M	MA			X				X			X	
13	[COM]PUNTOS DE ACCESO A LA RED	Sistemas	Jose Vila						X					A	M	M	A	MA			X				X			X	
14	[P] EMPLEADOS	Sistemas	Jose Vila										X	M	M	B	M	MB	X	X	X	X	X	X			X	X	X

15	[SW] BASES DE DATOS	Sistemas	Jose Vila				X							A	A	A	A	A	X	X	X	X	X	X			X		X
16	[AUX] UPS	Sistemas	Jose Vila								X			M	M	M	M	M			X				X			X		
17	[MEDIA] INFORMACION DIGITAL	Sistemas	Jose Vila							X				A	A	A	A	A	X	X	X	X					X			X
18	[MEDIA] ADMINISTRADOR DBA	Sistemas	Jose Vila							X				A	A	A	A	A	X	X	X	X	X				X			X
19	[D] DOCUMENTOS	Sistemas	Jose Vila	X										A	M	B	B	MA	X	X	X	X	X	X			X	X		
20	[MEDIA]CORREOS ELECTRONICOS	Sistemas	Jose Vila							X				B	B	B	M	A	X	X	X	X				X				X
21	[SW] SOFTWARE HEALTH SYSTEM	Sistemas	Jose Vila				X							A	A	A	A	A	X	X	X	X	X	X			X			X
22	[HW] DISCO DUROS	Sistemas	Jose Vila					X						B	B	B	M	A	X	X	X	X	X	X			X	X		X
23	[HW] MEMORIAS	Sistemas	Jose Vila					X						B	B	B	M	A	X	X	X	X	X	X			X	X		X

Fuente: el autor

Anexo 3 Análisis y tratamiento de los riesgos

MATRIZ DE ANALISIS Y TRATAMIENTO DE RIESGOS SEGÚN METODOLOGIA MAGERIT EMPRESA: CENTRO DE TERAPIAS INTEGRALES MISALUD SAS													
IDENTIFICACIÓN DE AMENAZAS, VULNERABILIDADES, ANALISIS DE RIESGOS, ESTRATEGIA DE CONTROLES Y PLAN DE TRATAMIENTO A APLICAR													
INFORMACIÓN DE LOS ACTIVOS DE INFORMACION													
GESTION DE RIESGOS: ANALISIS DE RIESGOS Y TRATAMIENTO DE LOS RIESGOS													
Activos de Información	**No. De Amenazas y Vulnerabilidades**	**Nombre del activo de información**	**VALORACIÓN DEL RIESGO DE LOS ACTIVOS**	**Amenazas Metodología Magerit**	**Vulnerabilidades**	**Probabilidad de vulneración (1 Muy raro, 2 poco probable, 3 posible, 4 probable, 5 prácticamente seguro)**	**Cálculo del riesgo neto (Valoración del riesgo ***	**Criticidad neta (1 a 4 despreciable (d), 5 a 9 baja (B) , 10 a 15 apreciable (a), 16 a 20 importante (i) , 21 a 25 crítico(C))**	**Calificación de Gestión (1 control no existe, 2 existe, pero no efectivo, 3 efectivo, pero no**	**Si la opción es 2 - 3 o 4 Indique el Control aplicado actual**	**Riesgo residual (riesgo neto dividido entre la**	**Criticidad residual (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20**	**Niveles de aceptación del riesgo (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I))**
[SW] SOFTWARE	1	[SA_HEALTH SYSTEM CONTABILIDAD]	12	[E2] Errores del administrador	Posible pérdida de información	5	60	C	1		60	C	I

[SW] SOFTWARE	2	[SW] SISTEMAS OPERATIVOS	11	[A] Ataques intencionados	Instalación de software no licenciado	1	11	A	1		11	A	M
[SW] SOFTWARE	3	[SW] OFFICE	8	[E2] Errores del administrador	Instalación de software no licenciado	2	16	I	1	Se tiene software licenciado.	16	I	I
[SW] SOFTWARE	4	[SW] BASES DE DATOS	20	[E2] Errores del administrador	Posible pérdida de información	2	40	C	1		40	C	I
[HW] EQUIPAMENTO INFORMÁTICO	5	[HW] SERVIDORES	16	[A] Ataques intencionados	Errores actualización hardware y software	4	64	C	1		64	C	I
[HW] EQUIPAMENTO INFORMÁTICO	6	[HW] COMPUTADORES	11	[E] Errores y fallos no intencionados	Errores actualización hardware y software	4	44	C	1		44	C	I
[HW] EQUIPAMENTO INFORMÁTICO	7	[HW] PORTATILES	11	[E] Errores y fallos no intencionados	Falla de suministro eléctrico	4	44	C	1		44	C	I
[HW] EQUIPAMENTO INFORMÁTICO	8	[HW] IMPRESORAS Epson L375	11	[E] Errores y fallos no intencionados	Errores actualización hardware y software	2	22	C			0	D	A
[HW] EQUIPAMENTO INFORMÁTICO	9	[HW] ESCANERES	11	[E] Errores y fallos no intencionados	Errores actualización hardware y software	2	22	C	1		22	C	I
[COM] REDES DE COMUNICACIONES	10	[COM] SWITCHES	8	[E] Errores y fallos no intencionados	Errores de configuración	1	8	B	1		8	B	M

[COM] REDES DE COMUNICACIONES	11	[COM] ROUTERS	8	[E] Errores y fallos no intencionados	Errores de configuración	4	32	C	1		32	C	I
[COM] REDES DE COMUNICACIONES	12	[COM]PUNTOS DE ACCESO A LA RED	19	[E] Errores y fallos no intencionados	Errores de configuración	4	76	C	1		76	C	I
[D] DATOS	13	[D] DOCUMENTOS	16	[E] Errores y fallos no intencionados	Denegación de Servicio	4	64	C	1		64	C	I
[Media] SOPORTE DE INFORMACIÓN	14	[MEDIA] INFORMACION DIGITAL	20	[E] Errores y fallos no intencionados	Modificación o destrucción de la información	4	80	C	1		80	C	I
[Media] SOPORTE DE INFORMACIÓN	15	[MEDIA] ADMINISTRADOR DBA	20	[E] Errores y fallos no intencionados	Modificación o destrucción de la información	3	60	C	1		60	C	I
[Media] SOPORTE DE INFORMACIÓN	16	[MEDIA]CORREOS ELECTRONICOS	12	[A] Ataques intencionados	Posible pérdida de información	4	48	C	1	Se cuenta con los mecanismos de autenticación para el ingreso.	48	C	I
[L] INSTALACIONES	17	[L] CENTRO DE DATOS Y CABLEADO	17	[A] Ataques intencionados	Incendio	4	68	C	1		68	C	I
[P] PERSONAL	18	[P] EMPLEADOS	12	[E] Errores y fallos no intencionados	Indisponibilidad del personal	4	48	C	1	Se mantiene relación sobre uso y manejo de la información con los funcionarios	48	C	I

Fuente: el autor

Anexo 4 Encuesta

Anexo B : Encuesta

Objetivo: la siguiente encuesta tiene como objetivo obtener información relevante por parte de los coordinadores del Centro de terapias integrales MISALUD sas. Con el fin de determinar la importancia de la implementación de un SGSI (Sistema de Gestion de Seguridad de la Información), esta encuesta es para desarrolla proyecto aplicado aprobado por la Universidad Nacional Abierta y a Distancia.

Fecha _____

Nombre _____

Preguntas

1. ¿Salvaguarda Copia de seguridad de los documentos de la empresa?
   Nunca () A veces () Casi Siempre () Siempre ()
2. ¿Implementa el cambio de claves de su equipo?
   Nunca () A veces () Casi Siempre () Siempre ()
3. ¿Cree Usted que es responsable de su equipo informático?
   Nunca () A veces () Casi Siempre () Siempre ()
4. ¿Sabe si existe un manual o documento donde se especifique las políticas de seguridad de la información?
   Nunca () A veces () Casi Siempre () Siempre ()
5. ¿Se le brindan capacitación y formación por parte de la Empresa acerca de la seguridad de la información?
   Nunca () A veces () Casi Siempre () Siempre ()
6. ¿Se le comunica cuando se establece algún procedimiento o política relativa a la seguridad de la información?
   Nunca () A veces () Casi Siempre () Siempre ()
7. ¿La empresa le ha enterado sobre el sistema de Gestion de Seguridad de la Información (SGSI)?
   Nunca () A veces () Casi Siempre () Siempre ()
8. ¿Piensa que es de suma importancia el desarrollo de políticas de seguridad de la información para el Centro de terapias integrales MISALUD sas??
   Nunca () A veces () Casi Siempre () Siempre ()

¿Por qué?

_____
_____
_____
___

Anexo 5 Evaluación de efectividad de controles

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	**INICIAL**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	20	100	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	10	100	**INICIAL**
A.8	GESTIÓN DE ACTIVOS	10	100	**INICIAL**
A.9	CONTROL DE ACCESO	10	100	**INICIAL**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	20	100	**INICIAL**
A.12	SEGURIDAD DE LAS OPERACIONES	20	100	**INICIAL**
A.13	SEGURIDAD DE LAS COMUNICACIONES	10	100	**INICIAL**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	20	100	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	10	100	**INICIAL**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	**INICIAL**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	**INICIAL**
A.18	CUMPLIMIENTO	20	100	**INICIAL**
PROMEDIO EVALUACIÓN DE CONTROLES		**15**	**100**	**INICIAL**

Fuente: El autor

Anexo 6 Brecha anexo A ISO 27001:2013

Fuente: El autor

Anexo 7 Formato de Vulnerabilidades encontradas

Vulnerabilidad:
Exim 4.69 remote code execution

Referencias: OWASP – Riesgos de Seguridad en Aplicaciones Web:
A6 – "Defectuosa configuración de seguridad "

CVE: N/A

Numero de Vulnerabilidades Identificadas:
1

Servicios- Items Afectados:
Servidor SMTP Exim smtpd 4.69
Puerto TCP 110-25

Descripción de la Vulnerabilidad:

Esta vulnerabilidad permite a un atacantes remoto poder ejecutar código arbitrario mediante el establecimiento de una sesión de SMTP que incluya varias órdenes (Comandos) de correo, junto con un mensaje de tamaño representativo, el cual contienen encabezados previamente elaborados.

Detalles de la Vulnerabilidad:

Esta vulnerabilidad afecta a las versiones igual o inferior a las **4.69** del servidor de correo EXIM.

Riesgo:

- Un atacante informático podría aprovecharse de esta vulnerabilidad para comprometer el sistema, y ejecutar código arbitrario con los privilegios del usuario con que se ejecuta el proceso/demonio del servidor de correo electrónico.

- Un atacante informático podría aprovecharse de esta vulnerabilidad para aumentar privilegios en el sistema, y lograr comprometerlo con permisos de usuario con altos privilegios.

Impacto:

- Perdida de reputación de la empresa dueña del aplicativo o sitio Web, o de la empresa que construyo el aplicativo o sitio Web.

- Perdida de la integridad y confidencialidad del servidor que contiene al sitio web www.xyz.com.co, ya que un usuario puede tomar el control parcial o total del servidor.

Evidencias:

Banner Grabbinbg. 

Recomendación para solucionar esta Vulnerabilidad:

- Actualizar el servidor a la última versión, o a una versión no vulnerable. Esta actualización debe de ser planeada de forma anticipada, con el fin de no causar denegación de servicios a los usuarios finales, además de documentar bien la actualización del cambio de versión, para no generar traumas en los usuarios finales.

Referencias Web:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4345
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4344
http://osvdb.org/69685
http://www.exploitsearch.net/index.php?q=69685+OSVDB
http://bugs.exim.org/show_bug.cgi?id=787
http://seclists.org/oss-sec/2010/q4/311
http://r00tsecurity.org/forums/topic/12750-exim-smtpd-469-exploit/
http://www.nessus.org/plugins/index.php?view=single&id=51179/
http://www.exploit-db.com/exploits/16925/

Observaciones:

El código Exploit (Código malicioso que explota esta vulnerabilidad) está disponible de forma gratuita en Internet, tanto a nivel de código para ser compilado, como a nivel de Frameworks de explotación, donde el atacante, ya encuentra todo listo para lanzar el ataque al servidor SMTP**.**

Anexo 8 Plan de acción seguridad informática

PLAN DE ACCIÓN SEGURIDAD INFORMATICA								
Eje temático	**Logro**	**Criterio**	**Subcriterio**	**Actividad**	**Producto / Meta**	**Responsable**	**Fecha programada**	**Recursos**
TIC SERVICIOS	**Servicios centrados en el usuario** Los usuarios cuentan con una oferta de trámites, servicios y espacios de comunicación a través de canales electrónicos usable	**Caracterización de usuarios** Busca conocer de una manera detallada las necesidades y características de los usuarios, de forma tal que las actividades de diseño, rediseño, comunicación y mejoramiento	La entidad realiza la caracterización de sus usuarios.	Actualizar la caracterización de usuarios en el canal presencial en las 36 Regionales	Informe de caracterización de usuarios del canal presencial	Secretaría General		Recursos técnicos y humanos

	s y accesibles que responden a sus necesidades y expectativas.	de trámites y servicios respondan a éstas.						
	Servicios centrados en el usuario Los usuarios cuentan con una oferta de trámites, servicios y espacios de comunicación a través	**Accesibilidad** Busca que los trámites y servicios disponibles por medios electrónicos cuenten con las características necesarias para que toda la población pueda acceder a ellos,	La entidad incorpora las directrices de accesibilidad. La entidad incluye las directrices de usabilidad en los trámites y servicios disponibles por medios electró	Garantizar que la página web institucional de la entidad cumpla con las directrices de accesibilidad y usabilidad.	Página web en cumplimiento de los estándares establecidos	Oficina de comunicaciones		Recursos técnicos, humanos y financieros (36 millones)

	de canales electrónicos usables y accesibles que responden a sus necesidades y expectativas.	incluso aquella que se encuentra en situación de discapacidad. **Usabilidad** Busca que los trámites y servicios disponibles por medios electrónicos sean de fácil uso, y proporcionen una mejor experiencia a los usuarios.	nicos. La entidad cumple los estándares establecidos para los sitios web.					
	Sistema integr	**Sistema web de**	La entidad habilita	Implementar el	Canal de PRQS	Secretaría		Recursos

	ado peticiones, quejas, reclamos y denuncias (PQRD) Los usuarios cuentan con múltiples canales que operan de forma integrada, para la atención de peticiones, quejas, reclamos y denuncias.	**contacto, peticiones, quejas, reclamos y denuncias** Busca garantizar que los usuarios cuenten con un canal de atención y comunicación con la entidad a través del sitio web, que permita realizar el seguimiento de PQRD	a través de su sitio web un canal de atención para contacto, peticiones, quejas, reclamos y denuncias (PQRD), y las atiende de acuerdo con ley y demás disposiciones vigentes.	canal de PQRS DF virtual	DF virtual en funcionamiento	General		técnicos, humanos y financieros (32 millones)
	Trámites y	**Trámites y**	La entidad	Gestionar los	Trámites	Secretaría		Recurso

	servicios en línea: Los usuarios pueden realizar un trámite o servicio, desde la solicitud hasta la obtención del producto, totalmente en línea.	**servicios en línea** Busca que los usuarios puedan gestionar los trámites y servicios ofrecidos por las entidades completamente en línea.	automatiza y presta en línea sus trámites y servicios priorizados, permitiendo al usuario: - Conocer plazos de respuesta - Recibir avisos de confirmación - Consultar el estado de avance del trámite o	trámites de la Dirección Nacional de Defensoría Pública y de la Dirección Nacional de Recursos y acciones Judiciales en el SUIT	gestionados	General, Direccional Nacional de Defensoría Pública y Dirección Nacional de Recursos y Acciones Judiciales		s técnicos y humanos
				Registro y certificación de cursos a cargo de la Dirección de Promoción y Divulgación	Servicio en Línea	Secretaría General, Dirección de Promoción y Divulgación y Grupo de Sistemas		Recursos técnicos y humanos

			servicio. - Realizar pagos electrónicos. - Conocer el registro de la fecha y la hora en la cual adelanta la solicitud del trámite o servicio.					
TIC GOBIERNO ABIERTO	**Transparencia** Busca facilitar el acceso a la información pública de	**Acceso a la información pública** Busca poner a disposición de los usuarios toda	La entidad pública la información básica y la establecida en la Ley de Transp	Actualizar la información del botón de transparencia y Acceso a la Información	Botón actualizado	Oficina de comunicaciones		Recursos técnicos y humanos

	manera permanente y permitir su aprovechamiento por parte de los usuarios.	la información de carácter público, a través de diversos canales electrónicos.	arencia y Acceso a la Información púbica, ley 1712 de 2014, en diversos formatos e idiomas.	Actualizar el índice de información clasificada y reservada- fase 1: asuntos administrativos	Índice actualizado fase 1	Oficina Jurídica		Recursos técnicos y humanos
				Analizar la información que está en poder o custodia de la entidad para identificar la clasificada y la reservada, de conformidad con las tablas de	Fase 2: Índice de información clasificada y reservada- asuntos misionales	Vicedefensoría, Oficina Jurídica y Gestión Documental		Recursos técnicos y humanos

				retención documental.				
				Actualizar el registro de activo de información	Registro de activos de información actualizado	Grupo gestión documental - Sistemas		Recursos técnicos y humanos
				Actualizar el esquema de publicaciones - información mínima obligatoria	Esquema de publicaciones actualizado- información mínima obligatoria	Secretaría General		Recursos técnicos y humanos
				Elaborar el esquema de publicaciones- información que se publica de manera	Publicación esquema de publicaciones - información que se publica de maner	Vicedefensoría y Oficina de Comunicaciones		Recursos técnicos y humanos

				proactiva	a proactiva			
				Elaborar el informe de solicitudes de acceso a la información de la vigencia 2016	Informe semestral	Secretaría General		Recursos técnicos y humanos
		Rendición de cuentas Busca fomentar el diálogo y la retroalimentación entre las entidades del Estado y los usuarios a través	La entidad informa a los usuarios sobre los resultados de su gestión a través de sus canales electrónicos.	Elaborar acta final de la audiencia pública con lo expuesto y los principales comentarios y preguntas recibidas de la ciudadanía	Acta publicada en la página web	Oficina de comunicaciones - Vicedefensoría		Recursos técnicos y humanos

		de acciones permanentes de rendición de cuentas, haciendo uso de medios electrónicos.						
		Datos abiertos Busca generar valor a partir del aprovechamiento de la información pública por parte de los usuarios.	La entidad identifica y publica datos en formato abierto, priorizando aquellos de mayor impacto en los usuarios.	Publicar y actualizar información en datos abiertos en www.datos.gov.co	Datos abiertos publicados	Oficina de comunicaciones		Recursos técnicos y humanos
				Divulgación y promoción de datos abiertos	Banner y hashtag	Oficina de comunicaciones		Recursos técnicos y humanos

TIC DE GESTIÓN	**Información**	**Diseño de los Componentes de Información** Busca estructurar y caracterizar los componentes de información.	La entidad provee y/o consume componentes de información a través de la Plataforma de Interoperabilidad.	Analizar el componente técnico de la Defensoría para la interoperabilidad	guía para la interoperabilidad	Grupo de Sistemas		Recursos técnicos y humanos
	Capacidades Institucionales	**Uso eficiente del papel** Busca el uso de eficiente de papel a través de la definición y adopción de buenas prácticas	La entidad define e implementa buenas prácticas para el uso eficiente del papel, mediadas por TI.	Implementar estrategias de promoción y divulgación de buenas prácticas para el uso eficiente del papel.	Informe de la implementación	Subdirección administrativa Gestión Documental Oficina de Comunicación		Recursos técnicos y humanos

		mediadas por TI.						
	Estrategia de TI Busca aportar valor al desarrollo sectorial e institucional de las entidades a través de una estrategia de TI	**Direccionamiento Estratégico de TI** Busca proporcionar las directrices para una estrategia de TI alineada con las estrategias del Estado, sectoriales e institucionales, desde el entendimiento de la misión, metas y objetivo	La entidad cuenta con un plan estratégico de TI, que incluye la identificación de retos y oportunidades de TI, la definición de políticas e iniciativas estratégicas de TI y la definición del portafolio de proyectos.	Definir y proponer para su adopción la arquitectura de TI al Comité de TI (Actualmente se tiene una arquitectura adoptada hace más de 10 años)	Documento de arquitectura de TI propuesta	Sistemas		Recursos técnicos y humanos
				Definir portafolio de proyectos	Documento de portafolio de proyectos establecidos	Sistemas		Recursos técnicos y humanos

		s de la entidad con el objetivo de generar valor público.						
	Gobierno de TI Busca aportar valor al desarrollo institucional y/o sectorial a través de la implementación de esquemas de gobernabilidad de TI, alineados a	**Esquema de Gobierno de TI** La entidad cuenta con un esquema de gobierno de TI que contemple políticas, procesos, recursos, gestión del talento y proveedores, compra	La entidad cuenta con un esquema de gobierno de TI que contemple políticas, procesos, recursos, gestión del talento y proveedores, compras, calidad, instancias de decisió	Definir estructura organizacional de TI	Estructura organizacional de TI establecida	Sistemas - Talento Humanos		Recursos técnicos y humanos
				Actualizar los procesos gestión de TI (cadena de valor)	Documento actualizado de procesos de gestión de TI (cadena de valor de TI)	Sistemas		Recursos técnicos y humanos
				Actualizar el portafolio de servicios	Documento de portafolio catálogo de servicios	Sistemas		Recursos técnicos y hum

	los procesos y procedimientos de la entidad.	s, calidad, instancias de decisión, estructura organizacional e indicadores de la operación de TI	n, estructura organizacional e indicadores de la operación de TI		establecidos actualizado			anos
		Implementación de la Estrategia de TI Busca desplegar los proyectos incluidos en el plan estratégico de TI y la conformación del	La entidad ejecuta el portafolio de proyectos a partir de la definición de su mapa de implementación, que incorpora los	Crear la mesa de ayuda y Punto único de contacto - PUC	Mesa de ayuda y PUC (Punto único de Contacto) establecido	Sistemas		Recursos técnicos y humanos

		catálogo de servicios que incluye la definición de la oferta de servicios de TI para usuarios internos y externos.	recursos asociados.					
SEGURIDAD Y PRIVACIDAD	**Definición del marco de seguridad y privacidad de la información y de los sistemas de**	**Diagnóstico de Seguridad y Privacidad** Busca determinar el estado actual del nivel de segurid	La entidad cuenta con un diagnóstico de seguridad y privacidad e identifica y analiza los riesgos	Establecer alcance del Modelo de Seguridad y Privacidad de la Información (MSPI) y su declaración de	Documento que establece objetivos, alcance y límites del MSPI, las políticas de segurid	Sistemas		Recursos técnicos y humanos

	información Busca definir el estado actual del nivel de seguridad y privacidad y define las acciones a implementar.	ad y privacidad de la información y de los sistemas de información.	existentes.	aplicabilidad	ad, la declaración de aplicabilidad del modelo y define la asignación del recurso humano, roles y responsabilidades			
				Realizar análisis de riesgos y vulnerabilidades y definir proyectos para reforzar la seguridad informática	Documento con el informe de análisis de riesgos, matriz de riesgos y plan de tratamiento de riesgos de	Sistemas		Recursos técnicos y humanos

					seguridad informática.			
		Plan de Seguridad y Privacidad de la Información Busca generar un plan de seguridad y privacidad alineado con el propósito misional.	La entidad define las acciones a implementar a nivel de seguridad y privacidad, así como acciones de mitigación del riesgo.	Establecer el plan de capacitación a usuarios en seguridad informática, políticas de seguridad y SGSI	Documento con el plan de comunicación, sensibilización y socialización a colaboradores	Sistemas		Recursos técnicos y humanos
				Definir el proceso de atención de incidentes informáticos	Documento contentivo del proceso de atención de incidentes informáticos	Sistemas		Recursos técnicos y humanos
				Establecer el plan de ejecució	Documento contentivo del	Sistemas		Recursos técn

				n de proyectos de seguridad informática	plan de ejecución de proyectos de seguridad informática			icos y humanos

Anexo 9 Análisis de amenazas, vulnerabilidad y nivel de riesgo

PARA ANALISIS DE AMENAZAS: (del listado escoja las que identifica en su empresa y califique de la siguiente manera:)	
Posible	Nunca ha sucedido pero no se descarta
Probable	Ya ocurrido en un lugar o condición similar
Inminente	Evento con información que lo hace evidente y detectable

PARA ANALISIS DE VULNERABILIDAD CALIFIQUE ASI:	
0.1 - 1.0	BAJA
1.1 - 2.0	MEDIA
2.1 - 3.0	ALTA

Definición de las amenazas				En Personas					En Recursos					En Sistemas y Procesos					
AMENAZAS	ÁREA (S)	ORIGEN	CALIF. AMENAZA	ORGANIZACIÓN	CAPACITACIÓN	DOTACION	CALIF.	INTERP	MATERIALES	EDIFICACIÓN	EQUIPOS	CALIF.	INTERP	SERVICIOS PÚBLICOS	APOYO AUTORIDADES	RECUPERACIÓN	CALIF.	INTERP	NIVEL RIESGO
			PROBABLE					BAJO					BAJO					BAJO	BAJO
			PROBABLE					BAJO					BAJO					BAJO	BAJO
			PROBABLE					BAJO					BAJO					BAJO	MED

																			IO
			PROBABLE					BAJO					BAJO					BAJO	MEDIO
			INMINENTE					BAJO					BAJO					BAJO	MEDIO
			PROBABLE					BAJO					BAJO					BAJO	MEDIO
			POSIBLE					BAJO					BAJO					BAJO	BAJO
			POSIBLE					BAJO					BAJO					BAJO	BAJO
			POSIBLE					BAJO					BAJO					BAJO	BAJO
			PROBABLE					BAJO					BAJO					BAJO	BAJO

Anexo 10 Cumplimiento plan de acción

RESPONSABLE / AREA	TEMA	FUNCIONARIO
Control interno	Revisiones de seguridad de la información	
	Revisión independiente de la seguridad de la información	
	Cumplimiento con las políticas y normas de seguridad.	
	CUMPLIMIENTO	
	Auditoría Interna Plan	
	Auditoría Interna Ejecución y Subsanación de hallazgos y brechas	
Gestión humana	Selección e investigación de antecedentes	
	Términos y condiciones del empleo	
Líder de Proceso 1	**PROCESO**	
	DESCRIPCIÓN DEL PROCESO	
Líder de Proceso 2	**PROCESO**	
	DESCRIPCIÓN DEL PROCESO	
Líder de Proceso 3	**PROCESO**	
	DESCRIPCIÓN DEL PROCESO	
Responsable de compras y adquisiciones	RELACIONES CON LOS PROVEEDORES	
	Seguridad de la información en las relaciones con los proveedores	
	Gestión de la prestación de servicios de proveedores	
Responsable de la continuidad	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
	Continuidad de la seguridad de la información	
	Planificación de la continuidad de la seguridad de la información	
	Implementación de la continuidad de la seguridad de la información	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	

	Redundancias	
	Disponibilidad de instalaciones de procesamiento de información	
Responsable de la seguridad física	SEGURIDAD FÍSICA Y DEL ENTORNO	
	ÁREAS SEGURAS	
	Perímetro de seguridad física	
	Áreas de despacho y carga	
	Visita al Centro de Computo	
Responsable de SI	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
	SEGURIDAD DE LOS RECURSOS HUMANOS	
	Antes de asumir el empleo	
	Durante la ejecución del empleo	
	Terminación y cambio de empleo	
	GESTIÓN DE ACTIVOS	
	CUMPLIMIENTO	
	Cumplimiento de requisitos legales y contractuales	
	CONTROL DE ACCESO	
	CRIPTOGRAFÍA	
	SEGURIDAD FÍSICA Y DEL ENTORNO	
	SEGURIDAD DE LAS OPERACIONES	
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
	Procedimientos de operación documentados	
	Gestión de cambios	
	Gestión de capacidad	
	Separación de los ambientes de desarrollo, pruebas y operación	
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	
	COPIAS DE RESPALDO	
	REGISTRO Y SEGUIMIENTO	
	Registro de eventos	

	Protección de la información de registro	
	Registros del administrador y del operador	
	Sincronización de relojes	
	CONTROL DE SOFTWARE OPERACIONAL	
	Instalación de software en sistemas operativos	
	GESTIÓN DE LA VULNERABILIDAD TÉCNICA	
	Gestión de las vulnerabilidades técnicas	
	Restricciones sobre la instalación de software	
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	
	Controles sobre auditorías de sistemas de información	
	SEGURIDAD DE LAS COMUNICACIONES	
	GESTIÓN DE LA SEGURIDAD DE LAS REDES	
	TRANSFERENCIA DE INFORMACIÓN	
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	
	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	
	DATOS DE PRUEBA	
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
	Alcance MSPI (Modelo de Seguridad y Privacidad de la Información)	
	Identificación y valoración de riesgos	
	Tratamiento de riesgos de seguridad de la información	
	Toma de conciencia, educación y formación en la seguridad de la información	
	Planificación y control operacional	
	Implementación del plan de tratamiento de riesgos	
	Indicadores de gestión del MSPI	

	Plan de seguimiento, evaluación y análisis del MSPI	
	Evaluación del plan de tratamiento de riesgos	
	Plan de seguimiento, evaluación y análisis del MSPI	
	Tratamiento de temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, o en los comités directivos interdisciplinarios de la Entidad	
	Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información.	
	La entidad conoce su papel dentro del estado colombiano, identifica y comunica a las partes interesadas la infraestructura crítica.	
	Las prioridades relacionadas con la misión, objetivos y actividades de la Entidad son establecidas y comunicadas.	
	La gestión de riesgos tiene en cuenta los riesgos de ciberseguridad	
	Detección de actividades anómalas	
	Respuesta a incidentes de ciberseguridad, planes de recuperación y restauración	
Responsable de TICs	Teletrabajo	
	Manejo de medios	
	Derechos de propiedad intelectual.	
	CONTROL DE ACCESO	
	SEGURIDAD DE LAS OPERACIONES	
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
	COPIAS DE RESPALDO	
	CONTROL DE SOFTWARE OPERACIONAL	
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	

	SEGURIDAD DE LAS COMUNICACIONES	
	GESTIÓN DE LA SEGURIDAD DE LAS REDES	
	TRANSFERENCIA DE INFORMACIÓN	
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
	Plan y Estrategia de transición de IPv4 a IPv6	
	Implementación del plan de estrategia de transición de IPv4 a IPv6	
	Redundancias	
Calidad	Procedimientos de control documental del MSPI	

Anexo 11 Listado maestro de documentos

NO.	DATOS E INFORMACIÓN PARA RECOLECTAR PARA LA EVALUACIÓN Lista de información BASICA a solicitar	NOMBRE DEL DOCUMENTO ENTREGADO	OBSERVACIONES
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)	GCM-001	**habilitación Entidad**
2	Misión	GCM-002	
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.	No Aplica	
4	Mapa de Procesos	GCM-005	
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	GCM-004	No se detalla área de seguridad
6	Políticas de seguridad de la información formalizada y firmada	GCM-010	políticas realizadas en base ley 1581 2012
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	No Tiene	En proceso
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección	No Tiene	En proceso
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección	No Tiene	En proceso
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección	No Tiene	En proceso
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)	No Tiene	En proceso
12	Procedimientos de control documental del MSPI	No Tiene	En proceso
13	Metodología de Gestión de riesgos	No Tiene	En proceso

14	Riesgos identificados y valorados de acuerdo con la metodología	No Tiene	En proceso
15	Planes de tratamiento de los riesgos	No Tiene	En proceso
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información	No Tiene	En proceso
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad	No Tiene	En proceso
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.	No Tiene	En proceso
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información	No Tiene	En proceso
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección	No Tiene	En proceso
21	Inventario de áreas de procesamiento de información y telecomunicaciones	No Tiene	En proceso
22	Diagrama de red de alto nivel o arquitectura de TI	No Tiene	En proceso
23	Inclusión de la seguridad de la información en la gestión de proyectos	No Tiene	En proceso
24	Inventario de partes externas o terceros a los que se transfiere información de la entidad	No Tiene	En proceso
25	Formato de acuerdo de transferencia de información	No Tiene	En proceso
26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden	No Tiene	En proceso
27	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.	No Tiene	En proceso
28	Plan de continuidad de la Entidad aprobado	No Tiene	En proceso
29	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información	No Tiene	En proceso
30	Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad	No Tiene	En proceso
31	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la	No Tiene	En proceso

	información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea.		
32	Indicadores y métricas de seguridad de la información definidos.	No Tiene	En proceso
33	Declaración de aplicabilidad	No Tiene	En proceso
34	Aceptación de los riesgos residuales por parte de los dueños de los riesgos	No Tiene	En proceso
	Lista de información para aquellas entidades que hayan avanzado en la fase de IMPLEMENTACIÓN		
35	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	No Tiene	En proceso
36	Avance en la ejecución del plan de tratamiento de riesgos	No Tiene	En proceso
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	No Tiene	En proceso
	Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO		
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	No Tiene	En proceso
39	Documento con el plan de auditorías internas y resultados, de acuerdo con lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.	No Tiene	En proceso
40	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.	No Tiene	En proceso
	Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA		
41	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.	No Tiene	En proceso
42	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua.	No Tiene	En proceso

Porcentaje de cumplimiento del MSPI en los procesos de la entidad	**# total de procesos**	**# de procesos definidos en el alcance**	**Total avance por procesos**

43	Con base al alcance definido en la política de seguridad y el total de procesos de la entidad, indicar los siguientes datos	42	4	10%

Anexo 12 Carta Entrega Diseño SGSI

Anexo C: Carta Entrega Diseño SGSI

Barranquilla 21 de mayo 2018

Doctora

Rosario de la Rosa

Gerente Centro de Terapias Integrales MISALUD SAS

Apreciada Doctora

Por medio de la presente se hace entrega de los resultados del Diseño del Sistema de Gestion de Seguridad de la Información, el cual fue elaborado con el fin de proporcionar la continuidad del negocio y el funcionamiento del proceso de la empresa. Su objetivo no está orientado a garantizar la seguridad sino a generar políticas y controles para que los riesgos de la seguridad de la información para que sean conocidos, asumidos, gestionados y minimizados por la empresa, de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se producen en la misma, en cuanto a riesgos, entorno y tecnología.

La estructura del Diseño se desarrolla en primer lugar con un marco de referencia que describe teóricamente un SGSI, la normatividad, que especifica los estándares de implementación de este. Se explican los mecanismos de recolección de la información y la metodología empleada y sus ventajas. Se identifican y valora las vulnerabilidades y amenazas de acuerdo los activos identificados. Se evalúan los riesgos, se genera un modelo de gestión según la norma y por último se recomienda un plan de acción según los riesgos más relevantes y que tienen un mayor nivel de prioridad.

Todo diseño genera estrategias informáticas y de gestión que dan la oportunidad de mejorar y percibir los procesos que están en un nivel mayor de riesgo, proporcionando controles basados en la norma ISO 27001:2013, lo que facilitaría en un futuro implementar un SGSI y solicitar una certificación lo que le daría mayor relevancia al Centro de Terapias Integrales MISALUD SAS con otras empresas del sector.

El informe se adjunta con todos los resultados.

Cordialmente,

Ing. Harry Marquez

Responsable Diseño SGSI