DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BAJO LA NORMA ISO27001:2013 EN LA E.P.S ASMET SALUD

ING. JONATHAN FERNANDO REYES ARTUNDUAGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA CEAD-SUR
TIMANA HUILA, COLOMBIA
2019

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BAJO LA NORMA ISO27001:2013 EN LA E.P.S ASMET SALUD

ING. JONATHAN FERNANDO REYES ARTUNDUAGA

Trabajo de grado:
Especialización en Seguridad Informática

Mg. Gabriel Mauricio Ramírez
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA CEAD-SUR
TIMANA HUILA, COLOMBIA
2019

CONTENIDO

LISTADO DE TABLAS **7**

LISTADO DE GRAFICAS **9**

LISTADO DE IMAGENES **10**

INTRODUCCION **11**

1. DEFINICIÓN DEL PROBLEMA **12**

DESCRIPCION DEL PROBLEMA 12
FORMULACIÓN DEL PROBLEMA 13

2. JUSTIFICACIÓN **14**

3. OBJETIVOS **16**

3.1 OBJETIVO GENERAL 16
3.2 OBJETIVOS ESPECÍFICOS 16

4. MARCO REFERENCIAL **17**

4.1 MARCO TEORICO 17
4.2 MARCO CONCEPTUAL 23
4.3 MARCO LEGAL 25
"Ley 1273 del 2009 ..... *25*
"Ley 1288 de 2009. ..... *26*
"Ley 1341 de 2009. ..... *27*
"Ley Grooming Argentina *27*
"Ley especial contra delitos informáticos en Venezuela. *27*
"Ley No 30096 de Perú. *28*
4.4 MARCO CONTEXTUAL 28
CONTEXTO DE LA EMPRESA 30
CONOCIMIENTO DE LA EMPRESA 30
NATURALEZA *30*
MISION DE LA EMPRESA *30*
VISION DE LA EMPRESA *31*

5. DISEÑO METODOLÓGICO **31**

COMPONENTE 31
DELIMITAR EL ALCANCE 31
IDENTIFICACIÓN DE ACTIVOS 31
DEFINICIÓN DE POLÍTICAS 31
EJECUTAR ANÁLISIS DIFERENCIAL 31

5.1 TIPO DE INVESTIGACIÓN 31
5.4 TÉCNICAS DE RECOLECCION 32
Observación *32*
Revisión de documentos *32*
Entrevistas *32*
5.2 POBLACIÓN 32
5.3 MUESTRA 32
5.5 LÍNEA DE INVESTIGACIÓN 33
6. RECURSOS 33
6.1 RECURSOS NECESARIOS 33
6.2 RECURSOS DISPONIBLES 33
7. SGSI PARA LA EPS 34
ACTIVIDADES 34
Fase 1. ..... *34*
Recolección de Información *34*
Fase 2. ..... *34*
Interpretación y análisis *34*
Fase 3. ..... *35*
Entrega de informe final *35*
FASE I. DIAGNOSTICO 35
DIAGNOSTICO SITUACION ACTUAL 35
RECOLECCIÓN DE ACTIVOS DE INFORMACIÓN 59
ANÁLISIS DE RIESGO 60
CUMPLIMIENTO ISO 27001:2013 64
OBJETIVOS DE CONTROL *66*
NIVEL BAJO DE CUMPLIMIENTO 66
NIVEL MEDIO DE CUMPLIMIENTO 67
NIVEL ALTO DE CUMPLIMIENTO 69
FASE II. PREPARACION 70
ANALISIS *70*
Dominios 70
8. DISEÑO DEL SGSI EN LA EPS ASMET SALUD 71
ALCANCE 71
POLITICA DEL SGSI 71
PLANIFICACION 72
CLASIFICACION DE ACTIVOS TECNOLÓGICOS *72*
Procesamiento y análisis de datos 73
FORTALEZAS Y DEBILIDADES *73*
GESTIÓN DOCUMENTAL 74

POLÍTICAS DE SEGURIDAD *74*
Control de acceso 74
Confidencialidad de la información 75
Propiedad intelectual 75
Software 75
Hardware 75
Uso de recursos 75
Correo electrónico 75
Usuarios y contraseñas 75
Auditorías internas *76*
Documental 76
Administración de indicadores *76*
ANÁLISIS DE RIESGOS 78
Aplicabilidad *78*
Parámetros *81*
Vulnerabilidad 81
Impacto 81
Efectividad del control 82
Análisis amenazas *82*
Impacto 82
Tipos de activos 82
Resultado de vulnerabilidades *83*
AUDITORIA DE CUMPLIMIENTO 84
Evaluación de cumplimiento 84
CONTROLES Y PLANES DE TRATAMIENTO 86
POLÍTICAS 89

9. MANUAL DE POLÍTICAS 92

INTRODUCCION 92
OBJETIVO 92
ALCANCE 92
REVISIÓN 92
GENERAL 93

10. PLAN DE CONTINUIDAD 96

ESTUDIO Y EVALUACIÓN DE RIESGOS 97
SELECCIÓN DE ESTRATEGIAS 97
EJECUCIÓN DEL PLAN 98
PRUEBAS Y MANTENIMIENTO 99

11. RESULTADOS 100

Análisis y discusión 100

12. CONCLUSIONES 103
13. RECOMENDACIONES 105
14. BIBLIOGRAFÍA 106
15. ANEXOS 109
AVAL PROYECTO DE GRADO 109
ENCUESTA REALIZADA A LOS FUNCIONARIOS DE LA EPS ASMET SALUD 110
RESULTADOS DE LA ENCUESTA 111

LISTADO DE TABLAS

TABLA 1 REQUISITOS NORMA NTC 27001 20
TABLA 2 LEY 1273 DEL 2009 26
TABLA 3 COMPONENTES ESTÁNDAR ISO/IEC 27001:2013 31
TABLA 4 TIPOS DE RECOLECCIÓN 32
TABLA 5 RECURSOS 33
TABLA 6 FASES DE EJECUCIÓN 34
TABLA 7 LISTA DE CHEQUEO 36
TABLA 8 PROMEDIO DE CALIFICACIÓN 39
TABLA 9 CLAUSULAS CONTEXTO DE LA ORGANIZACIÓN 40
TABLA 10 CLAUSULAS LIDERAZGO 41
TABLA 11 CLAUSULAS PLANIFICACIÓN 42
TABLA 12 CLAUSULAS SOPORTE 43
TABLA 13 CLAUSULAS OPERACIÓN 44
TABLA 14 CLAUSULAS EVALUACIÓN DE DESEMPEÑO 45
TABLA 15 CLAUSULAS MEJORA 46
TABLA 16 LISTA DE CHEQUEO DE CONTROLES 47
TABLA 17 CONTROLES POLÍTICAS DE SEGURIDAD 50
TABLA 18 CONTROLES ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 51
TABLA 19 CONTROLES SEGURIDAD DE LOS RECURSOS HUMANOS 51
TABLA 20 CONTROLES GESTIÓN DE LOS ACTIVOS 52
TABLA 21 CONTROLES CONTROL DE ACCESO 53
TABLA 22 CONTROLES CRIPTOGRAFÍA 54
TABLA 23 CONTROLES SISTEMA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO 55
TABLA 24 CONTROLES GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 56
TABLA 25 CONTROLES GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 57
TABLA 26 INVENTARIO DE ACTIVOS 59
TABLA 27 MATRIZ DE RIESGO VALORES 60
TABLA 28 VALORACIÓN DE IMPACTO 60
TABLA 29 PROBABILIDAD DE OCURRENCIA 61
TABLA 30 MATRIZ DE ELEMENTOS DE TOLERANCIA Y RESPUESTA A LOS RIESGOS 61
TABLA 31 VALORACIÓN DE POLÍTICAS DEL SGSI 62
TABLA 32 CUMPLIMIENTO DE CONTROLES 64
TABLA 33 CONTROLES CON BAJO NIVEL DE CUMPLIMIENTO 66
TABLA 34 CONTROLES CON NIVEL MEDIO DE CUMPLIMIENTO 67
TABLA 35 CONTROLES CON NIVEL ALTO DE CUMPLIMIENTO 69
TABLA 36 CUMPLIMIENTO 70
TABLA 37 DOMINIOS 70
TABLA 38 CLASIFICACIÓN DE RECURSOS 72
TABLA 39 NIVEL DE CUMPLIMIENTO 73

TABLA 40 FORTALEZAS DEBILIDADES 73
TABLA 41 INDICADORES DE GESTIÓN 77
TABLA 42 APLICABILIDAD 79
TABLA 43 FRECUENCIA DE VULNERABILIDAD 81
TABLA 44 IMPACTO 81
TABLA 45 VALORACIÓN 82
TABLA 46 AMENAZAS 83
TABLA 47 VULNERABILIDADES 83
TABLA 48 EVALUACIÓN DE CUMPLIMIENTO 84
TABLA 49 CONTROLES Y TRATAMIENTO DE RIESGOS 87
TABLA 50 POLÍTICAS 93
TABLA 51 PROCESOS DE LA EMPRESA 97
TABLA 52 EJECUCIÓN DEL PLAN 98
TABLA 53 NIVEL DE CONTROLES 100
TABLA 54 CUMPLIMIENTO POR DOMINIOS 101

LISTADO DE GRAFICAS

GRAFICA 1 PROMEDIO DE CALIFICACIÓN 39
GRAFICA 2 PROMEDIO NIVEL DE SEGURIDAD 40
GRAFICA 3 PROMEDIO CALIFICACIÓN CONTEXTO DE LA ORGANIZACIÓN 41
GRAFICA 4 PROMEDIO CALIFICACIÓN LIDERAZGO 42
GRAFICA 5 PROMEDIO CALIFICACIÓN PLANIFICACIÓN 43
GRAFICA 6 PROMEDIO CALIFICACIÓN SOPORTE 44
GRAFICA 7 PROMEDIO CALIFICACIÓN OPERACIÓN 45
GRAFICA 8 PROMEDIO CALIFICACIÓN EVALUACIÓN DE DESEMPEÑO 46
GRAFICA 9 PROMEDIO CALIFICACIÓN OPERACIÓN 46
GRAFICA 10 CONTROLES 5 POLÍTICAS DE SEGURIDAD 50
GRAFICA 11 CONTROLES 6 ORGANIZACIÓN DE LA SEGURIDAD 51
GRAFICA 12 CONTROLES 7 SEGURIDAD DE LOS RH 52
GRAFICA 13 CONTROL ES 8 GESTIÓN DE ACTIVOS 53
GRAFICA 14 CONTROLES 9 DE ACCESO 54
GRAFICA 15 CONTROLES 10 CRIPTOGRAFÍA 55
GRAFICA 16 CONTROLES 14 SISTEMA DE ADQUISICIÓN 56
GRAFICA 17 CONTROLES 16 GESTIÓN DE INCIDENTES 57
GRAFICA 18 CONTROLES 18 CUMPLIMIENTO 58
GRAFICA 19 CUMPLIMIENTO DE CONTROLES 65
GRAFICA 20 CONTROLES CON NIVEL BAJO CUMPLIMIENTO 66
GRAFICA 21 CONTROLES CON NIVEL MEDIO DE CUMPLIMIENTO 68
GRAFICA 22 CONTROLES CON NIVEL ALTO DE CUMPLIMIENTO 69
GRAFICA 23 INDICADORES DE GESTIÓN 78
GRAFICA 24 ESTADO DE MADUREZ 101
GRAFICA 25 ESTADO ACTUAL Y ESPERADO DE LOS DOMINIOS 102

LISTADO DE IMAGENES

IMAGEN 1 MODELO DE IMPLEMENTACIÓN 20
IMAGEN 2 RIESGOS SGSI 21
IMAGEN 3 PIRÁMIDE SGSI 22
IMAGEN 4 ACTIVOS DE SGSI ISO 27001 24
IMAGEN 5 CICLO PDCA 27

INTRODUCCION

En la actualidad la información está expuesta a diferentes amenazas, implementar un sistema para la preparación de registros de seguridad efectiva de los datos abarcando a todo el personal que hacen parte de estas organizaciones, empezando por los operarios hasta llegar a los directivos. Este proceso se conoce como SGSI, que se encuentra apoyado bajo los estándares internacionales, una de esas normas es la ISO/IEC 27001 que constituyendo con los procesos de mejoramiento de controles y políticas de seguridad continuamente.

Hoy en día la complejidad de la información como la dependencia de las empresas por adquirir nuevas tecnologías llevan a los expertos a afrontar nuevas amenazas que al pasar de los días toman más fuerza, llevando a las empresas a crear estrategias de resguardo de la información.

Se convierte en un privilegio de seguridad la necesidad de proteger la información, Asmet Salud es una EPS, la cual busca estandarizar las técnicas de información y garantizar la seguridad de los procesos, a través del establecimiento de SGSI. La realización del proyecto inspecciona el análisis y observación de peligros en relación con las políticas de la empresa.

En la EPS Asmet Salud no existen controles de seguridad para proteger la información, que a su vez pueda certificar la confidencialidad de manipulación de los datos al interior de la EPS. Se reconoce y detalla la estructura organizacional, mostrando en la actualidad el estado de la empresa basándonos a la norma ISO 27001:2013, definiendo estrategias y procesos a seguir, especificando las diferentes políticas a seguir en un SGSI.

Fundado en modelos, normas y estándares que con la utilización de buenas rutinas se pueda asegurar un manejo adecuado para la protección de información. La ISO/IEC 27001:2013 implanta instrucciones y técnicas para formalizar apropiadamente un proceso de mejoramiento continuo.

1. DEFINICIÓN DEL PROBLEMA

DESCRIPCION DEL PROBLEMA

Asmet Salud es una entidad prestadora de salud, la cual busca estandarizar sus sistemas operativos, garantizando las nuevas tecnologías de seguridad de información, a través del establecimiento Sistema de Gestión de la Seguridad de Información apoyado por el modelo ISO 27001:2013.

Teniendo en cuenta que Asmet Salud EPS no cuenta con políticas definidas en la protección de información dentro de la empresa, como tampoco no existe ningún tipo de distribución de responsabilidades y roles para la seguridad de los datos, no se cuenta con instrucciones de seguridad ante desastres naturales que lleguen a afectar los recursos de la empresa, una de las problemáticas que más se ve es el incorrecto uso de los activos tecnológicos, el inapropiado manejo del correo electrónico y la falta de control a la hora de navegar en Internet.

De esta manera, la empresa maneja un importante volumen de información que no cumple con las condiciones básicas de disponibilidad, confidencialidad e integridad que se encuentra expuesta a cualquier tipo de amenaza, por tal razón es fundamental que la EPS incorpore un SGSI, siguiendo lineamientos para cumplir con los objetivos y los requisitos determinados en cuanto a política de calidad, realizando un continuo mejoramiento en todos los procesos administrativos.

En la actualidad la EPS Asmet Salud no ostenta ningún control o técnica que permita identificar vulnerabilidades, riesgos, o ataques informáticos a lo que se expone la información, falta evidencia y documentación de instrucciones que logren resolver las insuficiencias y no poner en riesgo los recursos y activos de la empresa.

Al no detallar procedimientos y técnicas que permitan pronunciar apropiadamente las instrucciones que puedan certificar la disponibilidad, confidencialidad e integridad de la seguridad de los datos, se ve necesario poner en práctica un diseño de SGSI para poder disminuir los peligros y darle el procedimiento correcto a la información que maneja la empresa.

Por otra parte, la presencia de atacantes en las redes pone en peligro la información almacenada en lo equipos de la empresa, así como el mal uso que los empleados le dan a los activos, se debería manejar un marco de trabajo en la ejecución efectiva de controles de protección de la información.

La norma ISO/IEC 27001:2013 de seguridad de sistemas de información, es la cual está basado el diseño del SGSI, cuyo objetivo es efectuar los requerimientos

determinados dentro de las estrategias de calidad en la empresa en su continuo progreso de los diferentes métodos que se manejan.

Todas estas problemáticas que en un llegado tiempo puede desatar un conjunto de incidentes con relación a la administración de los datos e información. Cuando los servidores fallan pudría estar relacionado con el poco control que se realiza en la ejecución e instalación de software no validado o en actualización de procedimientos operativos.

Dentro la seguridad de la información milita diferentes tipos de peligros tanto técnicos como humanos, los funcionarios no resguardan o conservan la privacidad de los datos, manipulan los correos electrónicos institucionales para diferentes tipos de comunicación personal, utilizando gran variedad de contraseñas.

Por estos motivos, la intención de esta tesis es diseñar un SGSI en la EPS Asmet Salud apoyado en el modelo ISO/IEC 27001:2013, cuyo fin es catalogar las diferentes amenazas a los que se ve exhibida los datos, construir un instrumento que contenga políticas de seguridad para así poder resguardar la información sin miedo a perderla o ponerla en peligro.

El inconveniente reside en que no existe un SGSI en la EPS Asmet Salud; la intención de un SGSI, es minimizar riesgos y que estos sean conocidos por el personal de la empresa de forma eficiente y adaptando las medidas más importantes para salvaguardar la información estableciendo controles y políticas necesarias para la protección de los datos almacenados.

FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de un Sistema de Gestión de Seguridad de la Información apoyado en el modelo ISO/IEC 27001:2013, puede mitigar riesgos de disponibilidad, confidencialidad e integridad de recursos de información en la E.P.S. Asmet Salud?

2. JUSTIFICACIÓN

Las constantes reformas que se le realizan a la salud por parte del Gobierno Nacional exigen a las empresas invertir en tecnologías que apoyen la prestación de sus servicios[1]. El establecimiento de un SGSI, permitirá asegurar que la ejecución de controles adecuados sobre la disponibilidad, confidencialidad e integridad de los datos, adicional protegiendo el cumplimiento de la norma ISO 27001:2013[2], demostrando a sus clientes la seguridad con que se abordan los temas de protección de los datos.

Hoy en día la información se ha transformado en el recurso más valioso que toda empresa quiere proteger, ya sea de los ataques maliciosos o de los hackers que se quieren aprovechar de las vulnerabilidades afectando en muchos aspectos la confidencialidad, disponibilidad e integridad; por consiguiente, surge la necesidad de elegir dominios y métodos que ayuden a minimizar los riesgos de seguridad dentro de la empresa.

Para la EPS Asmet Salud es imprescindible resguardar y proteger los datos, dando cumplimiento a los fundamentos de disponibilidad, confidencialidad e integridad de la información, en atención a lo cual se debe efectuar componentes precisos que certifiquen el tratamiento correcto que se les dan a los datos de la empresa.

Un SGSI apoyado en el modelo ISO/IEC 27001:2013, suministrará escenarios necesarios para que la empresa garantice su gestión correspondiente, logrando optimizar las áreas con falencias relacionadas a la información dentro de la compañía, obteniendo mejor rendimiento en las tareas realizadas a diario de forma segura y rápida, facilitando la presentación de servicios necesarios.

Este proyecto es planteado viendo las necesidades que se presentan en la seguridad sobre los activos informáticos de la empresa por tanto requieren ser identificados y evaluados de acuerdo a sus amenazas y vulnerabilidades. Al verse perjudicada la información por distintas situaciones de tipo laboral, organizacional o de cualquier índole, es necesario corregir las circunstancias actuales y establecer una serie de protocolos de acuerdo a lo que estípula la norma ISO/IEC 27001:2013[3].

Por ende, para evitar que sea menoscabada la confianza de los funcionarios de la EPS, se ve preciso el levantamiento de inventario de activos, sus vulnerabilidades, amenazas, riesgos y grado de exposición, para determinar así los controles que deberán aplicarse poniendo en marcha la ejecución de SGSI.

---

[1] MINSALUD. Política de atención integral en salud. Tomado de: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/modelo-pais-2016.pdf

[2] ISOTools Colombia, Plataforma tecnológica para la gestión de la excelencia. Tomado de: https://www.isotools.com.co/plataforma-tecnologica-para-la-gestion-de-los-centros/

Un SGSI expone el compromiso de las empresas hacia la protección de los datos suministrando los componentes necesarios para establecer de forma eficaz los peligros que consigan quebrantar la protección de información, de modo que permitirá a la EPS cumplir los objetivos trazados, permitiendo organizar las bases necesarias para un apropiado modelo de seguridad garantizando su mejora continua.

Las compañías han tomado conciencia del valor que tienen los elementos de protección implementados, se ve la necesidad describir procesos que minimicen sucesos de protección de información, por lo tanto, el diseño de un SGSI apoyado en el modelo ISO 27001:2013, la cual brinda a la empresa identificar los riesgos informáticos, cumpliendo con los requerimientos de la norma.

Además, del resguardo de la información confidencial y los activos informáticos que se maneja dentro de la empresa, un SGSI facultara al departamento de sistemas emplear los diferentes tipos de prácticas de seguridad de la información como lo sugiere la norma ISO 27001:2013, generando conciencia al interior de los empleados sobre los riesgos que puede atravesar la información que es manipulada a través de prácticas y políticas que serán liderados por los administradores.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de Información bajo la norma ISO 27001:2013 para la EPS Asmet Salud, con la intensión de establecer soluciones en las áreas que presentan falencias de prestación de servicios que permita resguardar la disponibilidad, confidencialidad e integridad de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar el inventario de los diferentes activos informáticos que maneja la E.P.S Asmet Salud bajo la norma ISO 27001:2013.

- Priorizar los datos que maneja la EPS Asmet Salud, identificando las necesidades, requerimientos y vulnerabilidades que esta posee.

- Realizar el estudio de riesgos de la información de la EPS Asmet Salud bajo la norma ISO 27001:2013

- Establecer políticas y controles que garanticen la protección de información mediante el modelo ISO 27001:2013 minimizando riesgos identificados al interior de la empresa.

4. MARCO REFERENCIAL

4.1 MARCO TEORICO

Los diferentes procesos informáticos han llegado a lugares muy remotos de nuestro planeta, tocando todo punto de vista desde el empresarial hasta el personal, en la actualidad las empresas recopilan toda la información en diferentes bases de datos, las TI cumplen con un rol fundamental para llegar a la cima de todas las funciones establecidas, siendo la información que se maneja un componente clave para el éxito del negocio, no solo soportando estrategias de negocio ya existentes y que toda empresa emplea, sino también estando a la vanguardia de las nuevas tecnologías que evolucionan a pasos agigantados.

Los SGSI proporciona diferentes modelos en el establecimiento de la protección de los diferentes activos informáticos alcanzando los objetivos de la empresa, basados en la gestión de riesgos, aplicando las políticas y controles adecuados asegurando la implementación de cada uno de estos para su correcto funcionamiento. Incluyendo la empresa las diferentes políticas, procedimientos, y procesos basados en los diferentes estándares en gestión de seguridad.

"Norma ISO/IEC 27001 es una norma internacional que garantiza la utilización de controles para proteger los datos, puede ser implementada en cualquier empresa, proporcionando la metodología e implementación en la gestión de la seguridad de la información"[3].

"Norma ISO/IEC 27002. Anteriormente denominada ISO-17799, esta norma suministra pautas para la ejecución de los controles adecuados, 114 controles específicos que al ser utilizados se logra disminuir los riesgos de seguridad, esta norma se enfoca a todo tipo de empresa sin medir tamaño o naturaleza"[4].

"Norma ISO 27004 especifica como estructurar la medición de la seguridad de la información, este estándar estructura la medición los parámetros que se deben utilizar como y cuando se deben medir, ayudando a las organizaciones a cumplir con los objetivos de rendimiento y alcanzar el éxito"[5].

"Norma ISO 27005 se ocupa en la gestión de riesgos de seguridad de información, suministrando directrices para la gestión de riesgos, dando cumplimiento con los

[3] ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información, tomado de: http://www.lrqa.es/certificaciones/iso-iec27001/
[4] Seguridad de la información, tomado de https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/
[5] ISOTools, tomado de: https://www.isotools.cl/isoiec-27004/

exigencias de seguridad utilizando herramientas de detención de riesgos cibernéticos, apoyada por lo definido en la norma ISO 27001[6].

Cuando se habla de una nueva implementación esto se asocia con la evolución de las tecnologías, aunque hablamos en la forma como debemos valorar la información teniendo en cuenta los elementos que deben existir, asimismo hay que tener presente los diferentes riesgos que se encuentran en todas partes, no solo los informáticos si no también los naturales, humanos entre otros que puedan atacar las vulnerabilidades que hay dentro de los activos de información.

Este proyecto se apoya en diferentes percepciones permitiendo el avance hacia el objetivo propuesto, el diseño de un Sistema de Gestión de la Seguridad de la Información, destacando diferentes principios básicos: confidencialidad, disponibilidad e integridad.

Confidencialidad "es el respaldo por el cual la información está protegida ante cualquier ataque o de personas escrupulosas. Esta garantía se ejecuta por medio de reglas protegiendo la confidencialidad por medio de códigos especiales de identificación, en vez de utilizar nombres, también se pude limitar el número de personas el acceso a esta información manteniendo los datos protegidos"[7].

Disponibilidad habla de "la capacidad de garantizar la disposición de los datos y el sistema que los maneja en todo momento, siendo importante para la empresa la constancia de la información suministrada y guardada para que se encuentre disponible para los usuarios en el momento de ser solicitados"[8].

La mayoría de las empresas actualmente establecen procesos críticos que se efectúan de forma automática con el uso de nuevas tecnologías informáticas, confiando los datos que se suministra por los empleados del área de sistemas. Las tecnologías informáticas juegan un papel interesante en las diferentes estrategias de las empresas manteniendo una excelente relación con sus usuarios.

Es preciso que la empresa implante una metodología obteniendo una gestión apropiada de los datos, realizando un tratamiento de los riesgos para así lograr obtener el estado actual dentro de la protección de los recursos informáticos, determinar las vulnerabilidades que comprometen la protección de los datos para así poder establecer los diferentes elementos de seguridad que minimicen riesgos de disponibilidad, confiabilidad e integridad de la información.

---

[6] ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información, tomado de: https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

[7] Confidencialidad de la información tomado de: http://www.innsz.mx/opencms/contenido/investigacion/comiteInvestigacion/confidencialidadInformacion.html

[8] Confidencialidad, integridad y disponibilidad de la información tomado de: http://www.belt.es/expertos/HOME2_experto.asp?id=2245

Cuando se habla de integridad, se refiere a la "capacidad de garantizar la no modificación de los datos desde su creación, la información creada no puede ser manipulada sin autorización previa, siendo importante el cuidado de estos datos como los bancarios que hoy en día se manejan desde cualquier café internet o desde cualquier conexión a esta, garantizando que no sea manipulada o intrusos tengan acceso a esta"[5].

Seguridad de la información "son medidas que previenen y permiten proteger la información, a su vez manteniendo la disponibilidad, integridad y de datos al interior de la empresa, los hospitales y las empresas prestadoras de estos servicios manejan información confidencial por esta razón es necesaria la protección de estos datos de personas no autorizadas para la obtención de esta"[9].

"MAGERIT metodología de análisis y gestión de riesgos, relacionada con la utilización de uso de las tecnologías minimizando riesgos, generando confianza en el beneficio de los usuarios, basándose en los resultados obtenidos durante el análisis que se realiza"[10].

La implantación de un SGSI, sirve como instrumento de gestión permitiendo conocer, formalizar y minimizar los peligros que logren perjudicar la seguridad de la información de la EPS, utilizando estas acciones se puede resguardar la empresa frente a los diferentes peligros que pueden poner en riesgo la conformidad para alcanzar los objetivos.

Debido al permanente progreso de las tecnologías de información que exigen un mayor esfuerzo en el respaldo de la protección de los datos, las amenazas que también han evolucionado y cada vez son más precisas y avanzadas, atacando las debilidades más sensibles, para esto es preciso que las compañías cuenten con un SGSI apoyado en estándares de seguridad con la intención de poder mantener una seguridad alineada con las necesidades estratégicas de la empresa.

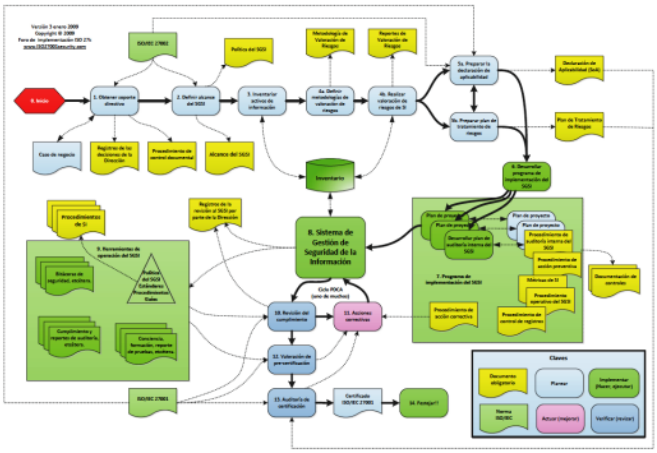
La norma ISO/IEC 27001:2013 detalla los requerimientos necesarios en la instauración o mejorar, teniendo en cuenta los diferentes riesgos que puedan generarse al interior de una empresa, puntualizando el diseño de un SGSI implantando dominios conforme a las necesidades de la empresa, la norma ISO/IEC 27001:2013 se apoya en el ciclo PDCA[11], comprendiendo los siguientes pasos para una buena documentación:

- **Procedimientos:** Suministran las instrucciones generando bases de acuerdo a las actividades.
- **Políticas:** Facilitan las pautas habituales de acción en cada caso.

[9] Gestión de seguridad de la información, tomado de: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/
[10] ISO 27001: El método MAGERIT, tomado de https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/
[11] ISOTools, https://www.isotools.org/evento/metodologia-implementacion-sgsi-pe7ago/

- **Registros:** Son las conclusiones que se adquieren en la duración de realización de las tareas.

Imagen 1 Modelo de implementación



Fuente: http://www.iso27000.es/doc_certificacion_all_archivos/image005.jpg

Instituto Colombiano de Normas Técnicas (ICONTEC) adopta la norma ISO/IEC 27001:2013 bajo la referencia NTC-ISO-IEC 27001[12], presenta diferentes requisitos que son necesarios para llevar a cabo lo señalado dentro de la norma. El contenido de la empresa determina el alcance, los límites y capacidad, certificando el cumplimento de la norma del SGSI en los temas internos y externos que puedan intervenir en los resultados esperados.

Tabla 1 Requisitos Norma NTC 27001

Requisitos	Descripción
Liderazgo	Se debe comprobar el cumplimiento de las políticas instauradas por la norma, asignando responsabilidades para su continuo mejoramiento.
Planificación	Se debe establecer una metodología para establecer los controles necesarios para mantener los óptimos niveles de seguridad.
Soporte	Se debe realizar una comunicación frecuente en cuanto a las políticas de seguridad para comprometer al mejoramiento continuo de la norma.
Operación	Se debe fundamentar cada proceso para llevar a cabo las actividades para valorar los peligros a los que se halla expuesta la empresa.

[12] Noviembre 11 de 2013, primera actualización

Evaluación	Vigilar las prácticas de protección de información midiendo la validez del SGSI, para verificar su optimo cumplimiento.
Mejora	Se deben aplicar correcciones necesarias y promover el mejoramiento continuo.

Fuente: el autor

Para entender que es el SGSI, se debe tener en cuenta que este ayuda a establecer los procedimientos y las condiciones de seguridad en relación a los propósitos y metas de la empresa, manteniendo un nivel de exposición bajo frente a los diferentes riesgos. Ver Imagen 2.

Imagen 2 Riesgos SGSI

Fuente: www.ISO27000.es

Beneficios al implementar un SGSI:

- Establece una sistemática en gestión de seguridad.
- Reduce riesgos de pérdida de la información.
- Permanentemente se hace revisión de controles y riesgos.
- Se identifican las debilidades gracias a las diferentes auditorías dentro de un SGSI.
- Cumple con la reglamentación actual sobre información personal, propiedad intelectual entre otras.
- Minimiza costos a la hora de realizar mejora de los procesos en el servicio.

Como lo determina la norma ISO 27001 los procesos se definen de forma integral, a la hora de efectuar un proyecto de análisis se debe seguir un camino, agrupando y ordenando las tareas que se designan dentro de la empresa, además incluye todas las dificultades para conseguirlo, la documentación de un SGSI se ha mostrado siempre como una pirámide de 4 niveles, los cuales se constituyen así:

Imagen 3 Pirámide SGSI

Fuente: www.ISO27000.es

Manual de seguridad nivel 1. Este nivel cumple eficazmente a la hora de dirigir e inspira todo el sistema, establece y explica los propósitos, objetivos, metas, responsables, controles, etc., que se manejan dentro de un SGSI.

Procedimientos nivel 2. Se manejan todos los documentos operacionales, que certifican la realización en carácter eficaz la programación, manipulación y control de las técnicas y métodos de protección de información.

Instrucciones, checklists y formularios nivel 3. En este nivel se puntualiza la forma de realización de procesos, labores y trabajos específicos relacionados con la protección de información.

Registros nivel 4. Aquí se suministran las diferentes evidencias que deben cumplir con las obligaciones del SGSI; a su vez se asocian los instrumentos de los niveles preliminares como salida, demostrando el cumplimiento con las diferentes indicaciones.

4.2 MARCO CONCEPTUAL

“Riesgos Informáticos, incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos, como equipos informáticos, periféricos, instalaciones, programas de cómputo, etc."[13], el peligro dentro de una cadena de requisitos que tenemos que entender su significado dentro del contexto de la seguridad de la información; podemos encontrar:

La disponibilidad “supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados”[14].

“La confidencialidad se conoce como una forma de prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados”[15], la información personal no se ventila a personas ajenas que no tienen que ver con la empresa, así se busca acertar con los compromisos de garantizar este tipo de datos.

La integridad “supone que la información se mantenga inalterada ante accidentes o intentos maliciosos, sólo se podrá modificar la información mediante autorización, el objetivo de la integridad es prevenir modificaciones no autorizadas de la información”[16].

Los activos informáticos son aquellos recursos (hardware y software) de alta validez que sujeta la información de vital importancia en cualquier empresa que al mismo tiempo debe ser protegida ante cualquier riesgo o amenaza, compone el proceso completo de comunicación dentro de la empresa y se encuentran relacionados.

Un ataque intencionado es originado por individuos que no tienen ninguna autorización por parte de la empresa, estos son los que realizan ataques o manipulan los equipos o la información de la empresa para de esta forma obtener beneficios propios, afectando el funcionamiento de los sistemas operativos.

---

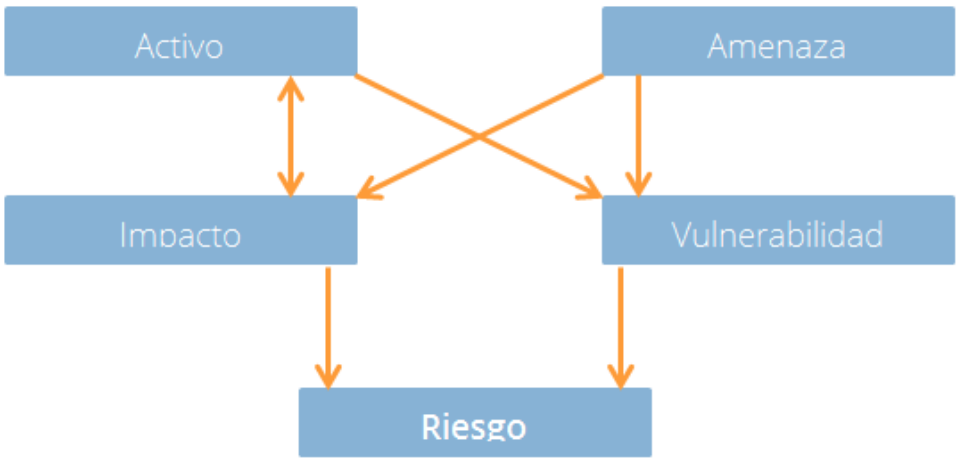
[13] Galeón.com, Riesgos informáticos, tomado de: http://auditoriadesistemas.galeon.com/productos2223863.html

[14] Blog especializado en Sistemas de Gestión de Seguridad de la Información, tomado de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

[15] SGSI, Blog especializado en Sistemas de Gestión de Seguridad de la Información, tomado de: https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

[16] Blog especializado en Sistemas de Gestión de Seguridad de la Información, tomado de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Imagen 4 activos de SGSI ISO 27001



Fuente: https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

Amenaza “es un riesgo al que estas expuestas las empresas que no cuentan con los equipos adecuados, expuestas a cualquier tipo de ataque informático, se tienden a llamar virus que solo es una de las tantas amenazas que hoy en día pueden afectar los datos e información que deseamos proteger sea personal o empresarial”[17].

Vulnerabilidad “son las debilidades que hay en los sistemas, estos pueden ser manipulados a la hora de ocasionar daños en el sistema operativo, actualmente existen muchos programas que pueden ayudar a que los sistemas operativos no presenten errores de programación, navegadores como Internet explorer entre otros, presentan profundos problemas de seguridad e inconvenientes en su funcionamiento diario los cuales los hackers los utilizan para realizar sus ataques y cumplir con sus malas intenciones”[18].

En las metodologías de análisis hay diferentes tipos para realizar el estudio y la evaluación de peligros informáticos, todos de distintas formas y manejando de forma diferente las situaciones, sin embargo, existen actividades que se manejan de la misma forma para el cumplimiento de diferentes actividades.

Para poder identificar las amenazas hay que encargarse de la identificación de estas que puedan afectar o dañar los activos que tienen relación con la protección de información, las amenazas constantemente hacen presencia sin darnos cuenta y son las causantes de daños y perjuicios dentro de la empresa.

[17] https://www.monster.es/orientacion-laboral/articulo/amenazas-informaticas
[18] https://tecnologia-informatica.com/vulnerabilidades-informaticas/

La identificación de vulnerabilidades se orienta en identificar las distintas vulnerabilidades que se pueden presentar o ser manipuladas por personas con malas intenciones, generando riesgo a los diferentes dispositivos de seguridad o las que puedan afectar directamente la diferente información que es manejada por la EPS.

La identificación de activos es el proceso que se realiza a cada tipo de activos que se encuentran críticos, que tienen relación directa en la confidencialidad, disponibilidad e integridad de los datos en la empresa, estos activos pueden ser datos, hardware, software, servicios, documentos y recursos humanos.

Los diferentes mecanismos para identificar los controles que sirven para detectar de donde provienen las amenazas que quieren atacar el sistema de información como también los diferentes salvaguardas que se podrían utilizar para mitigar los diferentes ataques.

4.3 MARCO LEGAL

En Colombia la legislación ha evolucionado para contrarrestar toda clase de delitos informáticos, en la actualidad existen normas que perciben elementos relacionados con el buen uso de las TICS. Algunas de estas leyes son:

“Ley 1273 del 2009. Se crean nuevas penas. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”[19].

Con gran importancia esta ley, fue adicionada al código penal colombiano llamada “de la protección de la información y de los datos”[20], se fracciona en 2 partes que suministran los artículos: Utilización de software malicioso, Violación de datos personales, Acceso abusivo a un sistema informático, Capturar de datos personales mediante suplantación, Apropiación de datos informáticos.

Se componen dos (2) capítulos con sus artículos en esta ley:

[19] Ley 1273 de 2009, MINTIC, tomado de: https://www.mintic.gov.co/portal/604/w3-article-3705.html
[20] Diario oficial, Ley 1273 de 2009, tomado de: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Tabla 2 Ley 1273 del 2009

Capítulos	Artículos	Explicación
CAPÍTULO PRIMERO "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"	**Artículo 269A.** Acceso abusivo a un sistema informático	Cuando se aprovechan las debilidades y se procede a ingresar en un sistema de información.
	Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación.	Se bloquea el sistema sin permiso o se impide el ingreso.
	Artículo 269C. Interceptación de datos informáticos.	Se intercepta de forma ilegal la información que es transmitida.
	Artículo 269D. Daño Informático.	Se elimina, malogra o perturba la información o equipos sin tener permiso.
	Artículo 269E. Uso de software malicioso.	Cuando se hace instalación y uso de un software que no es legal ni tiene permisos.
	Artículo 269F. Violación de datos personales.	Se toman los datos e información que existen en los equipos de empresas.
	Artículo 269G. Suplantación de sitios web para capturar datos personales.	Se crean paginas similares a las originales para tomar los datos e información que es valiosa.
	Artículo 269H. Circunstancias de agravación punitiva	Se hace pública la información confidencial de las empresas.
CAPÍTULO SEGUNDO "De los atentados informáticos y otras infracciones"	**Artículo 269I.** Hurto por medios informáticos y semejantes.	Se extrae la información sin permiso de los administradores de la empresa para hacerse pasar por otras personas.
	Artículo 269J. Transferencia no consentida de activos.	se hace pública la información robada con el ánimo de solicitar dinero para su recuperación.

Fuente: Ley 1273 de 2009, MINTIC

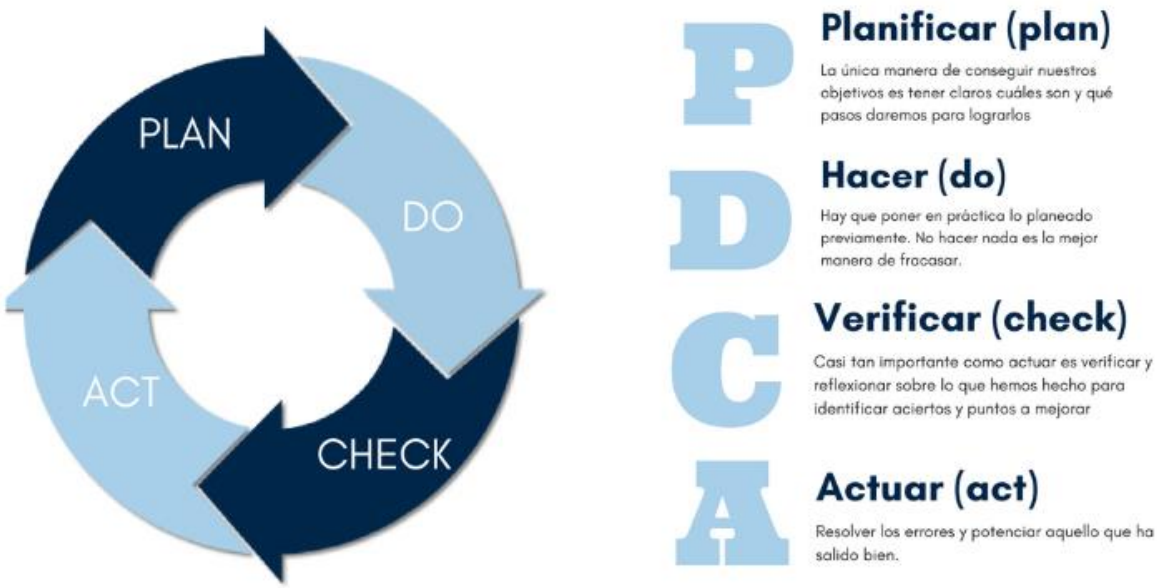
“Ley 1288 de 2009. Por medio del cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones”[21].

“ISO/IEC 27001:2005. Publicada el 15 de octubre de 2005, es el principal estándar de la familia de la ISO27000, y contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información. Se origina en la BS 7799-2:2002 y es la norma sobre la cual se certifican, por medio de auditores externos, los SGSI de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los controles no

[21] Congreso de la república, tomado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1288_2009.html

implementados. Recomienda el uso del ciclo Plan – Do – Check – Act para el diseño de un SGSI”[22].

Imagen 5 Ciclo PDCA



Fuente: https://www.stocklogistic.com/ciclo-pdca-mejora-logistica/

“Ley 1341 de 2009. Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"[23].

“Ley Grooming Argentina (Ley 26.904 – noviembre 2013). Según su Artículo 1°, que se incorporó como artículo 131 al Código Penal: Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma”[24].

“Ley especial contra delitos informáticos en Venezuela. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales

[22] Networking online, “Normas ISO/iec 27001,27002 y su estructura”, tomado de: http://jfherrera.wordpress.com/tag/isoiec-27000/.
[23] MINTIC, Ley 1341 de 2009, tomado de: https://www.mintic.gov.co/portal/604/w3-article-3707.html
[24] Ley de Grooming, tomado de: https://www.argentinacibersegura.org/noalgrooming/ley-de-grooming

sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley"[25].

"Ley No 30096 de Perú. La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia"[26].

4.4 MARCO CONTEXTUAL

ASMET SALUD EPS, "es una entidad establecida el 11 de diciembre del año 2015 a través de documento privado por la Asamblea Constitutiva, patentada en la Cámara de Comercio del Cauca bajo el número 38672, su cede principal está ubicada en la ciudad de Popayán (Cauca), representada por su Gerente General, el Dr. GUSTAVO ADOLFO AGUILAR VIVAS, y habilitada por la Superintendencia Nacional de Salud, según Resolución 127 de 2018"[27].

"Administra recursos del régimen subsidiado en salud, bajo un esquema de aseguramiento, de conformidad con la ley 100 de 1993 y normas reglamentarias, autorizada para entrar en operación desde el 01 de abril de 2018, compuesta por los siguientes órganos sociales para su dirección, administración y representación; Asamblea General de Accionistas, Junta Directiva y Gerencia General, con las facultades y atribuciones conferidas por los estatutos y la ley"[28].

Normatividad.

"Ley 1566 de 2012. Por la cual se dictan normas para garantizar la atención integral a personas que consumen sustancias psicoactivas"[29], es decretada por el congreso de Colombia el día 31 de julio del año 2012 y consta de 12 artículos los cuales reglamentan los temas relacionados con la atención que deben recibir personas que son adictas a sustancias psicoactivas.

"Ley 1616 de 2013. Por medio de la cual se expide la Ley de Salud Mental y se dictan otras disposiciones"[30] es decretada por el congreso de Colombia el 21 de

---

[25] Gaceta oficial de la república bolivariana de Venezuela, tomado de: https://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf
[26] LEY DE DELITOS INFORMÁTICOS LEY Nº 30096, tomado de: http://www.derecho.usmp.edu.pe/cedetec/normas/Ley_Delitos_Informaticos_Ley_30096.pdf
[27] Asmet Salud EPS, tomado de https://www.asmetsalud.org.co/corporativo
[28] Asmet Salud EPS, tomado de https://www.asmetsalud.org.co/corporativo
[29] Ley 1566 de 2012, tomado de file:///C:/Users/jofer/Downloads/ley1566de2012-1.pdf
[30] Ley 1616 de 2013, tomado de file:///C:/Users/jofer/Downloads/LEY_201616_20DEL_2021_20DE_20ENERO_20DE_202013.pdf

enero de 2013 cuyo objetivo es garantizar el ejercicio pleno del derecho que tienen las personas con problemas de salud mental.

“Ley 1733 de 2014. Ley Consuelo Devis Saavedra, mediante la cual se regulan los servicios de cuidados paliativos para el manejo integral de pacientes con enfermedades terminales, crónicas, degenerativas e irreversibles en cualquier fase de la enfermedad de alto impacto en la calidad de vida”[31]

“Ley 1751 de 2015. Por medio de la cual se regula el Derecho Fundamental a la Salud y se dictan otras disposiciones”[32], es decretada por el Congreso de Colombia y cuyo objetivo es garantizar los derechos fundamentales para la salud y los mecanismos de protección.

“Acuerdo 029 de 2011. Por el cual se sustituye el acuerdo 28 de 2011 que define, aclara y actualiza integralmente el Plan Obligatorio de Salud, se define el plan obligatorio de salud por la comisión reguladora en salud en ejercicio de sus facultades legales”[33].

“Acuerdo 032 de 2012. Por el cual se unifican los Planes Obligatorios de Salud de los Régimenes Contributivo y Subsidiado a nivel nacional, para las personas de dieciocho (18) a cincuenta y nueve (59) años de edad y se define la Unidad de Pago por Capitación UPC del Régimen Subsidiado”, modifica los planes obligatorios de salud (POS)[34].

“Decreto 1355 de Julio de 2018. Por el cual se modifica el Decreto 780 de 2016, Único Reglamentario del Sector Salud y Protección Social, en relación con el manejo de los recursos de propiedad de las entidades territoriales destinados al aseguramiento de la población afiliada al Régimen Subsidiado”[35].

“Decreto 1273 de Julio de 2018. Por el cual se modifica el artículo 2.2.1.1.1.7, se adiciona el Título 7 a la Parte 2 del Libro 3 del Decreto 780 de 2016, Único Reglamentario del Sector Salud y Protección Social, en relación al pago y retención de aportes al Sistema de Seguridad Integral y Parafiscales de los trabajadores independientes y modifica los artículos 2.2.4.2.2.13 y 2.2.4.2.2.15 del Decreto 1072 de 2015, Único Reglamentario del Sector Trabajo”[36].

“Decreto 710 de 2018. Por el cual se sustituye el Capítulo 3 del Título 2 de la Parte 5 del Libro 2 del Decreto 780 de 2016, Único Reglamentario del Sector Salud y

---

[31] Ley 1733 de 2014, tomado de file:///C:/Users/jofer/Downloads/Ley_201733_20de_202014_20__20Cuidado_20Paliativo.pdf
[32] Ley 1751 de 2015, tomado de: file:///C:/Users/jofer/Downloads/ley_1751_del_16_de_febrero_de_2015___ley_estatutaria_de_salud.pdf
[33] Acuerdo 029 de 2011, tomado de: https://www.asmetsalud.org.co/filedownload/show/title/acuerdo-029-de-2011-1413818472-0.89447800/src/@random54412c9a1e630
[34] Acuerdo 032 de 2012, tomado de: file:///C:/Users/jofer/Downloads/acuerdocres032de2012unificacionpos-1.pdf
[35] Decreto 1355 de 2018, tomado de: file:///C:/Users/jofer/Downloads/Decreto_1355_de_2018.pdf
[36] Decreto 1273 de 2018, tomado de: file:///C:/Users/jofer/Downloads/DECRETO_682_HABILITACION_18042018.pdf

Protección Social, en relación con las condiciones para la autorización de funcionamiento, habilitación y permanencia de las entidades responsables del aseguramiento en salud"[37].

CONTEXTO DE LA EMPRESA

La importancia de percibir y los elementos internos y externos de la empresa se pueden replicar gracias al modelo ISO/IEC 27001:2013, dentro estos elementos se pueden ver afectados por la ejecución del SGSI de manera positiva o negativa. Por esta razón, las políticas constituyen que la EPS determine las circunstancias y componentes cuando se ve rodeada en el momento de establecer al Sistema de Gestión de Seguridad de la Información.

CONOCIMIENTO DE LA EMPRESA

NATURALEZA

La E.P.S. Asmet Salud se encuentra ubicada en el municipio de Timana Huila, es una propiedad tomada en arriendo de dos pisos, en el primer piso funciona atención a usuarios y en segundo piso funcionan la parte administrativa incluyendo la parte de sistemas en el cual se manejan toda la parte informática y se encuentran los swichet, routers, entre otros equipos informáticos.

"Administra recursos del régimen subsidiado en salud, bajo un esquema de aseguramiento, de conformidad con la ley 100 de 1993 y normas reglamentarias, autorizada para entrar en operación desde el 01 de abril de 2018, compuesta por los siguientes órganos sociales para su dirección, administración y representación; Asamblea General de Accionistas, Junta Directiva y Gerencia General, con las facultades y atribuciones conferidas por los estatutos y la ley"[38].

MISION DE LA EMPRESA

"Somos una aseguradora en salud que, a través de un modelo de gestión integral del riesgo, contribuimos al mejoramiento de las condiciones de salud de nuestros afiliados"[39].

---

[37] Decreto 710 de 2018, tomado de: file:///C:/Users/jofer/Downloads/Decreto_710_de_2018.pdf
[38] Asmet Salud EPS, tomado de https://www.asmetsalud.org.co/corporativo
[39] Asmet Salud EPS, tomado de https://www.asmetsalud.org.co/corporativo

VISION DE LA EMPRESA

“Al 2023 seremos la mejor opción de aseguramiento social en salud, generando confianza en el sector y sostenibilidad financiera"[40].

5. DISEÑO METODOLÓGICO

Este proyecto se basa en un enfoque mixto, es preciso realizar diferentes actividades presentadas en el modelo ISO/IEC 27001:2013, dando inicio del presente proyecto, guiados por el planteamiento del problema en busca de alcanzar los propósitos planteados, se definen los siguientes componentes:

Tabla 3 Componentes estándar ISO/IEC 27001:2013

Componente	Descripción
Delimitar el Alcance	Definir los servicios, las áreas y los procesos en donde será aplicado el SGSI.
Identificación de Activos	Se ejecuta el levantamiento de activos que serán abordados para identificar y ejecutar el estudio de las amenazas que puedan perturbar la garantía de los datos de la empresa.
Definición de Políticas	Basándonos con las necesidades de la empresa, se plantean los objetivos básicos referentes de la protección de información, garantizando la disponibilidad, confidencialidad e integridad.
Ejecutar Análisis Diferencial	Se deben detectar las falencias que hay dentro de la empresa, determinando el nivel de cumplimiento y conformidad en que se encuentra la misma.

Fuente: el autor

5.1 TIPO DE INVESTIGACIÓN

Para este proyecto se utilizará una metodología tanto cuantitativa y a su vez cualitativa partiendo de los diferentes anexos que proporciona la norma ISO/IEC 27001:2013, manejando un proyecto aplicado basado en la investigación de campo, para la administración de riesgos con la intención de implementación del SGSI,

[40] Asmet Salud EPS, tomado de https://www.asmetsalud.org.co/corporativo

implementando una estructura de trabajo para que los miembros participen de las decisiones considerando los riesgos procedentes del uso tecnológico.

- ❖ Generar conciencia por la existencia de riesgos y las necesidades que existen al interior de la empresa.
- ❖ Descubrir, planificar el tratamiento oportuno para mantener los sistemas.
- ❖ Realizar procesos de auditoria, acreditación y evaluación según corresponda.

5.4 TÉCNICAS DE RECOLECCION

En la ejecución del presente proyecto se manejarán los siguientes métodos de recolección:

Tabla 4 Tipos de recolección

Técnica	Descripción
Observación	Asumir un enfoque claro del estado actual en que se encentra la empresa y hasta dónde quiere llegar.
Revisión de documentos	Nos faculta tener proyección para saber en qué estado se encuentra la empresa actualmente.
Entrevistas	En esta técnica se utilizarán preguntas de tipo abiertas y cerradas. ➢ Recolección de datos ➢ Análisis de sistemas operativos ➢ Clasificación y análisis e políticas de seguridad del sistema. Análisis de resultados.

Fuente: el autor

5.2 POBLACIÓN

La población que se tendrá en cuenta para la realización de las entrevistas son los funcionarios de la empresa.

5.3 MUESTRA

Se define como población a 10 funcionarios de la empresa Asmet Salud, dando cumplimiento a los objetivos del proyecto.

5.5 LÍNEA DE INVESTIGACIÓN

Para efectuar un SGSI en la empresa Asmet Salud se establece como factor inicial el modelo ISO/IEC 27001:2013, planteando temas en gestión de seguridad, y cumpliendo con las actividades.

6. RECURSOS

6.1 RECURSOS NECESARIOS

Tabla 5 Recursos

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	Ingeniero de sistemas	$ 2.000.000
Equipos y Software	1 Computador portátil: ❖ Procesador: Intel I3-3110M 2.4G ❖ Sistema Operativo WINDOWS 10 ❖ Discos Duro de 1 Tera ❖ Pantalla de 14" HD LED ❖ Memoria RAM 8 Gb ❖ Motor Gráfico Nvidia GTX ❖ BLUETOOTH 4.0 original en Motherboard ❖ 1 Puerto HDMI ❖ 1 RANURA LECTORA DE TARJETAS SD	$ 2.800.000
	1 Conexión inalámbrica Antena Wifi Usb Encore	$ 100.000
	2 Dispositivos USB	$ 64.000
	1 Sistema operativo Linux, software libre	$ 0
Viajes y Salidas de Campo		$ 0
Materiales y suministros		$ 0
TOTAL		**$ 4.964.000**

Fuente: Jonathan Fernando Reyes

6.2 RECURSOS DISPONIBLES

Se cuenta con el consentimiento de la parte administrativa de la empresa Asmet Salud, la documentación requerida para el impulso de este proyecto.

Se dispone de diferentes recursos necesarios frente el estudio del presente proyecto, se cuenta con internet, computador portátil con procesador Core I3, disco duro portable, USB, y demás que se necesiten.

Se tiene permiso para acceder a los dispositivos de cómputo, con la disposición y el apoyo de los funcionarios de la EPS.

7. SGSI PARA LA EPS

Se definen las diferentes técnicas para el diseño del SGSI de la EPS Asmet Saluden esta parte del proyecto, por tanto, se examinan las actividades cuya práctica admite conseguir los propósitos que se establecieron. Se relacionan los elementos como la información que fue recogida, se realizan las deducciones para cada una de las tareas que se manejan en las fases definidas para el diseño del SGSI.

ACTIVIDADES

Partiendo de las políticas establecidas por el modelo ISO/IEC 27001:2013 la cual describe observaciones en la ejecución de controles en seguridad en la E.P.S. Asmet Salud, se pondrá en funcionamiento acatando una serie de fases que permitan cumplir los propósitos y metas proyectados de acuerdo a las necesidades de la EPS.

Tabla 6 Fases de ejecución

FASES	DESCRIPCIÓN DE LA ACTIVIDAD
Fase 1. Recolección de Información	Se utilizan fuentes de tipo bibliográfico como documentos electrónicos, dando cumplimiento a los objetivos de este proyecto Exploración de documentos existentes al interior de la empresa sobre SGSI. Tipificación de vulnerabilidades existentes en la empresa en cuanto a seguridad informática para la aplicación de un SGSI.
Fase 2. Interpretación y análisis	El propósito de esta fase es aplicar las técnicas y estrategias basadas en la norma ISO, para encontrar los controles específicos que se pueden aplicar o que ya están siendo aplicados en el interior de la empresa.

Fase 3. Entrega de informe final	Se exponen los resultados obtenidos dentro del informe, manifestando los controles y políticas que son necesarias aplicar para protección de datos e información.

Fuente: El autor

FASE I. DIAGNOSTICO

DIAGNOSTICO SITUACION ACTUAL

La seguridad informática para Asmet Salud, como en otras empresas del sector, significa una sobrecarga de información, dando pauta a personas no autorizadas para que puedan acceder, alterar, vulnerar o robar información, hackear los dispositivos y activos donde se almacena la información que es de uso confidencial y de uso empresarial.

Se requiere proteger los bienes importantes de la empresa como procesos, datos e información que es suministrada a diario frente a delitos, para no colocar en peligro la disponibilidad, confidencialidad e integridad de los procesos que se llevan dentro de la empresa, por eso la importancia de un diseño SGSI apoyado en la norma ISO 27001:2013.

Asmet Salud EPS en la actualidad, con respecto al departamento de seguridad de la información, se encuentra en desventaja con respecto a otras EPS, puesto que las campañas publicitarias, especialmente las relacionadas con sus usuarios se ven muy expuestas al plagio, al manejar niveles casi nulos de confidencialidad.

El análisis GAP se realiza como parte de identificación del estado actual de cumplimiento de la EPS Asmet Salud, en cuanto a la protección de los datos, se realizó en cuanto respecta a dominios descritos basados en el modelo ISO 27001:2013, mediante el uso de la herramienta GAP se determina el estado actual y el estado al que se quiere llegar.

A partir del análisis que se realice posterior a la obtención de los resultados, se dará a conocer el estado actual de la EPS, respecto al cumplimento de los requisitos y controles definidos por la norma ISO27001:2013 en el diseño de un SGSI y las acciones y recursos que serán requeridos para lograr el cumplimiento del estado al que se desea llegar partiendo del estado en el que se encuentra actualmente la empresa.

Para llevar a cabo la revisión se utilizó una lista de verificación apoyada en los principios de la norma ISO 27001:2013, el cuestionario que se formuló a manera de

entrevista, se aplicó al ingeniero Oscar Javier Medina Garzón encargado del departamento de sistemas de la E.P.S. Asmet Salud.

El cuestionario se compone de preguntas según la norma ISO 27001:2013, el campo descripción donde se encuentra la pregunta que fue formulada al ingeniero de la oficina de sistemas, un campo de comentarios, donde se encuentran descritas las respuestas dadas a los interrogantes, campo observaciones/hallazgos donde el auditor tiene espacio para hacer las observaciones que considere necesarias, porcentaje de implementación, es una calificación dada en porcentajes del 0 al 100% en relación a la situación real de la E.P.S. Asmet Salud.

Tabla 7 Lista de chequeo

LISTA DE CHEQUEO

Fecha de verificación:

15	8	2018

Fecha de elaboración:

17	8	2018

Objetivo	Realizar revisión para establecer el estado actual de cumplimientos de requisitos respecto al modelo ISO 27001:2013
Alcance	Revisión controles según lo establecido por la norma ISO 27001:2013
Auditor	Jonathan Fernando Reyes Artunduaga
Encuestado	Oscar Javier Medina Garzón

Criterio norma ISO 27001:2013	Descripción	Comentarios	Observación	Porcentaje
CONTEXTO DE LA EPS				
Comprensión de la empresa y su contexto	¿La empresa determina las cuestiones que son pertinentes para la finalidad de SGSI?	Se tienen identificados los factores, pero no se cuenta con ningún tipo de documentación	N/A	20%
Conocimiento de las necesidades y expectativas	¿Cómo determinan los requisitos pertinentes al SGSI?	Se pueden incluir las obligaciones legales y contractuales.	N/A	20%
Determinación del alcance del SGSI	¿Cómo se establece el alcance de los límites del SGSI?	Considerar las diferentes cuestiones que se plantean en los dos numerales anteriores para definir procesos y alcance para documentar todos los procesos.	Los límites del SGSI serán definidas en el diseño que se entregue	0%
Sistema de gestión de la seguridad de la información	¿Cómo se establece, mantiene y mejora el SGSI?	Si se cumplen los parámetros, se debe formalizar su implementación de	No existe la implementación, mantenimiento y mejora continua del	0%

		acuerdo a los procesos que tenga definidos la empresa.	SGSI ya que no existe.	
LIDERAZGO				
Liderazgo y compromiso	¿Se tiene una política de seguridad?	No existe	N/A	0%
	¿La EPS dispone de recursos destinados al SGSI?	Se dispone de una persona como apoyo al proceso de la información sobre los procesos en los cuales se basa el diseño del SGSI	N/A	50%
	¿Se ha informado a la organización de la necesidad de un SGSI?	Se dio una capacitación a la gerencia de la EPS sobre la importancia.	N/A	50%
Política	¿Asmet Salud cuenta con políticas de seguridad para la información?	No existen	N/A	0%
Roles, responsabilidades y autoridades en la organización	¿Hay roles definidos en la EPS?	No se cuentan con roles definidos	N/A	0%
PLANIFICACIÓN				
Acciones para tratar riesgos y oportunidades	¿Cómo se planifican las labores para tratar los riesgos y oportunidades?	No hay una matriz de riesgos	N/A	0%
	¿Se cuenta con un proceso de valoración de riesgos?	No cuenta con este proceso	N/A	0%
	¿La EPS reconocen las vulnerabilidades de seguridad de Información?	No	N/A	0%
	¿Está definido y documentado el proceso de tratamiento de riesgos?	No se encuentra definido	N/A	0%
	¿Están determinados los controles para el manejo de riesgos?	No existen controles	N/A	0%
Objetivos de seguridad de la información y planes para lograrlo	¿Están establecidos los propósitos de seguridad de la información?	No se encuentran establecidos	N/A	0%
SOPORTE				
Recursos	¿Se han determinado recursos para el establecimiento de un SGSI?	No se han determinado	N/A	0%
Competencias	¿Hay conocimiento de los funcionarios de la empresa respecto a la seguridad dela información?	Los funcionarios hacen una prueba de manejo de tecnologías para el respectivo ingreso	N/A	20%

Toma de conciencia	¿Los empleados conocen las políticas, objetivos y los beneficios del SGSI?	No Cuenta con políticas	N/A	0%
Información documentada	¿Se encuentran documentadas las políticas, objetivos e información general del SGSI?	No cuenta con documentación	N/A	0%
OPERACIÓN				
Planificación y control operacional	¿Son definidas las actividades basadas en los requisitos de la seguridad de información?	No se han definido	N/A	0%
Valoración de riesgos de seguridad de la información	¿Llevan a cabo valoraciones de riesgo en la seguridad de la información?	No	N/A	0%
Tratamiento de riesgos de la seguridad de la información	¿Se han generado planes de tratamiento de los riesgos?	No se ha generado	N/A	0%
EVALUACIÓN DE DESEMPEÑO				
Seguimiento, medición, análisis y evaluación	¿Se mide el desempeño del SGSI?	No se mide	N/A	0%
Auditoria interna	¿Están planificados y establecidos programas en auditorías internas?	No	N/A	0%
MEJORA				
Mejora continua	¿Se evidencia mejora de la convivencia, adecuación, y eficacia del SGSI?	No	N/A	0%

Fuente: el autor

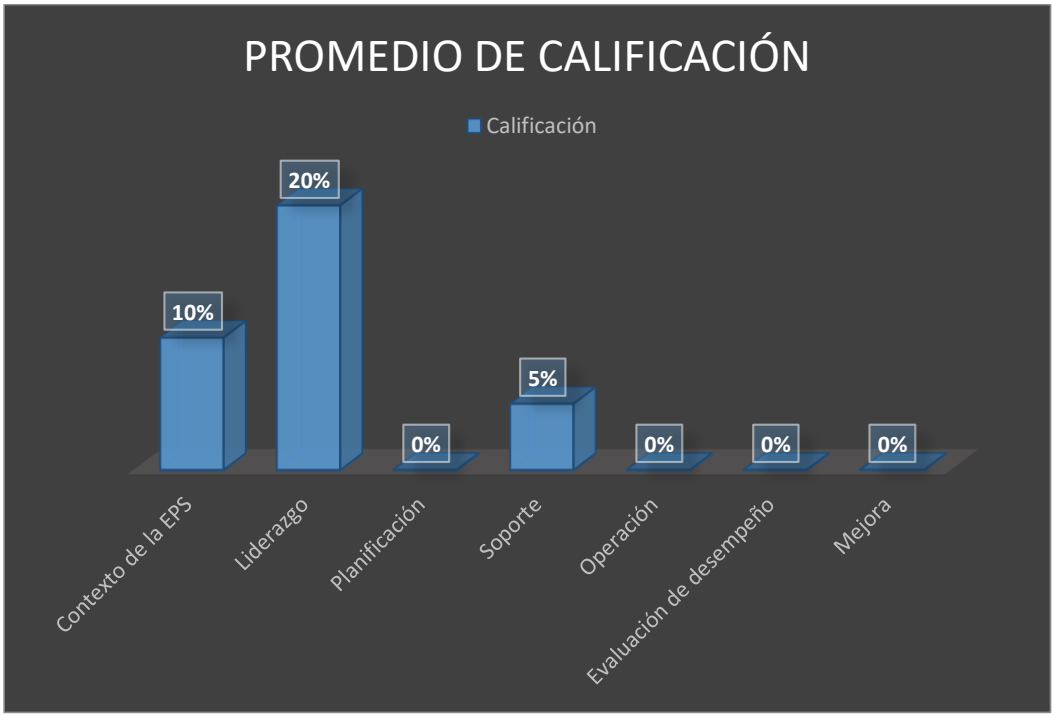
Llevado a cabo el análisis de las respuestas e identificando los hallazgos, evidencias, controles y partiendo de un criterio de análisis al cuestionario definido en el mismo formato, se puede ver la calificación que refleja el nivel de cumplimiento de la E.P.S. Asmet Salud, respecto a la norma ISO 27001:2013. Promedio de calificación numerales 4 al 10 norma ISO 27001:2013, el cual corresponde a un 3% de cumplimiento total respecto a los dominios de la norma, el 97% restante corresponde a incumplimientos, procesos existentes no documentados, cumplimientos parciales o en casos puntuales numerales que no aplican a los requerimientos definidos en la tabla 7.

Tabla 8 Promedio de calificación

Pregunta evaluada	Calificación
Contexto de la EPS	10%
Liderazgo	20%
Planificación	0%
Soporte	5%
Operación	0%
Evaluación de desempeño	0%
Mejora	0%
Nivel de seguridad	**5%**

Fuente: el autor

Grafica 1 Promedio de calificación



Fuente: el autor

Con respecto a los resultados obtenidos en la revisión, en el diseño se plantea como objetivo de cumplimiento en la totalidad de los controles, no se puede asegurar que en un 100%, para el caso particular de la EPS se ha puesto un umbral del 70%, aclarando que los dominios referentes a auditorías y mejora continua no son de cumplimiento en esta primera fase y quedan sujetos a disposición de la E.P.S. Asmet Salud.

Cumplimiento de los controles de las preguntas hechas en la lista de chequeo de acuerdo a la norma ISO 27001:2013. Promedio de calificación de las mismas en cuanto al modelo ISO 27001:2013 se evidencia el nivel de seguridad en la siguiente gráfica.

Grafica 2 Promedio nivel de seguridad

Fuente: el autor

Contexto de la EPS. Se realizó el proceso de tipificación de los factores que tienen algún tipo de impacto sobre el objetivo de la empresa, estos incluyen clientes, proveedores, competencia, proyectos en ejecución y por ejecutar; El hecho de que la seguridad de la información es un requisito y para este caso en especial una necesidad puesto que el conocimiento de la seguridad informática en la empresa está muy por debajo de los niveles que se consideran aceptables.

Tabla 9 Clausulas contexto de la organización

CONTEXTO DE LA ORGANIZACIÓN	
Conocimiento de la EPS y su contenido	20%
Conocimiento de las necesidades y expectativas	20%
Determinación del alcance del SGSI	0%
SGSI	0%

Fuente: el autor

Grafica 3 Promedio calificación contexto de la organización

Fuente: el autor

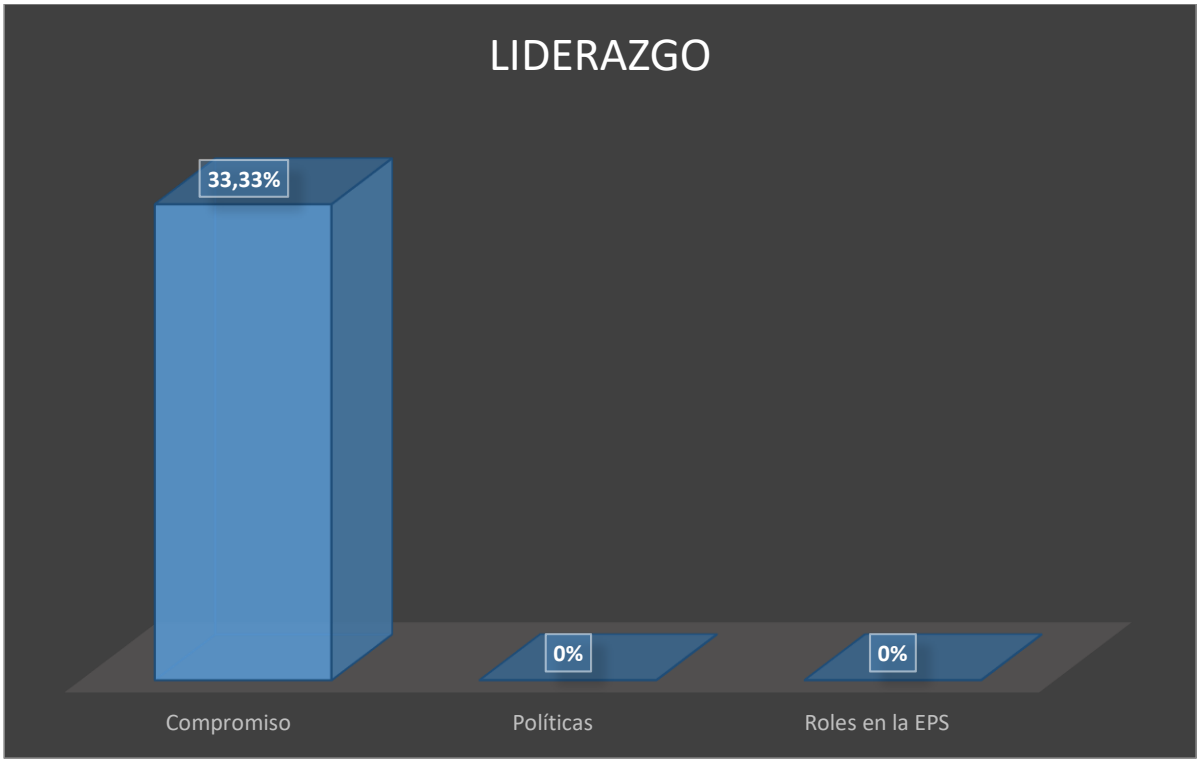
Liderazgo. Las áreas directamente participantes de la empresa como lo son la gerencia y la oficina de sistemas tienen conocimiento y plena conciencia de que la seguridad informática es una necesidad para ellos, se evidencian las falencias principales, como la documentación, las políticas y la falta de dirección de los procesos que en el momento se aplican. Como parte del apoyo al proceso del diseño del SGSI para la EPS Asmet Salud, la gerencia ha dispuesto de los recursos de información sobre procesos específicos y un recurso humano en la oficina de sistemas, para llevar a cabo este proceso.

Tabla 10 Clausulas Liderazgo

LIDERAZGO	
Compromiso	33.3%
Políticas	0%
Roles en la EPS	0%

Fuente: el autor

Grafica 4 Promedio calificación Liderazgo



Fuente: el autor

Planificación. Se identifica la necesidad de llevar a cabo un análisis de vulnerabilidades sobre los componentes de la infraestructura informática de Asmet Salud EPS, ya que al día de hoy no se cuenta con ningún análisis de este tipo que nos brinde la oportunidad de identificar el grado de vulnerabilidad frente a las amenazas de dispositivos informáticos y la información.

Tabla 11 Clausulas Planificación

PLANIFICACIÓN	
Acciones para minimizar riesgos	0%
Objetivos de seguridad	0%

Fuente: el autor

Grafica 5 Promedio calificación Planificación

Fuente: el autor

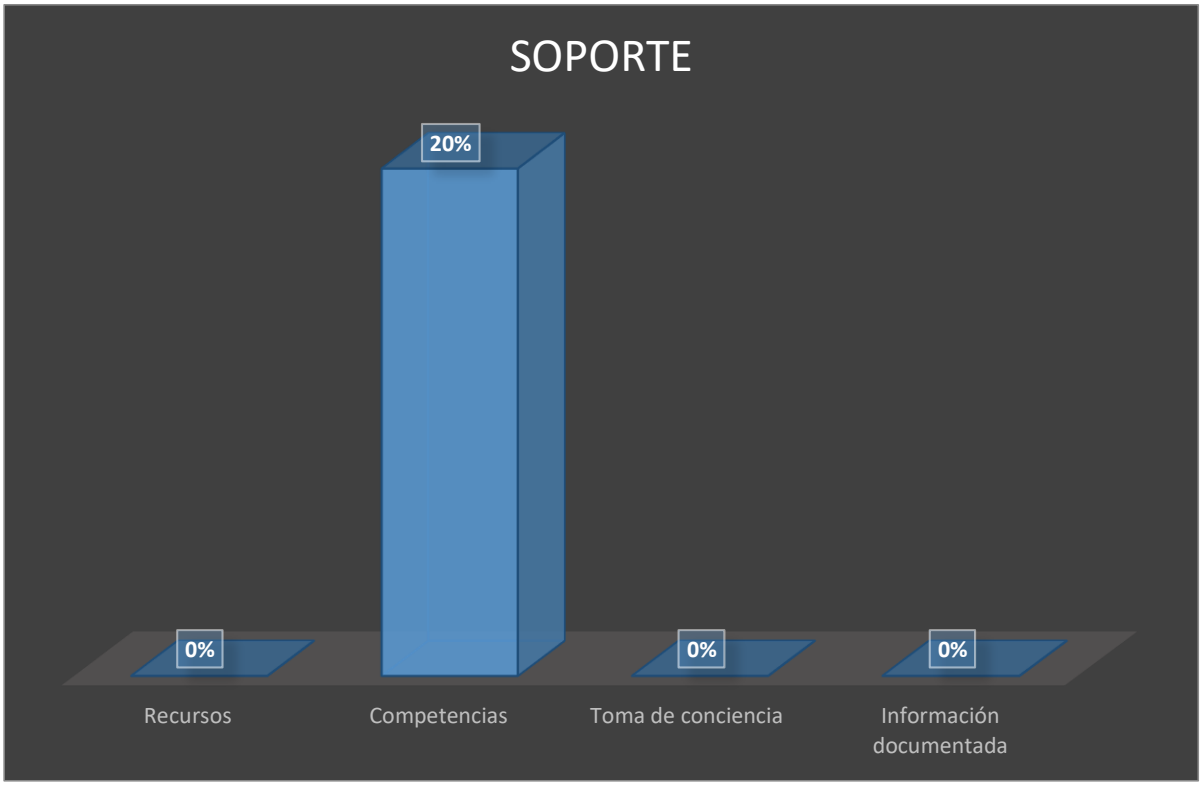
Soporte. Debido a que la empresa no cuenta con políticas definidas, ni instrucciones de seguridad documentados, la mayoría de los empleados de la empresa no conocen instrucciones o lineamientos sobre las técnicas procesos adecuadas dando cumplimiento con los estándares de protección de información.

Tabla 12 Clausulas Soporte

SOPORTE	
Recursos	0%
Competencias	20%
Toma de conciencia	0%
Información documentada	0%

Fuente: el autor

Grafica 6 Promedio calificación Soporte



Fuente: el autor

Operación. El proceso de mejora continua no está contemplado, debido a que sin existir una implementación, políticas o tratamiento de riesgos no hay ninguna medición que permita llevar un proceso de mejora

Tabla 13 Clausulas Operación

OPERACIÓN	
Planificación y controles	0%
Valoración de amenazas	0%
Tratamiento de riesgos	0%

Fuente: el autor

Grafica 7 Promedio calificación Operación

Fuente: el autor

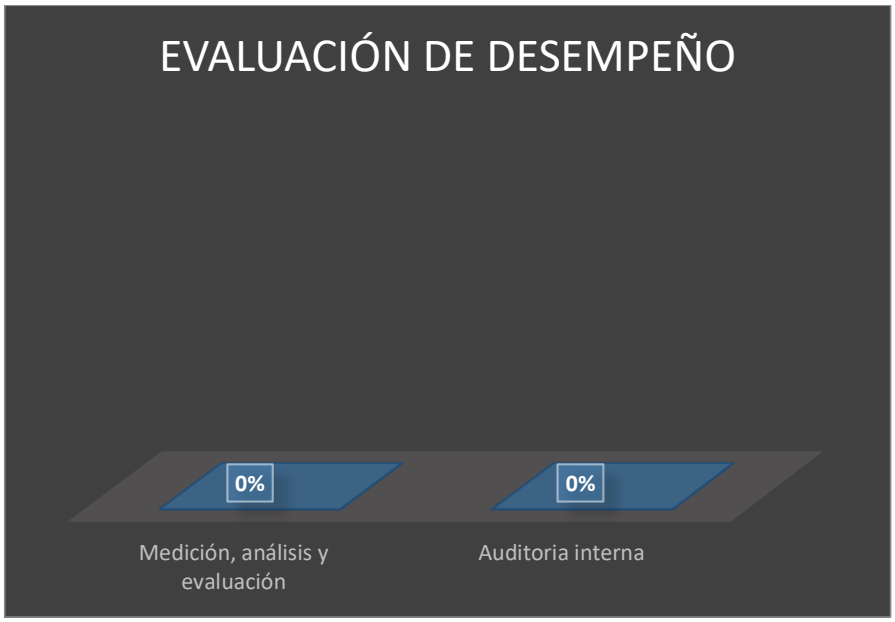
Evaluación de desempeño. no es posible llevar a cabo una evaluación de desempeño como tal, ya que al no estar documentado ningún proceso de seguridad de la información, no existe ninguna actividad sobre la cual medir el desempeño.

Tabla 14 Clausulas Evaluación de desempeño

EVALUACIÓN DE DESEMPEÑO	
Medición, análisis y evaluación	0%
Auditoria interna	0%

Fuente: el autor

Grafica 8 Promedio calificación Evaluación de desempeño



Fuente: el autor

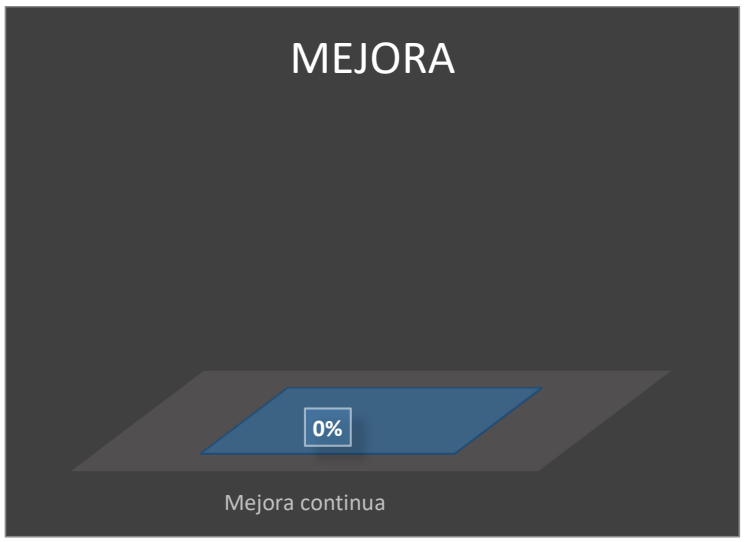
Mejora. No hay ninguna actividad definida sobre la cual se pueda hacer mediciones para generar un plan de mejora.

Tabla 15 Clausulas Mejora

MEJORA	
Mejora continua	0%

Fuente: el autor

Grafica 9 Promedio calificación Operación



Fuente: el autor

Tabla 16 Lista de chequeo de controles

LISTA DE CHEQUEO DE CONTROLES

Fecha de verificación:

15	8	2018

Fecha de elaboración:

17	8	2018

Objetivo	Realizar revisión para establecer el estado actual de cumplimientos de requisitos y controles respecto al modelo ISO 27001:2013
Alcance	Revisión controles norma ISO 27001:2013
Auditor	Jonathan Fernando Reyes Artunduaga
Encuestado	Oscar Javier Medina Garzón

Criterio norma ISO 27001:2013	**Descripción**	**Comentarios**	**Observación**	**Porcentaje**
5 POLÍTICAS DE SEGURIDAD				
5.1 Normas establecidas en la protección de información				
5.1.1 Directrices de seguridad	¿Se evidencia existencia de políticas, para la seguridad?	No hay evidencia de ningún tipo.	N/A	0%
5.1.2 Revisión de las políticas	¿La organización revisa, las políticas de seguridad?	No.	N/A	0%
6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
6.1 Clasificación interna				
6.1.1 Roles y responsabilidades	¿De qué manera se evidencia la asignación de roles?	No se encuentra definida	No hay roles de seguridad definidos	0%
6.1.2 División de deberes	¿La organización garantiza que las responsabilidades respecto a la seguridad?	No se evidencia esta asignación porque el área no está definida	N/A	0%
7 SEGURIDAD DE RECURSOS HUMANOS				
7,1 Durante la ejecución				
7.1.1 Responsabilidades	¿La EPS, exige a sus empleados el cumplimiento de las políticas de seguridad definidas?	Desde el momento que ingresan se les exige cumplimiento	Si se realiza la solicitud de cumplimiento	60%
7.1.2 Toma de conciencia	¿Se incluye la formación y concienciación a los empleados sobre la seguridad?	No	N/A	0%
7.1.3 Proceso disciplinario	¿Existe el proceso disciplinario formal para emprender acciones de violación a la seguridad?	No	N/A	0%
8 GESTIÓN DE ACTIVOS				
8.1 Compromiso				
8.1.1 Inventario	¿Se han identificado los activos de información para el cumplimiento de tareas?	Existe inventario de equipos y activos de información que pertenecen a la EPS	N/A	80%

8.1.2 Uso de activos	¿Se han definido políticas en las cuales se establecen los usos aceptables de los activos?	Existen diferentes definiciones para el uso de los activos	N/A	40%
8.1.3 Devolución	¿Aquellos activos que son propiedad de la organización deben ser retornados por los empleados/contratistas al finalizar la relación laboral?	Si	N/A	40%
8.2 Clasificación de información				
8.2.1 Clasificación información	¿Se ha clasificado información de acuerdo a los principios de la EPS?	La información se maneja de acuerdo a su clasificación y valoración de confidencialidad	N/A	40%
8.2.2 Disposición de los medios	¿Se ha definido un proceso para identificar la información de acuerdo a la clasificación?	La única definición es la de confidencialidad	N/A	40%
8.2.3 Manejo de información	¿Se ha definido un proceso para la administración de activos de acuerdo con la clasificación?	Si	N/A	40%
9 CONTROL DE ACCESO				
9.1 Obligaciones en el control de acceso				
9.1.1 Política de control	¿Se ha definido una política de acceso de acuerdo a los objetivos del negocio?	Si hay políticas	N/A	80%
9.2 Gestión de acceso a usuarios				
9.2.1 Registro y cancelación del registro	¿Se tiene implementado algún proceso para la creación y eliminación de cuentas de usuario?	Si	N/A	40%
9.2.2 Gestión de información de autenticación	¿Se tiene implementado un proceso para autenticación secreta?	No	N/A	0%
9.3 Responsabilidades del usuario				
9.3.1 Uso de la información de autenticación secreta	¿Se exige cumplimiento a los empleados la ley de confidencialidad?	No	N/A	0%
10 CRIPTOGRAFÍA				
10.1 Inspecciones criptográficos				
10.1.1 Políticas sobre el uso de controles	¿Existen políticas sobre el uso de controles criptográficos?	No	No están definidas	0%
10.1.2 Gestión de llaves	¿Existes procedimientos para el uso de llaves criptográficas?	No	No se cuenta con información cifrada	0%
14 SISTEMA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO				
14.1 Requisitos de seguridad				
14.1.1 Análisis y descripción de necesidades	¿Se definen obligaciones relacionados con seguridad?	No se encuentra definidos	N/A	0%

14.2 Seguridad en las técnicas de soporte				
14.2.1 Políticas de desarrollo seguro	¿Se contemplan aspectos de Desarrollo Seguro?	No aplica	No se aplica ningún tipo de desarrollo	0%
14.2.2 Ambiente de desarrollo seguro	¿Se establecen y protegen los ambientes de desarrollo?	No aplica	No se aplica ningún tipo de desarrollo dentro de la empresa	0%
14.2.3 Protección de datos de prueba	¿Cómo se asegura la protección de datos?	No aplica	N/A	0%
16 INFORMACIÓN EN GESTIÓN DE INCIDENTES DE SEGURIDAD				
16.1 Gestión de incidentes				
16.1.1 Reporte de debilidades de seguridad de información	¿Cómo se exige a todos los empleados que informen cualquier debilidad de seguridad de la información?	Se tienen controles para reportes de incidentes	Falta documentación de reportes	20%
16.1.2 Evaluación	¿Se tiene una metodología para decidir si un evento de seguridad se considera como un incidente de seguridad?	No se tiene ninguna metodología	N/A	0%
16.1.3 Responsabilidad y procedimientos	¿Se tiene establecida una política en la que se incluyan responsabilidades y procedimientos para la gestión de incidentes?	Se tienen políticas establecidas para reportes de incidentes	Falta documentación de políticas	40%
16.1.4 Recolección de evidencias	¿Se tiene definido un procedimiento para la identificación de evidencia originada por un incidente de seguridad?	No se tienen procedimientos definidos	N/A	0%
18 CUMPLIMIENTO				
18.1 Desempeño de requisitos legales y contractuales				
18.1.1 Derechos de propiedad intelectual	¿Qué procedimientos tiene implementados para asegurar los derechos de propiedad intelectual?	Si, se cuenta con gestión de calidad	N/A	40%
18.1.2 Reglamentación de controles criptográficos	¿Se usan controles criptográficos en la organización de reglamentación pertinentes?	No hay controles reglamentados	N/A	0%
18.1.3 Revisión de seguridad de la información	¿Cómo y con qué frecuencia revisa el enfoque de la seguridad?	No se realiza	N/A	0%
18.1.4 Desempeño con las políticas y normas de seguridad	¿Se revisa la normatividad de seguridad?	No se realiza	N/A	0%
18.1.5 Observación del cumplimiento técnico	¿Se hace revisión de los sistemas de información periódicamente?	No se realiza	N/A	0%

Fuente: el autor

Respecto a los resultados derivados en la lista de chequeo de controles, se puede establecer que la mayoría de estos controles no se cumplen según lo establecido

por la norma ISO 27001:2013, aclarando que los controles referentes a auditorías y mejora continua no son de cumplimiento en esta primera fase y quedan sujetos a disposición de la EPS Asmet Salud.

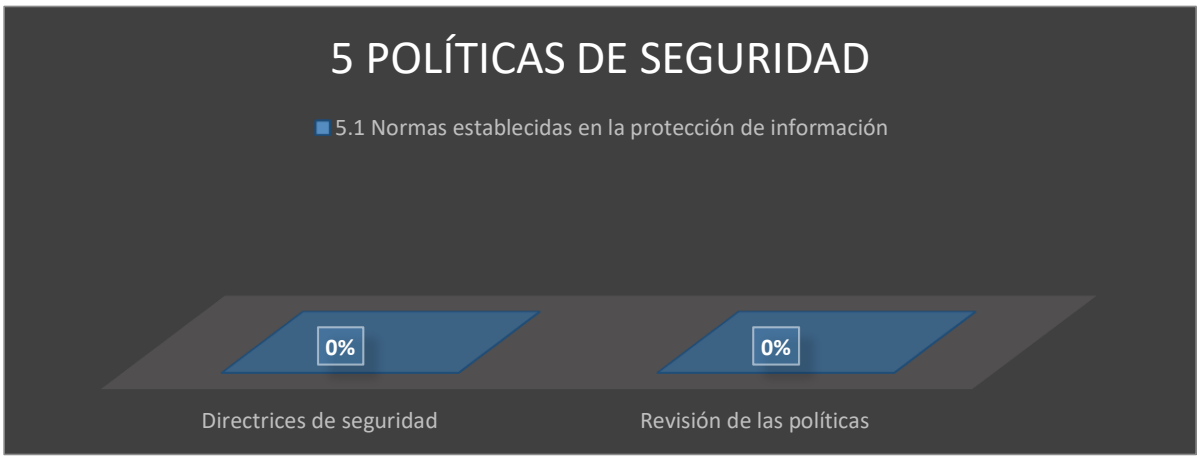
5 Políticas de Seguridad: Este numeral no cumple con lo determinado por la norma ISO 27001:2013 se puede observar que los numerales secundarios que se desprenden se encuentran en un nivel de cumplimiento de 0%, esto debido a que no existe una política definida, ni documentada por lo tanto tampoco se han hecho los procesos de aprobación y divulgación de la política por parte de la gerencia.

Tabla 17 Controles Políticas de seguridad

5 POLÍTICAS DE SEGURIDAD	
5.1 Normas establecidas en la protección de información	
5.1.1	Directrices de seguridad
5.1.2	Revisión de las políticas

Fuente: el autor

Grafica 10 Controles 5 Políticas de seguridad



Fuente: el autor

6 Organización de Seguridad de la información: Asmet Salud EPS no posee definidas áreas de seguridad, tampoco una persona que se encargue de las tareas que tienen que ver con estos temas, el personal del departamento de sistemas se dedica solamente con cosas que se manejan normalmente. La responsabilidad en cuanto al cumplimiento de la normatividad relacionada, es responsabilidad esencial de gerencia, se contempla la aplicabilidad de está en cuanto al impacto directo con la empresa y las consecuencias del cumplimiento o no de las mismas.

Todos los numerales secundarios del control 6 Organización de Seguridad de la información tienen un nivel de ejecución cumplimiento del 0% por lo tanto no cuenta con ninguna política para dispositivos móviles, a pesar de que los únicos

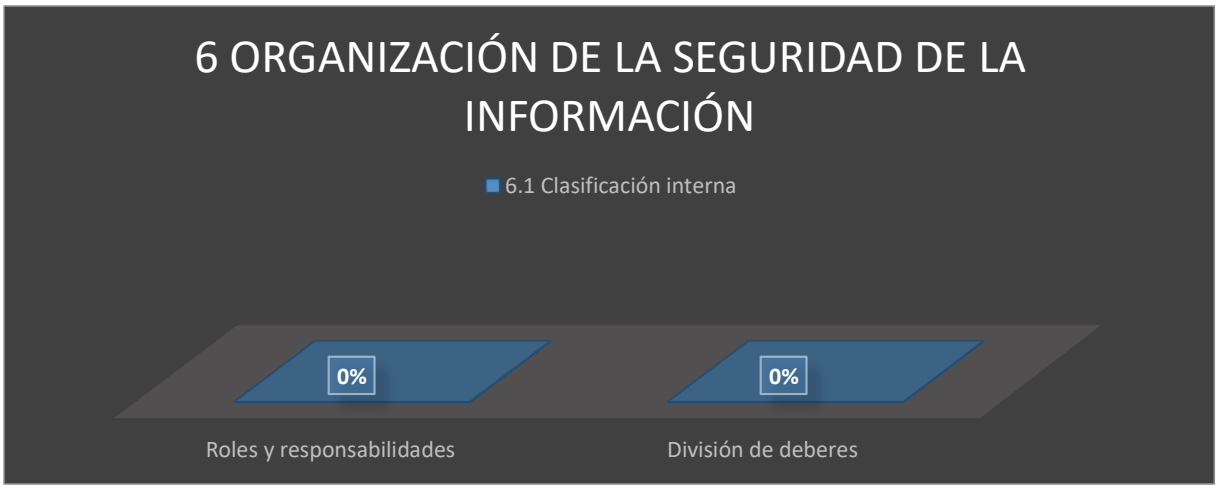
dispositivos móviles que se usan en la empresa son personales no se debe descartar una política para el uso de los mismos, el teletrabajo no está contemplado por el momento en la EPS.

Tabla 18 Controles organización de la seguridad de la información

6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1 Clasificación interna	
6.1.1	Roles y responsabilidades
6.1.2	División de deberes

Fuente: el autor

Grafica 11 Controles 6 Organización de la seguridad



Fuente: el autor

En la figura anterior se percibe que la EPS Asmet Salud no tiene definido roles y responsabilidades como tampoco división de deberes, no cuenta ni tiene definidas áreas de seguridad.

7 Seguridad de los recursos humanos: Una vez en ejecución del empleo no hay forma de hacer control o exigir que se cumpla con estándares de seguridad de los datos, debido a la no existencia, no se ponen en funcionamiento tecnicas de sensibilización ni tampoco concienciación a empleados, tampoco se encuentra definida una política o un proceso de cambio de funciones o terminación del contrato, solo un proceso sencillo de terminación del contrato y liquidación.

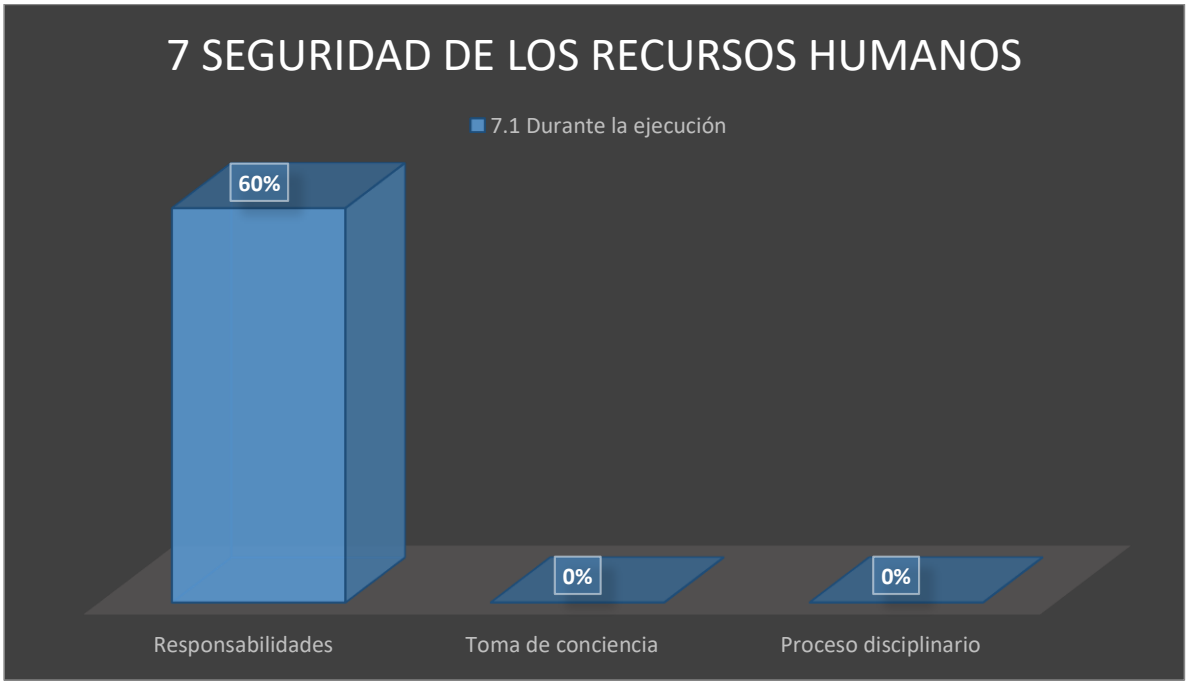
Tabla 19 Controles Seguridad de los recursos humanos

7 SEGURIDAD DE LOS RECURSOS HUMANOS	
7.1 Durante la ejecución	
7.1.1	Responsabilidades

7.1.2	Toma de conciencia
7.1.3	Proceso disciplinario

Fuente: el autor

Grafica 12 Controles 7 Seguridad de los RH



Fuente: el autor

8 Gestión de los Activos: La empresa mantiene registro de sus activos informáticos, audiovisuales y demás activos que son propiedad de la EPS Asmet Salud, aunque no se cuenta con registro de recursos de información que permitan cumplir con lo determinado en el modelo ISO 27001:2013. La empresa cuenta con un proceso no documentado donde se asegura de alguna forma que los empleados regresen los activos que les han sido asignados.

No se tiene una política definida sobre clasificación y uso de la información donde se tenga en cuenta el nivel de confidencialidad de la misma según lo descrito en la normatividad, considerando los pilares de seguridad como son, disponibilidad, confidencialidad e integridad.

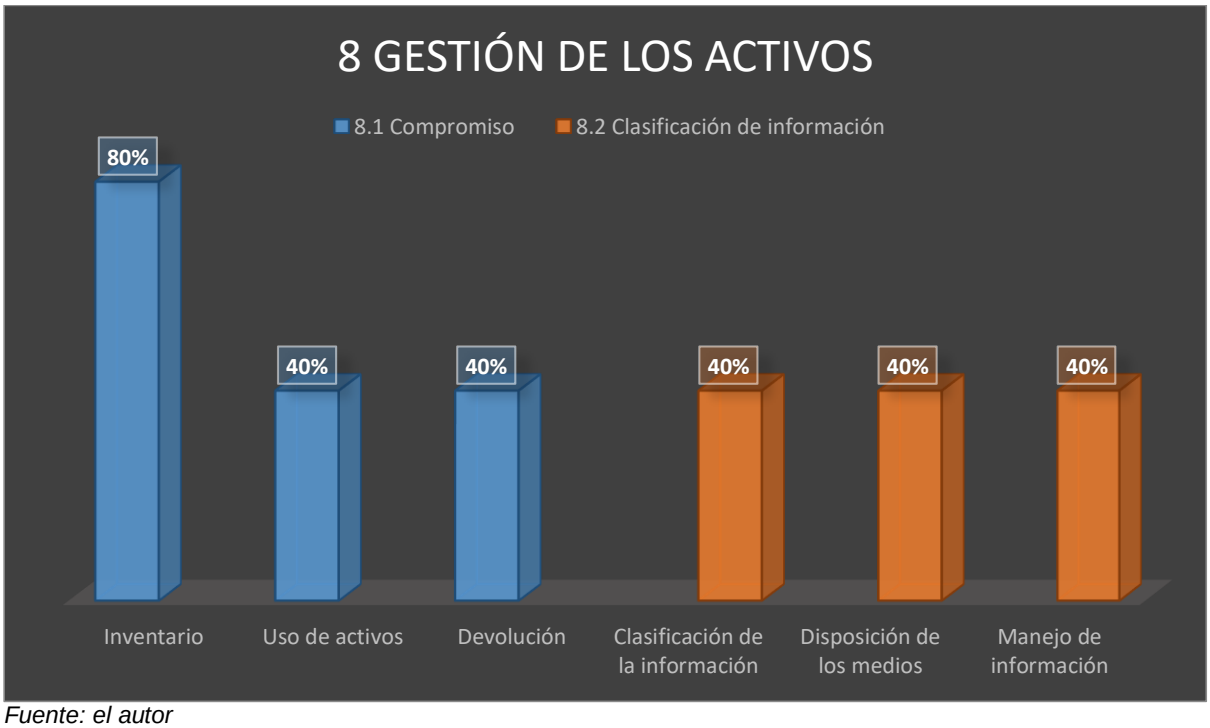
Tabla 20 Controles Gestión de los Activos

8 GESTIÓN DE LOS ACTIVOS	
8.1 Compromiso	
8.1.1	Inventario
8.1.2	Uso de activos
8.1.3	Devolución
8.2 Clasificación de información	

8.2.1	Clasificación de la información
8.2.2	Disposición de los medios
8.2.3	Manejo de información

Fuente: el autor

Grafica 13 Control es 8 Gestión de activos



Fuente: el autor

9 Control de Acceso: Las directrices de la EPS no se encuentran definidas, en su mayoría, el sistema de creación de usuarios y contraseñas para el acceso al sistema no está definido, el área de sistemas hay una persona encargada de supervisar el acceso, sin embargo, sin un procedimiento o política establecida es un control superficial.

Tampoco se cuenta con ningún tipo de procedimiento para reasignar funciones, modificar o quitar privilegios, para esto es necesario en primer lugar definir un sistema de usuarios de dominio. El software utilizado es licenciado, se usa software propietario comprado directamente a desarrolladores.

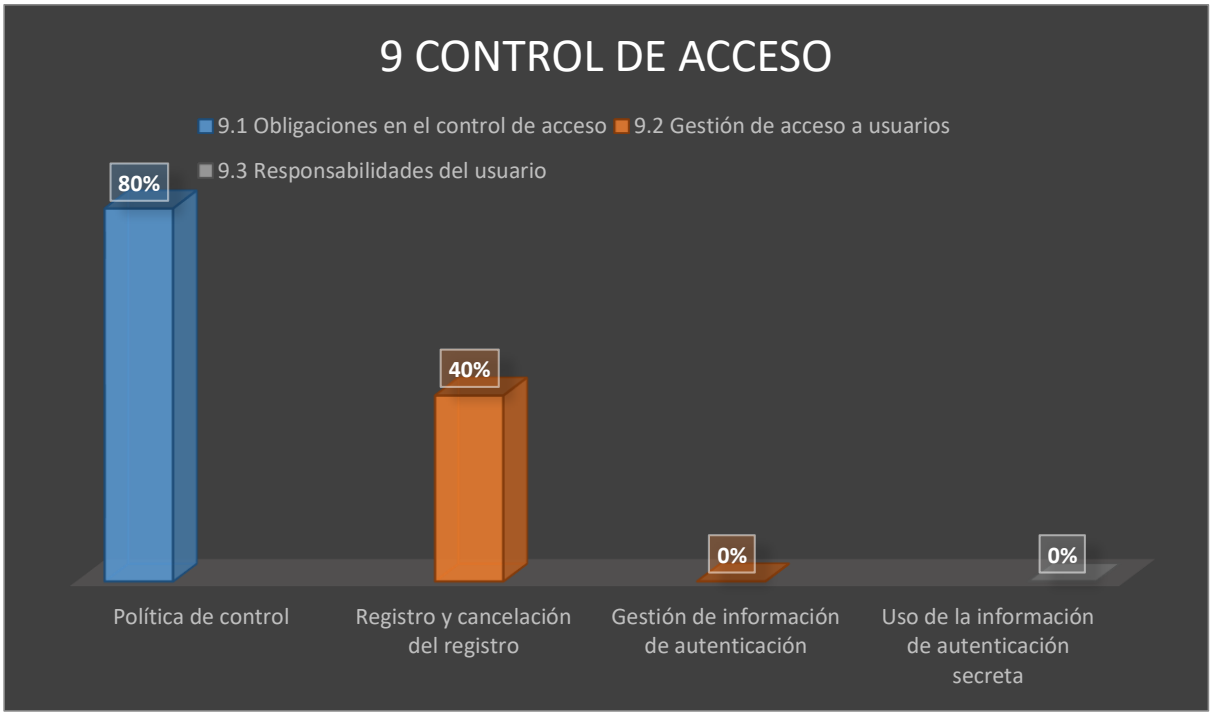
Tabla 21 Controles control de acceso

CONTROLES 9 CONTROL DE ACCESO	
9.1 Obligaciones en el control de acceso	
9.1.1	Política de control
9.2 Gestión de acceso a usuarios	
9.2.1	Registro y cancelación del registro

9.2.2	Gestión de información de autenticación
9.3 Responsabilidades del usuario	
9.3.1	Uso de la información de autenticación secreta

Fuente: el autor

Grafica 14 Controles 9 de acceso



Fuente: el autor

10 Criptografía: No existen controles criptográficos, la EPS Asmet Salud no utiliza ningún tipo de llave criptográfica, el intercambio de información se lleva a cabo generalmente a través de correos electrónicos, pero estos no llevan ningún tipo de algoritmo de cifrado. No se usa ningún tipo de VPN, ni virtualización de red, las conexiones en remoto se hacen a través de aplicaciones integradas de software como escritorio remoto o por medio de software como teamviewer.

Tabla 22 Controles Criptografía

10 CRIPTOGRAFÍA	
10.1 Inspecciones criptográficos	
10.1.1	Políticas sobre el uso de controles
10.1.2	Gestión de llaves

Fuente: el autor

Grafica 15 Controles 10 criptografía

Fuente: el autor

En la figura anterior que no se cuenta con ningún tipo de políticas o controles criptográficos al interior de la EPS Asmet Salud.

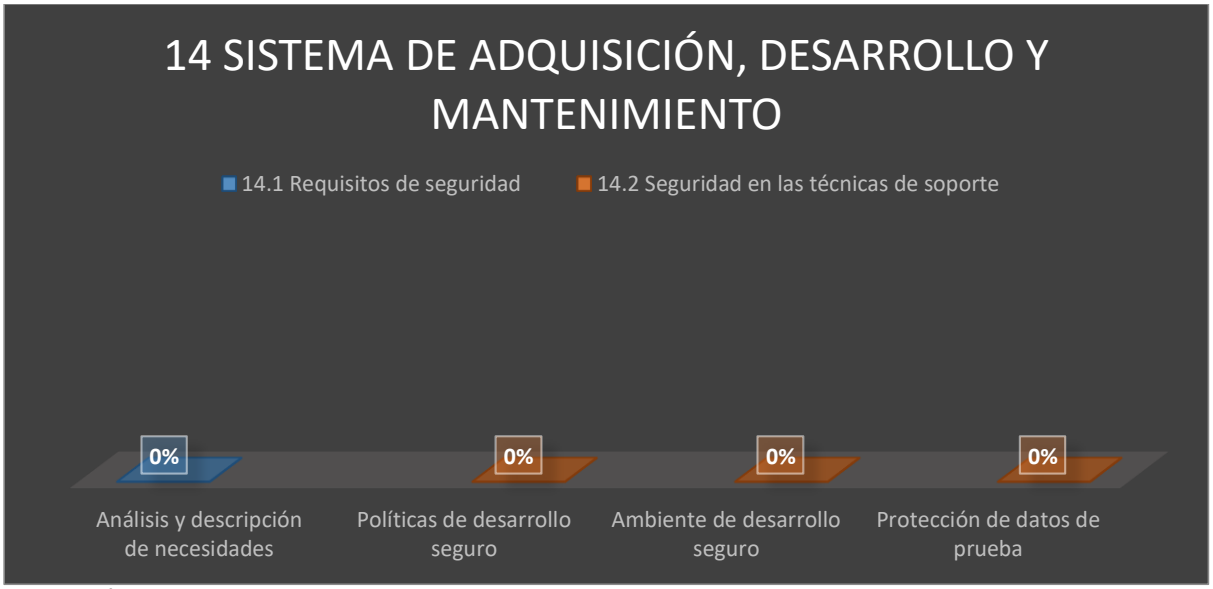
14 Sistema de adquisición, desarrollo y mantenimiento: En la E.P.S. Asmet Salud, no se tienen definidos requisitos de seguridad que se deben cumplir en cuanto a la adquisición de nuevo software o la actualización de software o aplicaciones existentes, en lo referente al uso de redes públicas no se ha definido ningún tipo de control guiado a mitigar fuga de información o acciones fraudulentas, no hace ningún tipo de desarrollo propietario, todo software que se usa en la empresa es desarrollado por casas desarrolladoras

Tabla 23 Controles sistema de adquisición, desarrollo y mantenimiento

14 SISTEMA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO	
14.1 Requisitos de seguridad	
14.1.1	Análisis y descripción de necesidades
14.2 Seguridad en las técnicas de soporte	
14.2.1	Políticas de desarrollo seguro
14.2.2	Ambiente de desarrollo seguro
14.2.3	Protección de datos de prueba

Fuente: el autor

Grafica 16 Controles 14 Sistema de adquisición



Fuente: el autor

La figura anterior muestra que la EPS Asmet Salud no tienen definidos requisitos de seguridad que se deben cumplir en cuanto a la adquisición de nuevo software o la actualización de software o aplicaciones existentes, en lo referente al uso de redes públicas.

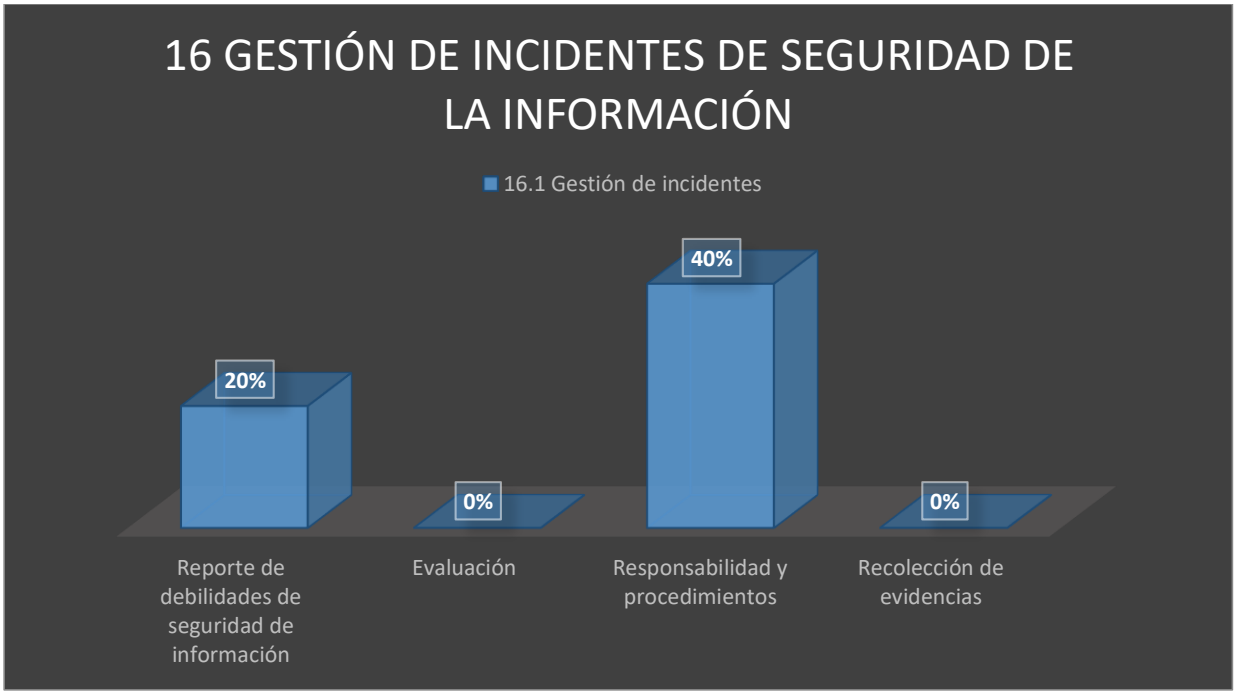
16 Gestión de Incidentes de Seguridad de la Información: Actualmente no han presentado incidentes que puedan afectar los objetivos de la EPS, la confidencialidad, integridad o disponibilidad de los datos, no hay políticas definidas en los activos de contención a sucesos de seguridad que permita detectar, reportar, catalogar, dar tratamiento, recolectar y salvaguardar evidencia de posibles incidentes, para los funcionarios no es una responsabilidad informar sobre la presencia de posibles incidentes.

Tabla 24 Controles gestión de incidentes de seguridad de la información

16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
16.1 Gestión de incidentes	
16.1.1	Reporte de debilidades de seguridad de información
16.1.2	Evaluación
16.1.3	Responsabilidad y procedimientos
16.1.4	Recolección de evidencias

Fuente: el autor

Grafica 17 Controles 16 Gestión de incidentes



Fuente: el autor

18 Cumplimiento: Asmet Salud EPS no se encuentra regulada por una empresa específica respecto a la seguridad de los datos, no se tiene definida una política en la que se establezcan los mecanismos para proteger la respecto a pérdida, destrucción, falsificación y acceso no autorizado, esta información se encuentra almacenada sin ninguna protección. Es necesario tener en cuenta que los directivos no han determinado políticas, por ende, estos no pueden revisarse y actualizarse de acuerdo a las necesidades.

Tabla 25 Controles gestión de incidentes de seguridad de la información

18 CUMPLIMIENTO	
18.1 Desempeño de requisitos legales y contractuales	
18.1.1	Derechos de propiedad intelectual
18.1.2	Reglamentación de controles criptográficos
18.1.3	Revisión de seguridad de la información
18.1.4	Desempeño con las políticas y normas de seguridad
18.1.5	Observación del cumplimiento técnico

Fuente: el autor

Grafica 18 Controles 18 Cumplimiento

Fuente: el autor

Conclusiones del análisis GAP. La EPS Asmet Salud, descubre la seguridad de la información como una necesidad inmediata, han llevado a cabo procesos y procedimientos en su mayoría comunicados verbalmente intentando definir roles y responsabilidades de seguridad informática en el área de sistemas, sin embargo, estos esfuerzos solo cubren algunos apartes de necesidades identificadas, pero no hacen parte de un proceso integral de la seguridad.

Se identifican necesidades de ejecución de un SGSI, como los lineamientos a seguir para proteger de manera adecuada la EPS, es indispensable garantizar la confidencialidad de los activos de información para generar seguridad, definir políticas que permitan proteger la información, los activos de la empresa y dar cumplimiento a las normas vigentes para la EPS Asmet Salud.

Apoyado en los resultados adquiridos en el análisis preliminar, se demuestra la necesidad de realizar levantamiento de activos relevantes y de importancia vital para la empresa, tomando como información principal el inventario de activos, realizando una matriz de riesgos, donde se identifiquen las principales amenazas a las que se puede ver comprometida la información calificada como crítica o confidencial, al tener el resultado de esta matriz de riesgos, realizar el levantamiento de un cuadro de controles teniendo como base el modelo ISO 27001:2013.

RECOLECCIÓN DE ACTIVOS DE INFORMACIÓN

Los recursos informáticos deben encontrarse registrados detalladamente dentro del inventario que se realiza anualmente por el departamento de sistemas, para saber su relevancia e importancia, como también a que empleado pertenece a la hora de hacer auditorias.

Los recursos deben tener toda la información relevante dentro del inventario que se realiza, para que sea fácil saber que propiedades y especificaciones técnicas tiene ese bien por si en un llegado caso de deba cambiar o hacer reposición. “Los responsables de los activos y la clasificación de la información. Todo el proceso para crear el inventario de activos es un aspecto muy importante a la hora de gestionar los riesgos de la organización implementando un Sistema de Gestión de Seguridad de la Información ISO-27001. Una empresa tiene que identificar sus activos y el valor relativo de éstos”[41].

Para realizar el inventario de activos de información en la EPS Asmet Salud, se realizó entrevista con uno de los dueños y la gerente de la empresa, también se tuvo en cuenta el material entregado por la empresa correspondiente al inventario de activos fijos que posee la empresa.

Tabla 26 Inventario de activos

Activo	Tipo	Proceso	Responsable
Contratos de servicio	Información	Gerencia	Gerencia
Servicios de garantía	Información	Gerencia	Gerencia
Nomina	Información	Financias	Contador
Televisor	Hardware	Gerencia	Gerencia
Servidor	Hardware	Sistemas	Oficina de sistemas
Computadores de mesa	Hardware	Sistemas	Oficina de sistemas
Computadores portátiles	Hardware	Sistemas	Oficina de sistemas
Discos de backups	Hardware	Sistemas	Oficina de sistemas
Scanner	Hardware	Sistemas	Oficina de sistemas
Servicio de internet	Red	Sistemas	Oficina de sistemas
Bases de datos	Red/Software	Sistemas	Oficina de sistemas
Correo electrónico	Red	Sistemas	Oficina de sistemas
Antivirus	Software	Sistemas	Oficina de sistemas
Página web	Software	Sistemas	Oficina de sistemas
Licencia de software	Software	Sistemas	Oficina de sistemas
Empleados	Conocimiento	Recursos humanos	Oficina de recursos humanos

Fuente: el autor

[41] SGSI Blog especializado en Sistemas de Gestión. Tomado de: https://www.pmg-ssi.com/2017/06/implementar-sistema-gestion-seguridad-de-la-informacion/

ANÁLISIS DE RIESGO

Implica conocimiento de riesgos que puede presentar la empresa, este estudio nos permite evaluar y decidir la forma de tratarlos, así mismo se pueden definir los controles adecuados en su respectivo procedimiento. Este proceso involucra atención de los orígenes y principios de donde provienen estos riesgos como también sus consecuencias.

Aquí se pueden identificar los riesgos con el propósito de estipular el impacto y el valor que se le asigna a cada uno de ellos, en este caso los valores asignados son: Muy Alto, Alto, Medio, Bajo y Muy Bajo, como se puede observar en la siguiente tabla.

Tabla 27 Matriz de riesgo valores

Riesgo	Valor
Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy alto	5

Fuente: el autor

El impacto que puede ocasionar la afectación de los activos de información se valoró de acuerdo a cuatro aspectos los cuales son imagen, legal, financiero y operatividad continua, en la siguiente tabla se puede apreciar la valoración de impacto y la descripción de cada valor.

Tabla 28 Valoración de impacto

Descripción	Valor	Imagen	Legal	Financiero	Operatividad
		Afectación sobre la reputación e imagen de la empresa	**Resoluciones administrativas por incumplimiento**	**Pérdida de ingresos que genera la empresa**	**Tiempo que afecta la operación de procesos**
Sin trascendencia	1	Grupo de empleados	Multas	Sin consecuencias económicas	Ajustes de actividades
Menor	2	Todos los empleados	Demandas	Bajas consecuencias económicas	Cambio de procedimientos
Moderado	3	Usuarios en la ciudad	Investigaciones disciplinarias	Consecuencias económicas medianas	Cambio en la interacción de procesos
Mayor	4	Usuarios en la región	Investigaciones fiscal	Altas consecuencias económicas	Servicios intermitentes
Catastrófico	5	Usuarios del país	Sanciones	Consecuencias nefastas	Detención de procesos

Fuente: el autor

Para la evaluación de los riesgos fue establecida por la probabilidad de ocurrencia, el riesgo es el resultado de la operación entre el valor del impacto y la afectación de un activo con la probabilidad de ocurrencia, conforme a la tabla 29 se estableció la posibilidad de ocurrencia.

Tabla 29 Probabilidad de ocurrencia

Valor	Nivel de probabilidad	Descripción
1	Muy baja	Puede ocurrir en condiciones excepcionales
2	Baja	Puede ocurrir en cierto momento
3	Media	Puede ocurrir en cualquier momento
4	Alta	Probablemente ocurrirá en la mayoría de circunstancias
5	Muy alta	Ocurre en la mayoría de circunstancias

Fuente: el autor

Identificados los riesgos que pueden afectar la EPS Asmet Salud se definieron los niveles de riesgo, para lo cual se diseñó una matriz llamada elementos de tolerancia y respuesta a los riesgos en donde se puede prestar atención a los diferentes limites que fueron establecidos como inferiores y superiores.

Tabla 30 Matriz de elementos de tolerancia y respuesta a los riesgos

Limites		Nivel de riesgo	Respuesta de riesgo
Inferior	Superior		
0	50	Baja	Asume el riesgo
51	140	Moderada	Mitiga, evita el riesgo
141	270	Alta	Mitiga, evita el riesgo
271	370	Extrema	Mitiga, evita el riesgo

Fuente: el autor

Identificados y examinados los riesgos, como el impacto que tienen para el buen desempeño de la EPS Asmet Salud se puede realizar el plan de procedimiento de los riesgos apoyándonos en los apuntes de la norma ISO 27001 que aplican para riesgos identificados. El plan de tratamiento se basa en establecer los controles necesarios para tratar los riesgos identificados.

Para tener un punto de partida de cómo se encuentra la EPS Asmet Salud en el municipio de Timana Huila en cuanto a la norma ISO 27001:2013 se efectúa una valoración de políticas del SGSI que nos permite comparar el estado de cumplimiento de este estándar:

Tabla 31 Valoración de políticas del SGSI

		Control	Estado
5	**Políticas de seguridad**		
5.1	**Normas establecidas en la protección de información**		
Objetivo: Brindar orientación y soporte, para la seguridad de la información de acuerdo con los requisitos y reglamentos pertinentes.			
5.1.1	Directrices de seguridad	Control: precisar las políticas de seguridad, aprobada por los altos directivos, comunicársela a funcionarios y a las partes pertinentes.	No cumple
5.1.2	Revisión de las políticas	Control: las políticas de seguridad de la información se deben revisar en intervalos significativos, para asegurar la eficacia continua.	No cumple
6	**Organización de seguridad de la información**		
6.1	**Clasificación interna**		
Objetivo: Implantar un marco de gestión iniciando y controlando la operación de la seguridad de información dentro de la E.P.S.			
6.1.1	Roles y responsabilidades	Control: puntualizar y establecer las responsabilidades de la seguridad de información	No cumple
6.1.2	División de deberes	Control: separar las responsabilidades reduciendo posibilidades de alteración y el uso ilícito de los recursos de la EPS.	No cumple
7	**Seguridad de recursos humanos**		
7.1	**Durante la ejecución**		
Objetivo: Certificar que los empleados entiendan sus responsabilidades y roles para el cumplimiento de sus deberes.			
7.1.1	Responsabilidades	Control: gerencia debe requerir a todos los funcionarios la ejecución en los procesos de seguridad de acuerdo con las políticas y procedimientos establecidos por la EPS.	Cumplimiento parcial
7.1.2	Toma de conciencia	Control: los funcionarios de la EPS reciben capacitaciones apropiadas y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	No cumple
7.1.3	Proceso disciplinario	Control: se debe detallar procesos que sanciones a los funcionarios que cometen faltas graves en cuanto a seguridad de los datos.	No cumple
8	**Gestión de activos**		
8.1	**Responsables**		
Objetivo: Identificar los recursos de la empresa definiendo responsabilidades correctas de protección.			
8.1.1	Inventario de activos	Control: identificar los recursos al procesamiento de información, elaborando su respetivo inventario.	Cumple
8.1.2	Uso de activos	Control: identificar y efectuar pautas para el uso de recursos de información.	Cumplimiento parcial
8.1.3	Devolución	Control: al terminar contrato se debe realizar la debida devolución de los recursos asignados a los empleados.	Cumplimiento parcial
8.2	**Clasificación de la información**		
Objetivo: Asegurar que los datos recibe adecuado manejo de protección, de acuerdo con su importancia.			
8.2.1	Clasificación de la información	Control: implementar procedimientos de acuerdo a la clasificación de información adoptado por la EPS.	Cumplimiento parcial
8.2.2	Disposición de medios	Control: efectuar procesos en la utilización de cursos, de acuerdo a la clasificación de información adoptado por la E.P.S.	Cumplimiento parcial

8.2.3	Manejo de información	Control: clasificar la información dependiendo los requisitos legales y valor.	Cumplimiento parcial
9	**Control de acceso**		
9.1	**Obligaciones en el control de accesos**		
Objetivo: Limitar el acceso a la información de procesamiento de información.			
9.1.1	Políticas de control de acceso	Control: establecer, documentar y revisar políticas para la obtención de la información confidencial en base a los requisitos de la EPS.	Cumple
9.2	**Gestión de acceso de usuarios**		
Objetivo: Certificar el acceso de usuarios autorizados y restringir el acceso no autorizado a la información de la E.P.S.			
9.2.1	Registro y cancelación de usuarios	Control: registrar cambios al terminar contratos o trabajos, cancelando el ingreso a personas no autorizadas.	Cumplimiento parcial
9.2.2	Gestión de información de autenticación	Control: controlar la asignación de autenticación de la información.	No cumple
9.3	**Responsabilidades del usuario**		
Objetivo: Solicitar informes a los empleados al hacer uso de protección de su información.			
9.3.1	Uso de información autenticación	Control: requerir a los empleados el uso adecuado de información confidencial.	No cumple
10	**Criptografía**		
10.1	**Controles**		
Objetivo: Certificar el adecuado uso de criptografía protegiendo la confidencialidad, autenticidad e integridad de la información.			
10.1.1	Gestión de llaves	Control: implementar políticas en el uso de llaves criptográficas, durante los procesos de manipulación de información.	No cumple
10.1.2	Políticas a controles	Control: implementar políticas en el uso de controles criptográficos para la protección de datos.	No cumple
14	**Sistema de adquisición, desarrollo y mantenimiento**		
14.1	**Requisitos de seguridad**		
Objetivo: Certificar la integridad de los sistemas de información en cada proceso, incluyendo las necesidades que se prestan sobre redes y equipos de información.			
14.1.1	Análisis y descripción de necesidades	Control: incluir los requisitos de protección de información y los nuevos sistemas de información a la hora de realizar mejoras.	No cumple
14.2	**Seguridad en las técnicas de soporte**		
Objetivo: implementar el diseño en los ciclos de seguridad de la información.			
14.2.1	Políticas de desarrollo seguro	Control: implantar reglas en el desarrollo de software en el interior de la E.P.S.	No aplica
14.2.2	Ambiente en el desarrollo seguro	Control: establecer convenientemente los ambientes para las actividades de desarrollo de sistemas.	No cumple
14.2.3	Protección de datos de prueba	Control: realizar pruebas de funcionalidad de la protección de la información.	No aplica
16	**Información de gestión de incidentes de seguridad**		
16.1	Gestión de incidentes		
Objetivo: Certificar la eficacia y comunicación en la gestión de incidentes de seguridad y debilidades de la información.			
16.1.1	Reporte por debilidades	Control: solicitar a los empleados reportes de debilidades encontradas en la seguridad de información.	Cumplimiento parcial
16.1.2	Evaluación	Control: evaluar y clasificar los diferentes incidentes de seguridad de la información.	No cumple

16.1.3	Responsabilidad e instrucciones	Control: establecer responsabilidades para asegurar respuestas rápidas sobre incidentes de seguridad de la información	Cumplimiento parcial
16.1.4	Recolección de evidencias	Control: definir procedimientos a la hora de identificar la preservación de evidencias de la información.	No cumple
18	**Cumplimiento**		
18.1	**Requisitos legales y contractuales**		
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.			
18.1.1	Derechos propiedad intelectual	Control: implementar instrucciones que aseguren el cumplimiento apropiado del reglamento de los derechos de propiedad intelectual.	Cumplimiento parcial
18.1.2	Reglamentación de controles criptográficos	Control: utilizar controles criptográficos para el cumplimiento de las funciones asignadas.	No cumple
18.1.3	Revisión	Control: revisar los enfoques de la organización para el uso adecuado de información cuando ocurran cambios significativos.	No cumple
18.1.4	Cumplimiento de políticas y normas	Control: revisar regularmente el cumplimiento de los procesos de seguridad de información en cada área.	No cumple
18.1.5	Reconocimiento del desempeño técnico	Control: revisar periódicamente el cumplimiento de estándares de seguridad.	No cumple

Fuente: Icontec.

CUMPLIMIENTO ISO 27001:2013

Establece niveles de acatamiento en la EPS, en cuanto a propósitos y metas de controles determinados en la tabla 6, del modelo ISO/IEC 27001:2013, del cual permite puntualizar operaciones orientadas al propósito de resguardar y proteger la disponibilidad, confidencialidad e integridad de los datos de la EPS.

Se empleó la lista de chequeo a la hora de ejecutar este análisis apoyada en un conjunto de interrogaciones, estos fueron respondidos por los empleados de las diferentes dependencias de la EPS de conformidad a los controles del estándar ISO/IEC 27001:2013, encaminados con la protección de datos que se manejan.

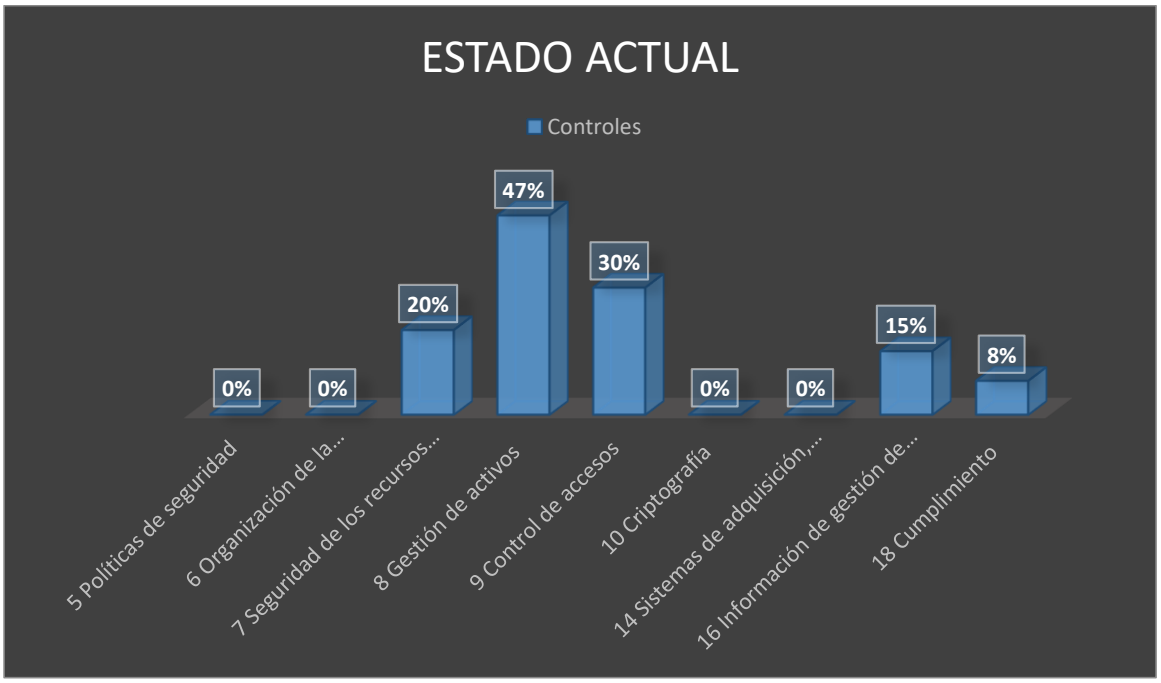
Tabla 32 Cumplimiento de controles

Control	Estado actual
5 Políticas de seguridad	0%
6 Organización de la seguridad de la información	0%
7 Seguridad de los recursos humanos	20%
8 Gestión de activos	47%
9 Control de accesos	30%
10 Criptografía	0%
14 Sistemas de adquisición, desarrollo y mantenimiento	0%
16 Información de gestión de incidentes de seguridad	15%
18 Cumplimiento	8%

Fuente: el autor

Se puede observar el estado actual de los diferentes tipos de control que se encontraron dentro de la empresa Asmet Salud, como también el porcentaje que se ha asignado a cada uno de estos controles que han sido tomados como base a la norma ISO/IEC 27001:2013.

Grafica 19 Cumplimiento de controles



Fuente: el autor

La ejecución del SGSI de concordancia al nivel de acatamiento con los registros determinados dentro del estándar ISO/IEC 27001:2013, llevara un esfuerzo desmedido a la EPS puesto a la carencia de controles. Algunos solicitan la mejora de dispositivos con el propósito de certificar la eficacia de los diferentes instrumentos tecnológicos.

El nivel de desempeño de los controles propuestos por la norma ISO 27001:2013, muestra el estado que tiene la EPS frente a la dirección de protección de los datos, como también el estado de desempeño con las vigentes normas con proporción a la seguridad y grado de riesgos de la EPS desde los controles establecidos por la norma.

OBJETIVOS DE CONTROL

NIVEL BAJO DE CUMPLIMIENTO

Con relación al modelo ISO/IEC 27001:2013, los objetivos de control con un nivel de cumplimiento bajo por parte de la EPS, son los que se encuentran con 0%, implicando un riesgo ALTO en la protección de información dentro de la EPS por falta de estos controles que no están generando ningún tipo de protección a los recursos de información.

Tabla 33 Controles con Bajo nivel de cumplimiento

CONTROL	CUMPLIMIENTO
5 Políticas de seguridad de la información	0%
6 Organización de la seguridad de la información	0%
10 Criptografía	0%
14 Sistemas de adquisición, desarrollo y mantenimiento	0%

Fuente: el autor

Grafica 20 Controles con nivel bajo cumplimiento

Fuente: el autor

5. Políticas de seguridad de la información (0%)

Respecto con la protección de datos se encuentran determinadas en la guía las cuales no se encuentran aprobados y tampoco son supervisados por los directivos de la EPS, entorpeciendo el cumplimento de los funcionarios en la ejecución de tareas en la EPS, se ve indispensable la utilización de políticas de seguridad.

6. Organización de la seguridad de la información (0%)

Las funciones y compromisos en la protección de los datos no se encuentran definidas, lo por lo tanto son compromisos que se deben certificar para formar un adecuado SGSI, lo cual es esencial para conocer los actuales peligros que aparecen y exponen la protección de información, siendo indispensables que la empresa comience a socializar con sus empleados diferentes temas que tengan que ver con la seguridad de la información.

10. Criptografía (0%)

No se cuenta con los diferentes componentes de cifrado para proteger la información, por lo que significa un alto riesgo, pues no certifica la confidencialidad, autenticidad e integridad de los datos con un gran valor de la EPS. Esta situación implica consentimientos legales al no cumplir con las normas que se requiere para realizar una protección adecuada de los datos. Serian adecuado que la EPS, instaure procesos con técnicas de cifrados con propósitos de proteger la información.

14. Sistemas de adquisición, desarrollo y mantenimiento (5%)

Regularmente no se verifican los procesos delicados de la empresa, al momento de llevar a cabo cambios en los diferentes sistemas que se manejan en los procesos de la EPS no se certifica que los servicios se lleven a cabo, en consecuencia, se ve necesario instaurar pautas adecuadas con el fin de proteger los datos que son parte fundamental en los procesos que se manejan dentro de la EPS.

NIVEL MEDIO DE CUMPLIMIENTO

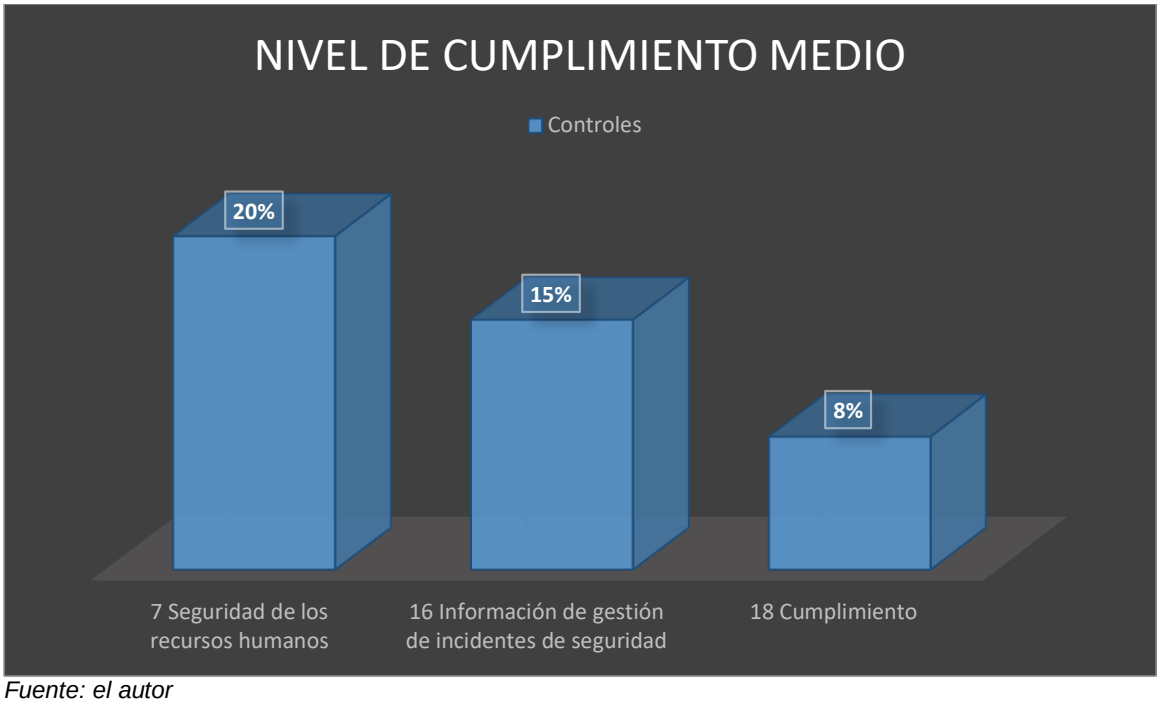
Los controles que se encuentran en un nivel medio de cumplimiento según lo establecido por el estándar ISO/IEC 27001:2013, están establecidos entre el 5% y el 20%, en consecuencia, conlleva a un riesgo MEDIO en la protección de datos de la EPS, indicando que ciertos controles no se encuentran certificados de forma adecuada y representan debilidades permitiéndose darle paso a que se efectúen las amenazas quebrantando la información de la EPS.

Tabla 34 Controles con nivel Medio de cumplimiento

CONTROL	CUMPLIMIENTO
7 Seguridad de los recursos humanos	20%
16 Información de gestión de incidentes de seguridad	15%
18 Cumplimiento	8%

Fuente: el autor

Grafica 21 Controles con nivel medio de cumplimiento



Fuente: el autor

7. Seguridad de los recursos humanos (20%)

Los procesos que se manejan en la EPS no garantizan que los empleados se encuentren notificados apropiadamente con los compromisos y tareas de seguridad y protección de la información, siendo fundamental que sean capacitados en las áreas que deben llevar a cabo para la buena administración de información de la EPS.

16. Información de gestión de incidentes de seguridad (0%)

Asmet Salud cuenta con pocos procesos encargados de los sucesos de seguridad, por ende, se ve la necesidad de implementar tareas que ayuden a cumplir con las metas que permitan salvaguardar eficazmente los datos sin poner en peligro la información administrada por los usuarios de la EPS.

18. Cumplimiento (8%)

Debido a que la empresa no tiene documentados los procesos de instauración de las actividades de cifrado que se realizan para poder cumplir con los procesos de proteger la información. Para poder amparar y custodiar los datos que son suministrados a diario en la EPS, se debe implementar un SGSI cumpliendo con las políticas de seguridad estipuladas.

NIVEL ALTO DE CUMPLIMIENTO

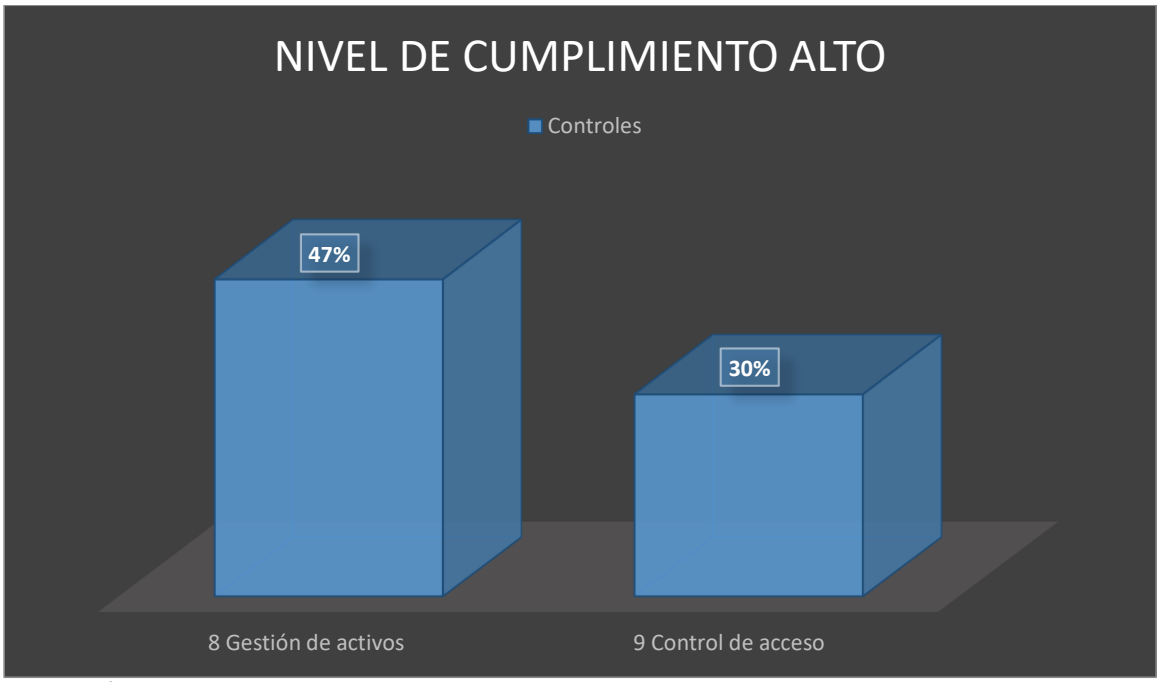
A continuación, se presentan los controles cuyo cumplimiento es alto dentro de la EPS Asmet de la forma que sugiere la norma ISO/IEC 27001:2013, estos tienen valoración por encima del 30%, por lo cual representa un mínimo riesgo para la información que se maneja en la EPS gracias a que los controles están implementados.

Tabla 35 Controles con nivel Alto de cumplimiento

CONTROL	CUMPLIMIENTO
8 Gestión de activos	47%
9 Control de acceso	30%

Fuente: el autor

Grafica 22 Controles con nivel alto de cumplimiento



Fuente: el autor

8. Gestión de activos (47%)

Cuenta con la identificación de los recursos informáticos mediante la administración que se le hace a la información, lo que equivale un mínimo riesgo, aunque es preciso clasificar e identificar los recursos de la EPS, mediante procesos que ayuden a mantener o aumentar de nivel dependiendo de las condiciones de los datos. Asmet Salud posee pautas en el uso de los recursos informáticos, generando que los empleados conozcan sus responsabilidades y consecuencia de sus acciones.

13. Control de acceso (30%)

Este control cuenta con un cumplimiento alto puesto que las redes de la empresa se encuentran bien dirigidas, se debe certificar la correspondiente separación en las actividades de información, establecer una revisión periódica para que las obligaciones establecidas en la norma ISO 27001 se cumplan a cabalidad y se mantenga el nivel de cumplimiento por la empresa.

FASE II. PREPARACION

ANALISIS

Examina el estado inicial de la empresa, definiendo las debilidades y fortalezas dentro del cumplimiento de políticas de seguridad referente al modelo ISO/IEC 27001:2013. En este período se toman controles de la norma, para evaluar el desempeño de estos por parte de la empresa Asmet Salud conforme a la seguridad informática.

Teniendo en cuenta el cumplimiento se realiza el porcentaje de los controles como podemos observar en la siguiente tabla en la evaluación de los controles.

Tabla 36 Cumplimiento

Nombre	Valor	Porcentaje	Descripción
No aplica	0	N/A	No es aplicable en la empresa
No existe	1	0%	No existe el control en la empresa
Inicial	2	20%	Se aplican practicas con inconsistencias
Repetible	3	40%	Se aplica pero no se documenta
Definido	4	60%	Se documenta pero no se mide
Administrado	5	80%	Se miden con frecuencia
Optimizado	6	100%	Da cumplimiento

Fuente: El autor

Tabla 37 Dominios

Dominios	Control de acceso.
	Criptografía.
	Cumplimiento.
	Gestión de activos.
	Gestión de incidentes.
	Mantenimientos de sistemas.
	Organización de seguridad de información.
	Políticas de protección de información.
	Seguridad en recursos humanos.

Fuente: El autor

PROCESO DE GESTION DE RIESGOS. El objetivo de estos procesos dentro de la EPS es efectuar, instituir y conservar el sistema de administración de riesgos, conforme con los procedimientos determinados por la normatividad vigente. Al identificar riesgos que puedan poner en peligro los datos y verificar las causas y posibles soluciones que se le puedan dar.

PROCESO DE GESTION TECNOLÓGICA. Su propósito es establecer activos tecnológicos en la EPS, certificando la disponibilidad, confidencialidad, e integridad. Tiene como responsabilidad gestionar las plataformas de procesos, gestionando cambios para garantizar la protección de la información, tiene como alcance el proyecto del plan estratégico y la apropiada prestación de los servicios de la empresa.

8. DISEÑO DEL SGSI EN LA EPS ASMET SALUD

Ciertas actividades primordiales en el diseño de un sistema de gestión de seguridad de la información es participación de los altos directivos para llevar a cabo un proyecto de esta magnitud, ya que los objetivos y procesos que se manejan para la gestión de los datos de la EPS se tiene que conocer por los directivos, por esta razón todo el personal debe comprometerse con la gestión de los riesgos para que la empresa no se comprometa a un ataque o amenazas.

ALCANCE

El alcance del SGSI de la EPS Asmet Salud, comprende únicamente la técnica de administración tecnológica, que envuelve la organización de las instalaciones e instalación de plataformas de procesos, administración de aplicaciones e incidentes como el cambio de sistemas operativos en los equipos de la empresa. El SGSI se empleará exclusivamente en la sede de la EPS situada en el municipio de Timana Huila, sin limitar ni entorpecer las funciones que se manejan.

POLITICA DEL SGSI

Asmet Salud, encaminada en generar el avance razonable dando cumplimiento a la misión, visión, y complaciendo con las necesidades de usuarios y demás interesados, define funciones de protección de datos en la EPS, con el propósito de obedecer con las peticiones legales atribuidas por la empresa y el SGSI.

Conservar buenas costumbres de protección de información certificando la disponibilidad, confidencialidad e integridad de los datos, suministrando seguridad a los usuarios a la hora de aplicar el sistema de gestión de seguridad de la información, garantizando continuidad de los servicios y la seguridad.

PLANIFICACION

Aquí se implementan las tareas oportunas cuyo objetivo es garantizar que el diseño del Sistema de Gestión de Seguridad de la Información logre las metas planteadas y las operaciones que logren minimizar las amenazas, definir el margen alrededor de la protección de los datos con la responsabilidad de cumplir las tareas asignadas en la agrupación de los recursos de información.

Alcance caracterización de activos. De acuerdo a la eficacia del SGSI, por lo que solo aprecia el objetivo tecnológico, en consecuencia, exclusivamente se reconocen activos que gestiona y ordena la información utilizada por la dirección de tecnología de la EPS.

Privacidad de la información. En consecuencia, el presente proyecto no describe el nombre de ningún programa que son utilizadas en las labores diarias, se describe su propósito, a petición de la confidencialidad de la información por parte de la EPS Asmet Salud.

CLASIFICACION DE ACTIVOS TECNOLÓGICOS

Los recursos tecnológicos que maneja la EPS Asmet Salud abarca las medidas, representaciones que se emplearon a la hora de especificar el nivel crítico que se pueden encontrar los recursos informáticos, aquí se identifican los activos informáticos de acuerdo a la metodología, por lo que se ordena en la siguiente clasificación:

Tabla 38 Clasificación de recursos

ACTIVO	DESCRIPCIÓN
Servicios	Precisa los servicios prestados
Datos	Copias de respaldo, Backups, credenciales, datos de validación, control de acceso, registro de tareas.
Software	Sistemas operativos, aplicaciones, bases de datos, sistema de información
Hardware	Medios físicos, equipos tecnológicos
Personal	Empleados con funciones de sistemas de información.
Redes	Comunicaciones
Instalaciones	Establecimiento donde funciona la EPS

Fuente: El autor

Procesamiento y análisis de datos

Realizadas las entrevistas al personal de la empresa, se verifica el diligenciamiento total de las encuestas, procedemos a analizar los resultados, seguido a esto ingresamos la información en una hoja de cálculo para la tabulación de los resultados. Se realiza un análisis a la empresa para observar la situación actual tomando los controles que se manejan dentro de la norma ISO27001:2013.

Tabla 39 Nivel de cumplimiento

Nombre	Descripción	Valor
No existe	No se evidencia el estándar dentro de la empresa	0
Inicial	Se practican estándares con inconsistencias	1
Repetible	Se practican estándares pero no documentado	2
Definido	Se documenta pero no medido	3
Administrado	Se realizan procesos medidos a espera de mejoras	4
Optimizado	Define el cumplimiento practicando las mejoras	5

Fuente: el autor

Podemos observar en la tabla anterior, la asignación de calificación que van de 0 a 5, donde 0 es no existe ningún tipo de control o no se evidencia estándar dentro de la empresa a la hora de iniciar el SGSI, y 5 se define como el cumplimiento y las prácticas de mejoras dentro de los modelos establecidos dentro del modelo ISO/IEC 27001:2013.

FORTALEZAS Y DEBILIDADES

Partiendo del estándar ISO/IEC 27001:2013 de manera que describe el análisis para la ejecución de controles de seguridad en la E.P.S. Asmet Salud, se evidencia una serie de fortalezas y debilidades a la hora de realizar el boceto de un sistema de gestión de seguridad de la información.

Tabla 40 Fortalezas Debilidades

Debilidades	Fortalezas
Carece de documentos con políticas de seguridad.	Se tiene conciencia en los roles que se manejan.
Falta definir responsabilidades de la seguridad informática.	Se realiza inventario para la asignación de activos a los empleados.
Faltan políticas para el correcto uso de los activos asignados.	Hay controles para sitios restringidos sin ser definidos.
Faltan políticas de protección en los registros criptográficos.	Se evidencian controles para la realización de mantenimiento en los computadores.

No posee actualización del software en los equipos.	Existen normas básicas de seguridad.
No se realiza capacitación a los empleados en temas de seguridad informática.	
Falta documentar los incidentes ocurridos.	
Hay falencias sobre cómo proceder en los casos de incidentes.	
Se carece en las instrucciones de protección de datos.	
No hay políticas para el cambio de contraseñas.	
Carece de realización de backups.	

Fuente: el autor

GESTIÓN DOCUMENTAL

Es preciso que el sistema de gestión de seguridad de información contenga gestión documental, exponiendo archivos y documentos existentes para la ejecución de la norma ISO. HELENA ROJAS VALDUCIEL[42], afirma que la documentación sirve de pauta para el análisis de implementación de un SGSI, como también para garantizar las decisiones tomadas conforme con la protección de datos al interior de cualquier empresa.

POLÍTICAS DE SEGURIDAD

Existen varias normas que son de gran importancia aplicar en el momento de implementar un SGSI como la disponibilidad, confidencialidad e integridad, razones por cual los métodos de protección se deben documentar, comprometiendo a todos los empleados de la EPS, para que se apropien de las políticas y normas establecidas de un SGSI.

Hay que resaltar que las normas y políticas se manejan de manera confidencial, que solo los empleados que tienen acceso puede manipular esta información cumpliendo con las funciones asignadas.

Control de acceso

- Cambio con regularidad de claves utilizando estándares de seguridad.
- Verificación de identidad de usuarios para la autorización al acceso de recursos físicos o lógicos.

[42] Helena Rojas Valduciel, Elaboración de un plan de implementación de la ISO/IEC 27001:2013, tomado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/40297/1/hrojasvTFM1214.pdf

Confidencialidad de la información

- Se debe respetar las normas de confidencialidad dictadas por la empresa.
- La información no debe suministrar a personal ajeno de la empresa.

Propiedad intelectual

- No instalar programas o aplicaciones ajenas al cumplimiento de las funciones establecidas por las políticas dela empresa.

Software

- Prohibido la descarga de programas o aplicaciones no autorizados por la empresa.
- Inspección de todos los medios extraíbles por medio de antivirus.
- Informar cualquier anomalía que se presente con el software.
- Realizar backups periódicamente.
- Solicitar actualizaciones de programas y antivirus.

Hardware

- Solicitar autorización para poder retirar equipos de las instalaciones de la empresa.
- Reportar daños de equipos y evitar la manipulación de estos.
- No realizar copias de documentos o archivos sin autorización.
- No utilizar memorias y otros dispositivos móviles en los equipos.

Uso de recursos

Los equipos asignados por parte de la empresa a los empleados son de uso exclusivo para las tareas asignadas y no para uso personal.

Correo electrónico

- El correo electrónico asignado por la empresa es solo de uso laboral.
- Verificar los adjuntos de los correos parea descartar virus.
- Descartar cualquier tipo de correo del cual se sospeche.
- Evitar el reenvió de cadenas y correos maliciosos.

Usuarios y contraseñas

- Cada empleado contara con su usuario y contraseña debidamente establecida por la empresa.

- Las contraseñas tendrán caducidad cada 30 días.
- Las contraseñas deben de tener caracteres alfanuméricos.

Auditorías internas

La ejecución de un SGSI faculta a las empresas conseguir una certificación internacional, logrando ser más competitiva y cumpliendo con los estándares de seguridad.

Es necesario que la empresa realice las siguientes auditorias:

Documental

Para realizar este tipo de auditoria los encargados tienen el compromiso de inspeccionar la documentación que ostenta la empresa, es importante estudiar el alcance y las políticas que posee la empresa en cuanto a controles, realizando análisis de riesgos, para darle solución lo más pronto posible.

Después de realizar el anterior proceso se prepara un informe minucioso donde se dan a conocer las debilidades y fortalezas del SGSI, como también se deben explicar las inconformidades encontradas.

Certificación

Aquí se debe cumplir a cabalidad con lo descrito no se deben presentar inconformidades y debe haber un funcionamiento eficaz de políticas al interior de la empresa. Estas auditorías por lo general se realizan anualmente con el propósito de identificar el cumplimiento del SGSI, identificando el funcionamiento de los procesos y los controles, minimizando las diferentes amenazas a que se expone la protección de los datos.

Administración de indicadores

Enfoca la exactitud de eficiencia de componentes que se ejecutan en un modelo de seguridad de información, estos indicadores sirven como elaboración de mejoramiento, permitiendo tomar decisiones de mejora. Requisitos que se deben cumplir dentro de la gestión de indicadores:

- Ser de importancia en los objetivos de la empresa.
- Servir como apoyo en los análisis de riesgos.
- Ser imparcial.
- Evaluar controles de seguridad dentro de la empresa.

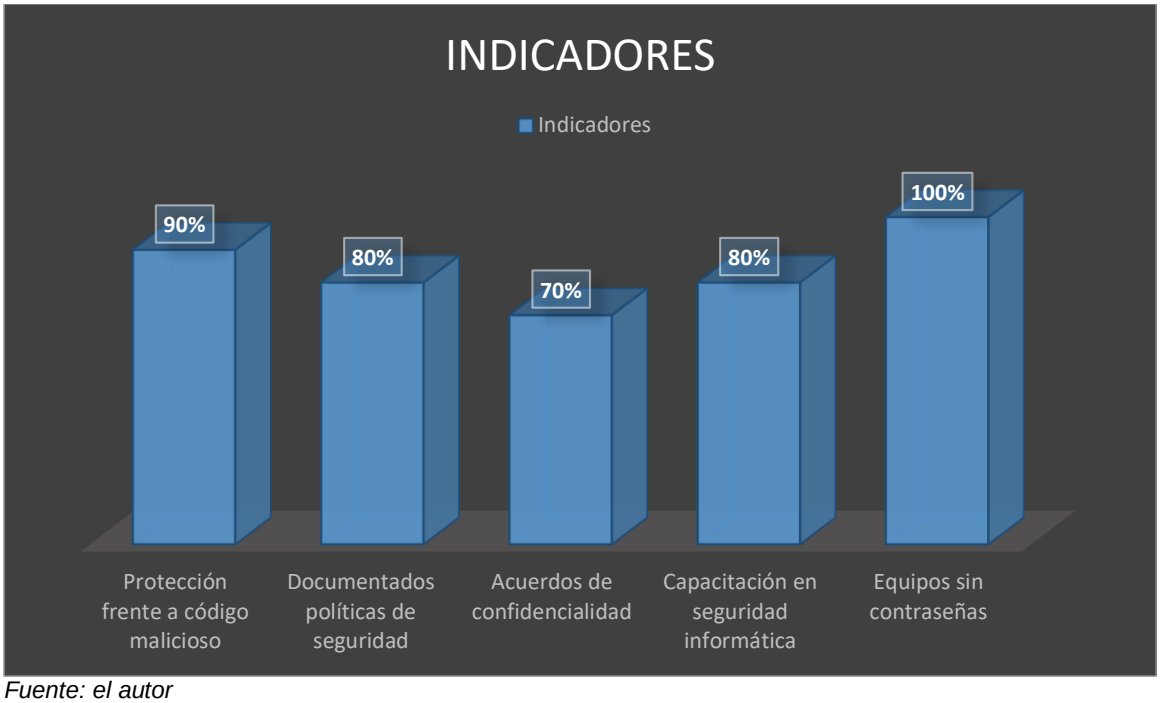
Existe gran variedad de indicadores que se pueden implementar, en ocasiones es importante implementar los más relevantes, donde el análisis del SGSI nos mostrara los indicadores de seguridad en los equipos de cómputo para ver la eficacia del desarrollo del proyecto.

Tabla 41 Indicadores de gestión

Indicador	Objetivo	Frecuencia	Responsable	Valor
Protección frente a código malicioso	Definir la protección frente a ataques maliciosos	Mensual	Sistemas	90%
Documentados políticas de seguridad	Medir los documentos existentes sobre seguridad informática	Trimestral	Sistemas	80%
Acuerdos de confidencialidad	Adquirir valores de confidencialidad con los empleados	Semestral	Recursos humanos	70%
Capacitación en seguridad informática	Identificar los roles que se han asignado frente a seguridad	Trimestral	Recursos humanos	80%
Equipos sin contraseñas	Identificar los equipos que no cuentas con seguridad de usuario y contraseña	Mensual	Sistemas	100%

Fuente: el autor

Grafica 23 Indicadores de gestión



Fuente: el autor

En la gráfica 23 se puede percibir los diferentes porcentajes que se manejan en los indicadores de gestión dentro de la EPS Asmet Salud.

ANÁLISIS DE RIESGOS

Para la ejecución de este proyecto que se basa en un diseño de un sistema de gestión de seguridad de la información cimentado en el modelo ISO/IEC 27001:2013, en la EPS Asmet Salud, se realizara por medio del uso de la metodología de investigación de campo.

Aplicabilidad

Según Halena Valduciel, un escrito SGSI debe estar sujeto con el estándar ISO/IEC 27001:2013, mostrando políticas que serán implementadas al interior de la empresa, también puntualiza los controles que se excluyen y sus causas (Valduciel, 2014).

La aplicabilidad a los controles no se limita a los estándares de la norma ISO, se puede hacer uso de diferentes controles cuando se consideren necesario.

Aspectos para la selección de controles.

- [EL] Exigencia legal
- [DC] Deberes contractuales
- [ON] Obligaciones del negocio
- [RA] Resultado de análisis de riesgos

Tabla 42 Aplicabilidad

	Control	*Descripción*	*Controles seleccionados*				*Aplicabilidad*
			EL	DC	ON	RA	
5	***Políticas de seguridad***						
5.1	*Normas establecidas en la protección de información*						
5.1.1	*Directrices de seguridad*	Existen políticas en la protección de información sin documentar, dar a conocer el proceso de SGSI por los empleados.	X		X		Si
5.1.2	*Revisión de las políticas*	Se debe constituir procedimientos que admita la observación periódica de las políticas de la seguridad.	X		X		Si
6	***Organización de la seguridad de la información***						
6.1	*Clasificación interna*						
6.1.1	*Roles y responsabilidades*	Se definen roles y responsabilidades de acuerdo a las políticas del SGSI.	X		X		Si
6.1.2	*División de deberes*	Asignar por separado los deberes de cada funcionario evitando el mal uso de los activos de la empresa.	X		X		Si
7	***Seguridad de recursos humanos***						
7.1	*Durante la ejecución*						
7.1.1	*Responsabilidades*	Exigir a los empleados acatar con las políticas de protección de información.		X	X		Si
7.1.2	*Toma de conciencia*	Realizar capacitaciones en temas de protección de información a los funcionarios de la E.P.S. Asmet Salud.			X		Si
7.1.3	*Proceso disciplinario*	Establecer sanciones al incumplimiento de las políticas de seguridad.			X		Si
8	***Gestión de activos***						
8.1	*Responsables*						
8.1.1	*Uso de activos*	Compromiso de los empleados con el uso de los activos de la empresa.	X		X		No
8.1.2	*Inventario de activos*	Describir un inventario detallado de cada activo existente al interior de la empresa.	X		X		No
8.1.3	*Devolución*	Establecer políticas para el reintegro.	X		X		No
8.2	*Clasificación de la información*						
8.2.1	*Manejo de información*	Contar con políticas para él sus adecuado de los activos.			X		Si
8.2.2	*Codificación de la información*	Establecer instrucciones en la clasificación de datos.			X		Si

8.2.3	*Disposición de los medios*	Proteger toda información cuando se realicen labores diferentes.			X		Si
9	***Control de acceso***						
9.1	*Obligaciones en el control de accesos*						
9.1.1	*Políticas de control de acceso*	Establecer controles al ingresar a la información.			X		Si
9.2	*Gestión de acceso de usuarios*						
9.2.1	*Gestión de información de autenticación*	Establecer pautas al personal que tiene permiso a la información delicada de la empresa.			X	X	Si
9.2.2	*Registro y cancelación de usuarios*	Registrar al personal que tiene permisos a los datos.	X		X	X	Si
9.3	*Responsabilidades del usuario*						
9.3.1	*Uso de información autenticación*	Establecer perfiles de mayor importancia para el acceso a la información.		X	X	X	Si
10	***Criptografía***						
10.1	*Controles*						
10.1.1	*Gestión de llaves*	Establecer controles de confidencialidad, disponibilidad e integridad de la información.	X		X		Si
10.1.2	*Políticas a controles*	Establecer políticas de confidencialidad, disponibilidad e integridad de información.	X		X		Si
14	***Sistema de adquisición, desarrollo y mantenimiento***						
14.1	*Requisitos de seguridad*						
14.1.1	*Análisis y descripción de necesidades*	Tener en cuenta el momento que la empresa quiera realizar cambio de sistema de información			X		Si
14.2	*Seguridad en las técnicas de soporte*						
14.2.1	*Políticas de desarrollo seguro*	Establecer políticas en el desarrollo de software protegiéndolo para evitar vulnerabilidades	X		X		No
14.2.2	*Ambiente en el desarrollo seguro*	Tener protegidos los controles de acceso.	X		X		No
14.2.3	*Protección de datos de prueba*	Ejecutar experimentos a las aplicaciones para evitar fugas de información.	X		X		Si
16	***Información de gestión de incidentes de seguridad***						
16.1	*Gestión de incidentes*						
16.1.1	*Reporte por debilidades*	Informar sobre eventos, identificando las posibles debilidades de seguridad.			X		Si
16.1.2	*Responsabilidad e instrucciones*	Especificar los procedimientos que permitan una reacción rápida.			X		Si
16.1.3	*Evaluación*	Evaluar la seguridad de información cuando se presente un evento.			X		Si
16.1.4	*Recolección de evidencias*	Definir controles a la hora de documentar los incidentes.			X		Si
18	***Cumplimiento***						
18.1	*Requisitos legales y contractuales*						

18.1.1	*Derechos propiedad intelectual*	Cumplir con las políticas de derechos de autor y software.	X	X	Si
18.1.2	*Reglamentación de controles criptográficos*	Cumplir con los controles criptográficos.	X	X	Si
18.1.3	*Revisión*	Inspeccionar periódicamente el SGSI.		X	Si
18.1.4	*Cumplimiento de políticas y normas*	Inspeccionar el desempeño de las políticas de seguridad.		X	Si
18.1.5	*Reconocimiento del desempeño técnico*	Revisar el desempeño por parte de los funcionarios en las políticas de seguridad.		X	Si

Fuente: el autor

Parámetros

En este espacio delimitamos los diferentes parámetros que son utilizados como guía para efectuar un correcto análisis de riesgo.

Vulnerabilidad

Cuando hablamos de vulnerabilidad nos referimos claramente a las debilidades o fallos que existen al interior de la empresa, permitiendo que una amenaza pueda concretarse sobre cualquier activo, por esta razón debemos inspeccionar todos los activos cada año.

Tabla 43 Frecuencia de vulnerabilidad

Frecuencia	
Vulnerabilidad	Valor
[MF] Muy frecuente	Quincenal
[F] Frecuente	Bimestral
[PF] Poco frecuente	Anual

Fuente: el autor

Impacto

Nos referimos a la pérdida de un activo medido en porcentaje.

Tabla 44 Impacto

Descripción	**Porcentaje**
[Cr] Critico	80-100
[Al] Alto	60-80
[Me] Medio	40-60
[Ba] Bajo	20-40
[MB] Muy bajo	<20

Fuente: el autor

Efectividad del control

Aquí podemos comprobar la eficacia que podemos observar en las medidas de protección de los riesgos.

Tabla 45 Valoración

Descripción	Valor
[Cr] Critico	95%
[Al] Alto	75%
[Me] Medio	50%
[Ba] Bajo	30%
[MB] Muy bajo	10%

Fuente: el autor

Análisis amenazas

Consideramos el nivel de riesgo al que se ven expuestos los medios que pueden originar inconvenientes o daños de seguridad, las amenazas que pueden existir en un SGSI las podemos clasificar en diferentes grupos como: desastres naturales, ataques intencionados, errores y fallos no intencionados.

Impacto

- [Au] Autenticidad
- [Co] Confidencialidad
- [Di] Disponibilidad
- [In] Integridad
- [Tr] Trazabilidad

Tipos de activos

- [D] Datos
- [HW] Hardware
- [SW] Software
- [I] Instalaciones
- [P] Personal
- [R] Redes
- [S] Servicios

Tabla 46 Amenazas

Conjunto	Amenaza	Extensión dañada					Activos perjudicado						
		A	C	I	D	T	I	HW	SW	D	R	S	P
Desastres naturales	Fuego			✓			✓	✓			✓	✓	✓
	Daños por Inundación			✓			✓	✓	✓	✓	✓	✓	
Desastres de Origen Industria	Fuego			✓	✓		✓	✓					
	Daños por inundaciones			✓	✓		✓	✓					
	Avería física			✓	✓		✓	✓	✓				
	Fallas eléctricas			✓	✓			✓	✓	✓		✓	
	Falla servicios de comunicación				✓						✓		
Errores no intencionados	Error de usuario		✓	✓	✓				✓	✓		✓	
	Software pirata		✓	✓	✓				✓				
	Error de mantenimiento			✓	✓			✓	✓				
	Fugas de información		✓				✓		✓	✓	✓	✓	✓
Ataques intencionados	Manipulación de registros			✓					✓				
	Ingeniería social		✓	✓	✓								✓
	Acceso sin autorización		✓	✓			✓	✓	✓	✓	✓	✓	
	Ataque destructivo				✓		✓	✓					

Fuente: el autor

Resultado de vulnerabilidades

Se realiza estudio de vulnerabilidades elaborando uso de varios procesos de observación, entrevistas.

Ahora se detalla cada vulnerabilidad que posee la empresa, se agrupan mediante el tipo de amenazas.

Tabla 47 Vulnerabilidades

Origen	Amenaza	Vulnerabilidad
Desastres naturales	Fuego	Falta de controles para detectar este tipo de daños.
	Daños por agua	Faltan controles para la detección de incendios.
	Daños por origen físico	Falta de controles de mantenimiento preventivo de hardware y software.
Errores no intencionados	Alteración de información	No existen controles de verificación de información y almacenamiento.
	Destrucción de información	No se hallan controles, falta de políticas de backups.
	Errores de configuración	Faltan controles para monitorear la configuración de activos.
	Error de mantenimiento	Falta de controles de mantenimiento preventivo.
	Fuga de información	No existe políticas en el manejo de información confidencial.

Ataques con intención	Ingreso no autorizado	No existen ningún tipo de control al momento de acceder a la información de la E.P.S.
	Estudio de trafico	Faltan políticas para monitoreo al tráfico de la red.
	Ataque destructivo	Faltan políticas de instalación y equipos informáticos.
	Ingeniería social	Falta de capacitación en seguridad informática al personal de la empresa.

Fuente: el autor

AUDITORIA DE CUMPLIMIENTO

Evaluación de cumplimiento

Se valora la etapa de cumplimiento de cada control que se encuentra contemplada bajo la norma ISO/IEC 27001:2013, a continuación, encontraremos cada dominio con el resultado asignado.

Tabla 48 Evaluación de cumplimiento

	Control	***Cumplimiento***	***Nivel***	***Departamento***	***Descripción***	***Porcentaje***
5	***Políticas de seguridad***					***80%***
5.1	*Normas establecidas en la protección de información*					
5.1.1	*Directrices de seguridad*	*Si*	*5*	*Seguridad*	*Administrado*	*80*
5.1.2	*Revisión de las políticas*	*Si*	*5*	*Seguridad*	*Administrado*	*80*
6	***Organización de la seguridad de la información***					***80%***
6.1	*Clasificación interna*					
6.1.1	*Roles y responsabilidades*	*Si*	*5*	*Seguridad*	*Administrado*	*80*
6.1.2	*División de deberes*	*Si*	*5*	*Seguridad*	*Administrado*	*80*
7	***Seguridad de recursos humanos***					***27%***
7.1	*Durante la ejecución*					
7.1.1	*Responsabilidades*	*Si*	*5*	*Recursos humanos*	*Administrado*	*80*
7.1.2	*Toma de conciencia*	*No*	*1*	*Recursos humanos*	*No existe*	*0*
7.1.3	*Proceso disciplinario*	*No*	*1*	*Recursos humanos*	*No existe*	*0*
8	***Gestión de activos***					***47%***
8.1	*Compromiso*					
8.1.1	*Inventario*	*Si*	*5*	*Recursos humanos*	*Administrado*	*80%*
8.1.2	*Uso de activos*	*No*	*3*	*Recursos humanos*	*Repetible*	*40%*
8.1.3	*Devolución*	*Si*	*5*	*Recursos humanos*	*Administrado*	*40%*
8.2	*Clasificación de información*					
8.2.1	*Clasificación información*	*No*	*3*	*Recursos humanos*	*Repetible*	*40%*

8.2.2	*Disposición de los medios*	*No*	*3*	*Recursos humanos*	*Repetible*	*40%*
8.2.3	*Manejo de información*	*No*	*3*	*Recursos humanos*	*Repetible*	*40%*
9	***Control de acceso***					***40%***
9.1	*Obligaciones en el control de acceso*					
9.1.1	*Política de control*	*Si*	*5*	*Seguridad*	*Administrado*	*80%*
9.2	*Gestión de acceso a usuarios*					
9.2.1	*Registro y cancelación del registro*	*No*	*3*	*Seguridad*	*Repetible*	*40%*
9.2.2	*Gestión de información de autenticación*	*No*	*1*	*Seguridad*	*Repetible*	*0%*
9.3	*Responsabilidades del usuario*					
9.3.1	*Uso de la información de autenticación secreta*	*No*	*1*	*Seguridad*	*No existe*	*0*
10	***Criptografía***					***0%***
10.1	*Inspecciones criptográficos*					
10.1.1	*Políticas sobre el uso de controles*	*No*	*1*	*Seguridad*	*No aplica*	*0*
10.1.2	*Gestión de llaves*	*No*	*1*	*Seguridad*	*No aplica*	*0*
14	***Sistema de adquisición, desarrollo y mantenimiento***					***10%***
14.1	*Requisitos de seguridad*					
14.1.1	*Análisis y descripción de necesidades*	*No*	*3*	*Seguridad*	*Repetible*	*40%*
14.2	*Seguridad en las técnicas de soporte*					
14.2.1	*Políticas de desarrollo seguro*	*No*	*1*	*Seguridad*	*No aplica*	*0*
14.2.2	*Ambiente de desarrollo seguro*	*No*	*1*	*Seguridad*	*No aplica*	*0*
14.2.3	*Protección de datos de prueba*	*No*	*1*	*Seguridad*	*No existe*	*0*
16	***Información de gestión de incidentes de seguridad***					***15%***
16.1	*Gestión de incidentes*					
16.1.1	*Reporte de debilidades de seguridad de información*	*Si*	*1*	*Seguridad*	*Administrado*	*20*
16.1.2	*Evaluación*	*No*	*1*	*Seguridad*	*No existe*	*0*
16.1.3	*Responsabilidad y procedimientos*	*Si*	*1*	*Seguridad*	*Administrado*	*40*
16.1.4	*Recolección de evidencias*	*No*	*1*	*Seguridad*	*No existe*	*0*
18	***Cumplimiento***					***8%***
18.1	*Desempeño de requisitos legales y contractuales*					
18.1.1	*Derechos de propiedad intelectual*	*No*	*1*	*Seguridad*	*Inicial*	*0*
18.1.2	*Reglamentación de controles criptográficos*	*No*	*1*	*Seguridad*	*No aplica*	*0*
18.1.3	*Revisión de seguridad de la información*	*Si*	*1*	*Seguridad*	*Inicial*	*0*

18.1.4	*Desempeño con las políticas y normas de seguridad*	*Si*	*1*	*Seguridad*	*Inicial*	*0*
18.1.5	*Observación del cumplimiento técnico*	*No*	*1*	*Seguridad*	*Inicial*	*40*

Fuente: El autor

CONTROLES Y PLANES DE TRATAMIENTO

Plan de tratamiento de riesgos. Se identifican cuales riesgos tienen amenazas o vulnerabilidades en común estos pueden ser tratados mediante diferente tipo de controles, partiendo del hecho de que puede servir para más de un control en la mayoría de los casos, en la siguiente tabla se describen los pasos a seguir para el tratamiento a los riesgos identificados.

Tabla 49 Controles y tratamiento de riesgos

Control	Riesgo encontrado	Referencia Norma ISO	Activo	Causa	Tratamiento	Actividad	Responsable
Control 1	Fuga de información	Criptografía	Información contractual, informes	No existen controles de seguridad para fuga de información	Mitigar riesgos	Implementar procedimientos para gestión de medios.	Oficina de sistemas
Control 2	Perdida de imputabilidad	Políticas de seguridad	Informe de depuración de datos Información del Correo electrónico	No existen políticas que definan el buen uso de los sistemas de información.	Mitigar riesgos	Deben ser aceptadas las políticas de seguridad por todos los empleados mediante una firma escrita. Las políticas de seguridad se deben examinar en dado caso que existan cambios.	Oficina de sistemas
Control 3	Pérdida de integridad de la información	*Organización de seguridad de la información. *Control de acceso. *Sistemas de adquisición, desarrollo y mantenimiento.	Información de novedad del personal	Personas no autorizadas puede consultar y modificar documentos del personal de todas las áreas.	Mitigar riesgos	*Revisar el acceso de a los activos de información. *Asignar los diferentes usuarios para el acceso de información. *Aplicar principios del menor privilegio.	Gerencia
Control 4	Pérdida de la confidencialidad de información	Gestión de activos	Carpetas Compartidas con información general	No existen controles de seguridad para la fuga de información	Mitigar riesgos	* Implementar procedimientos en la gestión de medios. * Si no se necesita el medio en la organización se debería remover de forma que no sea recuperable. * Requerir autorización a la hora de retirar un activo.	Oficina de sistemas
Control 5	Pérdida de la continuidad del proceso	Gestión de activos	Plan de acción y de adquisidores	La disposición física de las carpetas, así como el uso y traslados necesarios para la ejecución de las labores.	Asumir el riesgo	* Generar campañas de sensibilización sobre el uso y traslado de información. * Definir e implementar procedimiento de etiquetado y clasificación de la información. * Incluir archivos que permitan el almacenamiento seguro de la información.	Gerencia

Control 6	Extravió de la disponibilidad de datos	* Gestión de activos * Control de accesos	Bodega de datos	Presenta un alto grado de confidencialidad por lo que se requiere exclusividad en el almacenamiento.	Mitigar riesgos	* Definir políticas de control de acceso a los sistemas de información. *Definir políticas de almacenamiento de información. Debe ir alineado con el procedimiento. * Realizar estudio periódico de los derechos de acceso a la información.	Oficina de sistemas
Control 7	Perdida de la integridad de los datos	* Protección del bienestar * Criptografía	Base de datos	Los archivos de nómina o entidades financieras, se consolidan mediante un proceso manual.	Mitigar riesgos	* Realizar sensibilizaciones y toma de conciencia a los funcionarios sobre la seguridad de la información. * Establecer procedimientos de firma digital en la documentación critica garantizando la integridad de la información.	Secretaria
Control 8	Extravio de la integridad y disponibilidad de información	Control de acceso	Documentos de novedades del persona	Documentos de novedades del personal se compartida sin permisos definidos.	Mitigar riesgos	* Documentar, implementar y difundir políticas de control de acceso a la información. * Establecer instrucciones de registro, monitoreo y cancelación de acceso a la información. * Establecer un procedimiento de Gestión de Contraseñas para y asegurar. * Restringir el acceso a información confidencial a personas no autorizadas.	Secretaria Oficina de sistemas

Fuente: el autor

En la tabla 49 se agrupan los riesgos encontrados según la importancia relevante para los activos de información de la EPS Asmet Salud, los cuales pueden ser mitigados, compartidos, eliminados o aceptados, los controles que dan como resultado de la exposición de controles y riesgos sugeridos por la norma ISO 27001:2013, la aplicación de estos controles garantiza la defensa apropiada de las metas de la empresa, puesto que estos están directamente ligados a los activos de información de la misma.

POLÍTICAS

Política general. En la EPS Asmet Salud los datos son un recurso primordial con el fin de prestar los servicios y toma eficiente de decisiones, por esto se debe hacer un compromiso ante la protección de la información más significativas como parte estratégica hacia el afianzamiento de una cultura de seguridad. Como instrumento que admita establecer y reducir los peligros a que se ve expuesta la información, beneficia la disminución de costos, construye una sociedad segura garantizando el desempeño de las exigencias legales.

Los funcionarios que tienen responsabilidades sobre los procesos de información apropiándose de los lineamientos incluidos en el documento de las políticas, cuyo propósito es mantener la disponibilidad, confidencialidad e integridad de datos. Apoyándose por normas e instrucciones encaminando el uso apropiado de los datos de la EPS sujetos al modelo ISO 27001:2013.

Política de protección de la información. La Gerencia de Asmet Salud tiene la responsabilidad de aprobar y divulgar las estrategias en protección de los datos, siendo aprobadas por todo el personal de la EPS, mediante una firma escrita; lo anterior asegura el derecho de la EPS, al principio de repetición e investigación sobre delitos informáticos.

Para ello previamente, la EPS Asmet Salud, debe aprobar, difundir y sensibilizar a funcionarios en las estrategias de protección de la información, se deben verificar los diferentes cambios que pueden ocurrir en intervalos, salvaguardando la eficacia y continua adecuación.

Organización en la protección de la información. El compromiso en la protección de los datos, no es exclusiva de la gerencia de la EPS Asmet Salud, es un compromiso de todas las áreas que componen la EPS, y de cada uno de los empleados de la misma.

El personal no debe suministrar ningún tipo de información de la EPS, a personas externas sin las autorizaciones respectivas. La oficina de sistemas de la empresa debe verificar los permisos de acceso de a la información por parte de cada uno de los funcionarios.

Gestión de activos. Los titulares de los datos son los responsables de seleccionarla conforme al rango de sensibilidad, la gerencia de la EPS, en colaboración del departamento de sistemas debe implementar programas de sensibilización y divulgación de normas para la seguridad de información.

Es obligación de empleados de la EPS realizar gestión de incidentes adecuada aplicando las enseñanzas aprendidas, aplicando acuerdos de confidencialidad de los datos, se deben formalizar sensibilizaciones y toma de conciencia a los empleados sobre la seguridad.

Seguridad de recursos Humanos. El personal vinculado con la EPS debe tener conocimiento y poner en práctica la presente política independiente del tipo de vinculación que tenga con la EPS, teniendo la obligación de sostener la información reservada que le sea facilitada para desarrollar sus actividades.

Se deben implantar políticas de uso en los activos de información en el que considere los roles responsables, cuando los recursos son retirados se debe hacer registro documentado y aprobado por parte de la empresa. La gerencia debe realizar campañas de sensibilización sobre el uso y traslado de información que se genere en la empresa con el compromiso y responsabilidad sobre la información que se maneja.

Es responsabilidad de la oficina de sistema definir y establecer técnicas de etiquetado o clasificación de los datos que ayude al control e identificación de la información tanto en su generación, transito o destrucción. Es necesario incluir archivos que permitan el almacenamiento seguro de la información implementando controles que permitan la trazabilidad del uso o préstamo de la información.

Control de acceso. La gerencia de la EPS en combinación con el departamento de sistemas de Asmet salud son responsables de implementar controles de seguridad en el monitoreo y control de las instalaciones como también en el registro de ingreso.

Conforme a las labores de cada empleado se realizarán instrucciones con el fin de denegar o proporcionar acceso a internet o a las redes, teniendo en cuenta la

distribución con los datos se establecen métodos para el respaldo y backups, efectuar controles adicionales para identificar posibles intrusos.

Sistemas de adquisición, desarrollo y mantenimiento. El departamento de tecnologías tiene como responsabilidad diseñar las fechas y tiempos en los que se realizaran los diferentes tipos de mantenimiento tanto en el servidor como en los medios de almacenamiento de información, también creación de roles y responsabilidades. Se debe especificar métodos a la hora de ejecutar backups o copias de seguridad donde se especifiquen los sistemas críticos de información como los métodos de realizar la restauración cuando sea necesario.

Cumplimiento. Se debe implementar procesos legales para asegurar que la información entregada sea integral; incluyendo firma de cláusulas y acuerdos donde se involucre las técnicas de asociamiento en la administración del servicio de la empresa con sus usuarios.

Se debe realizar exploraciones a los niveles de cumplimiento en los servicios suministrados en la EPS, y verificar el cumplimiento de los acuerdos, la gerencia o quien delegue estará encargada de revisar periódicamente los informes de servicio elaborados por los empleados llevando a cabo auditorías y acciones sobre las cuestiones identificadas.

9. MANUAL DE POLÍTICAS

INTRODUCCION

El SGSI está basado en un enfoque hacia la gestión de amenazas para la protección de información en cualquier empresa, con el propósito de determinar, implementar y mejorar la protección de los datos, no es un solo proceso, es un sistema que sirve para componer la protección de información, inicialmente en el alcance certificando y extendiéndose de forma general en la organización.

Este documento contiene una guía de políticas en protección de la información para Asmet Salud EPS, con la intención de ofrecer como un archivo concentrado de información y procedimientos que serían necesarios concediendo procesos en las respuestas y decisiones en cualquier tipo de interrupción en las operaciones de los servicios prestados.

OBJETIVO

Exponer a los empleados y personas relacionadas con la E.P.S. Asmet Salud los diferentes estándares y políticas de seguridad que se deben llevar a cabalidad para cumplir con el fin de mantener la protección de los datos, activos e información y su preservación.

ALCANCE

Las políticas determinadas en este manual, serán para la aplicación de empleados y personas que tienen algún tipo de relación con la E.P.S. Asmet Salud, como también para el uso de cualquier activo informático que este en el interior de la infraestructura de la EPS.

REVISIÓN

Las políticas establecidas en este manual tendrán una revisión anual o en su defecto cuando se reporte algún cambio que pueda afectar dichas políticas en la entidad, asegurando el adecuado servicio y protección de la información que se maneja en cada requerimiento identificado.

En la tabla 50, se podrá observar las diferentes políticas que se han estipulado en el manual que será aplicado a todos los empleados de la EPS Asmet Salud, para dar cumplimiento con el diseño de un SGSI apoyado en los controles del estándar ISO/IEC 27001-2013.

Tabla 50 Políticas

Política	Descripción
General	Es el reconocimiento general que constituye la posición de la EPS Asmet Salud respecto al resguardo de recursos informáticos, soportado los procesos y lineamientos que se basan dentro de la misión, visión y funciones de la EPS, así mismo en la asignación de responsabilidades generales y específicas en la administración de la seguridad de información. Asmet Salud E.P.S., se compromete a proteger la información que es generada en los procesos que se manejan en la prestación de los diferentes servicios, se definen lineamientos para lograr mitigar riesgos en las diferentes dependencias que manejan información. La E.P.S. Asmet Salud se compromete a proteger la información procesada en los diferentes procesos que se manejan, como también de las instalaciones físicas evitando el acceso de personal o autorizado que puedan generar riesgos, interferencia o daños de la información que se maneja.
Gestión de recursos	Esta clasificación va conforme a la sensibilidad y reserva de la misma y se identifica el responsable del mismo, los empleados una vez terminado su contrato deben de hacer entrega de los activos físicos y de la información para continuar con los trámites de finalización del empleo. No es permitido el uso de almacenamiento en línea o cualquier programa que se utilice por medio de internet, es prohibido que los empleados descarguen, utilicen o manipulen programas no autorizados causando perdida en los servicios.

	La realización de backups se debe programar con el departamento de sistemas quienes son los únicos que tienen permiso de extraer información confidencial. Los equipos que se emplean por los empleados para el cumplimiento de sus funciones no se deben utilizar para propósitos personales como escuchar música, reproducción de videos, entre otros, solo se deben utilizar para el almacenamiento de información de la EPS.
Seguridad de los recursos humanos	Los empleados deben comunicar las anomalías, o riesgos de información que puedan afectar los equipos y los datos ante el departamento de sistemas. El departamento de sistemas realiza revisión periódica de cada elemento asignado a los empleados para el cumplimiento de sus funciones para optimizar su buen funcionamiento. Los empleados al ingresar a trabajar en la EPS, firman un compromiso de confidencialidad en el uso de información privada como también de sus funciones y compromisos. Los directivos de la EPS, presentaran capacitaciones sobre temas relacionados con la protección de los datos en todos los departamentos o áreas de la empresa, para así poder disminuir las amenazas que se puedan presentar. En el momento que se termine un contrato, este debe ser informado al departamento de sistemas para desactivar y eliminar los diferentes usuarios y contraseñas creadas para los funcionarios de la empresa.
Acuerdos de Confidencialidad	Las personas que aspiran a posesionarse en un cargo dentro de la EPS Asmet Salud, aceptara las condiciones sin perjudicar la protección de la información.
Respaldo	Toda información que maneja Asmet Salud EPS tendrá que ser resguardada periódicamente a través de controles y lineamientos apropiados certificando la confidencialidad, disponibilidad e integridad de los datos. Para la realización Backups la empresa debe elegir medios de almacenamiento de buena calidad y estos medios a su vez deben de estar en inmediaciones externas donde

	funciona la E.P.S., cumpliendo con las medidas y controles de seguridad.
Uso de internet	El acceso a internet deberá ser usados con fines estrictamente laborales, los empleados deben abstenerse de ingresar a páginas que no son permitidas por la empresa. Actividades no permitidas: ✓ Descarga de archivos, música, videos y otros contenidos de multimedia. ✓ No utilizar los equipos de cómputo para chats y redes sociales.
Uso de correo electrónico institucional	El correo electrónico asignado por la E.P.S., es para uso laboral, los empleados deben de abstenerse de enviar información por este medio y que no tenga que ver con las funciones asignadas, acatando las normas de seguridad para su utilización y evitar el uso de software malicioso. No permitido: ✓ El envío de spam a usuarios. ✓ Cometer acciones ilícitas desde el correo empresarial. ✓ No se permite el envío de archivos ejecutables.
Uso de software	Para actualizar cualquier software, los empleados tendrán que hacer la solicitud al departamento de sistemas quienes son los encargados de estas actualizaciones. Cada empleado se hará cargo de cada activo informático asignado por el departamento de sistemas para la ejecución de tareas asignadas.
Contraseñas	Cada funcionario es responsable de su usuario y contraseña que se le es asignado para cada función. Los empleados que ingresan a la empresa para poder iniciar labores deben cambiar la contraseña asignada cumpliendo con los siguientes parámetros: ✓ Debe tener como mínimo ocho caracteres. ✓ Debe poseer caracteres alfanuméricos. El departamento de sistemas envía un mensaje a cada equipo cada 60 días solicitando el cambio de contraseña, al

	no hacerse el usuario se bloqueara y deberá hacer solicitud de desbloqueo ante este departamento.
Protección contra software malicioso	Cada equipo informático debe tener instalada una aplicación para la detección de cualquier ataque informático que se pueda presentar, se debe asegurar que esta aplicación o programa se actualice permanentemente y no pueda ser manipulada por ninguna persona. Todo empleado debe hacer un scanner de cualquier dispositivo de almacenamiento móvil antes de ser utilizado en los equipos para no poner en peligro la información que esta albergada en estos.
Gestión de incidentes	Los empleados de la EPS Asmet Salud, se comprometen a informar cualquier evento que perjudique la disponibilidad, confidencialidad e integridad dentro de la protección de datos. El departamento de sistemas es el encargado para la realización de configuración y mantenimiento de los equipos informáticos que se utilizan en la empresa. Asmet Salud EPS, define los controles que se deben manejar la administración de incidentes en la protección de información, garantizando buen funcionamiento en las actividades de planificación, atención y mejora continua.

Fuente: el autor

10. PLAN DE CONTINUIDAD

Es de gran importancia que la EPS Asmet Salud cuente con un esquema de continuidad, que certifique los movimientos que corresponden seguir cuando se presenten casos de riesgos y amenazas, por lo que este plan tiene que ser conocido por cada uno de los empleados con el propósito de minimizar riesgos, protegiendo los datos que se maneja.

ESTUDIO Y EVALUACIÓN DE RIESGOS

Tabla 51 Procesos de la empresa

	Proceso	Descripción	Responsable
Estratégicos	Planeación estratégica	Formular, diseñar y establecer programas orientados al logro de los resultados	Departamento de Planeación y calidad
	Gestión jurídica	Asegurar la defensa de intereses de la EPS Asmet Salud siempre enmarcadas en normas legales vigentes.	Departamento de Jurídica
Apoyo	Talento Humano	Programar actividades de bienestar, promoviendo el desarrollo de la empresa fomentando un excelente ambiente laboral.	Departamento talento humano
	Gestión financiera	Ejecutar actividades de administración de los recursos financieros	Departamento de recursos financieros
	Bienes y servicios	Programar la adquisición de bienes y servicios por cada una de las dependencias de la EPS.	Departamento recursos financieros
Evaluación	Control interno	Establecer objetivos para la evaluación de controles, gestión, resultados y seguimiento en la mejora de la EPS	Departamento de control interno
	Calidad garantía	Originar el proceso de mejora en disposición en la atención de usuarios, implementando tácticas de evaluación y monitoreo.	Departamento de Planeación y calidad

Fuente: el autor

SELECCIÓN DE ESTRATEGIAS

- ✓ Garantizar la efectiva detección, restauración y recuperación de daños efectuados dentro del sistema, volviendo a las condiciones normales de funcionamiento.

- ✓ Tomar las medidas necesarias frente a interrupciones presentadas en el servicio suministrado, considerando la misión de la empresa.

EJECUCIÓN DEL PLAN

Tabla 52 Ejecución del plan

Fallos en software	✓ Informar los inconvenientes presentados a todas las áreas de la EPS. ✓ Hacer uso de documentos manuales para continuar la operación de las funciones mientras se recupera el sistema. ✓ Verificar que la información suministrada en los documentos sea ingresada al sistema de manera clara.
Fallos en Hardware	✓ Informar los inconvenientes presentados a todas las áreas de la EPS. ✓ Hacer uso de documentos manuales para continuar la operación de las funciones mientras se recupera el sistema. ✓ Determinar el origen de la falla y establecer tiempos de mejora. ✓ Verificar que la información suministrada en los documentos sea ingresada al sistema de manera clara.
Daño en servicio de internet	✓ Informar los inconvenientes presentados a todas las áreas de la EPS. ✓ Determinar el origen de la falla. ✓ Realizar cambio de equipo si la falla presentada es de la EPS. ✓ Comunicar a la empresa prestadora del servicio la falla ocurrida.
Daño en servicio de correo electrónico	✓ Informar los inconvenientes presentados a todas las áreas de la EPS. ✓ Se realiza revisión de los servidores para saber dónde ocurrió el problema. ✓ Reiniciar equipos para validación del servicio.
Daño en equipo de cómputo	✓ Informar al departamento de sistemas la falla ocurrida en el equipo de cómputo. ✓ Identificar el tipo de daño y verificar el tipo de arreglo. ✓ De ser necesario el traslado del equipo, informar del hecho. ✓ Realizar el paso de la información del equipo afectado a otro para la continuación de labores. ✓ Dar a conocer cuando el equipo ya esté en óptimas condiciones para su reintegro.

Fuente: el autor

PRUEBAS Y MANTENIMIENTO

Se debe hacer revisión y actualización del plan de continuidad habitualmente, e integrarlo a las funciones y procesos que se realizan a diario por parte de la EPS Asmet salud, dar a conocer en todas las áreas la importancia que tiene el presente plan de continuidad con el fin de perfeccionar cada proceso que se presta.

11. RESULTADOS

El diseño de SGSI entregado a la EPS Asmet Salud tiene como finalidad disminuir las amenazas las cuales se puedan presentar y estar exhibida, minimizando fuga de información, en especial de los datos confidenciales, esto con intensión de mejorar el nivel seguridad.

Con el diseño del SGSI ayudará a la EPS Asmet Salud a implantar políticas y controles para la protección de la información, con la intención de salvaguardar los niveles de exposición, minimizando conflictos a la que pueda estar expuesta con fin de proteger de forma adecuada los activos y los diferentes tipos de datos que se manejan.

Análisis y discusión

Después de plasmar detalladamente cada control y asumiendo que la empresa definió que el 60% o más el nivel aceptable de cumplimiento, se puede concluir que hace falta trabajar mucho más para poder alcanzar los estándares mínimos del SGSI, es de anotar que en la actualidad la empresa obtiene un 35% del cumplimiento de la norma.

Distribución de controles:

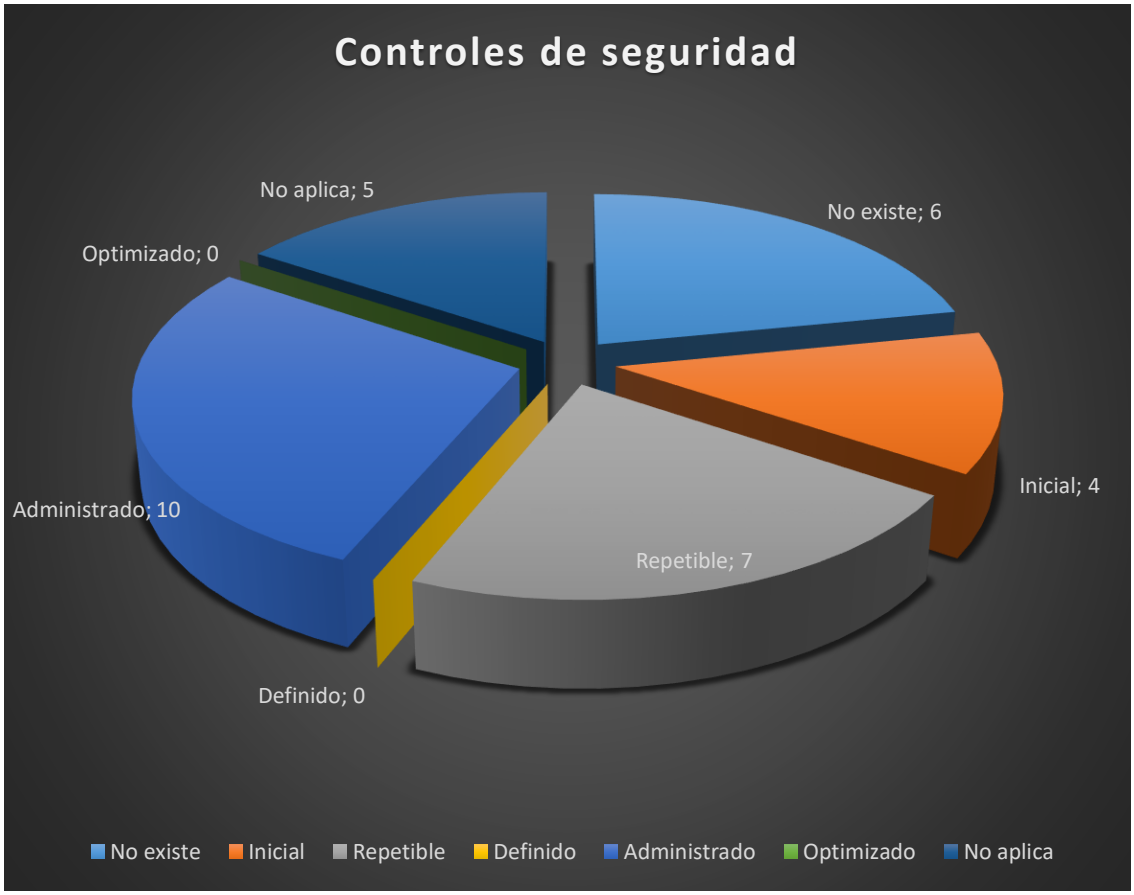
Tabla 53 Nivel de controles

Nivel	Control
Administrado	10
No existe	6
Repetible	7
No aplica	5
Inicial	4
Definido	0
Optimizado	0

Fuente: El autor

Podemos apreciar que en la empresa cuenta con 10 controles a los que se les efectúa comprobación, 6 controles que no existen, 7 controles sin documentar, 5 controles que no se aplican y 4 controles de alguna practica con inconsistencias.

Grafica 24 Estado de madurez



Fuente: El autor

Tabla 54 Cumplimiento por dominios

	Control	Porcentaje
5	*Políticas de seguridad*	*80%*
6	*Organización de la seguridad de la información*	80%
7	*Seguridad de recursos humanos*	27%
8	*Gestión de activos*	47%
9	*Control de acceso*	40%
10	*Criptografía*	0%
14	*Sistema de adquisición, desarrollo y mantenimiento*	10%
16	*Información de gestión de incidentes de seguridad*	15%
18	*Cumplimiento*	16%
	TOTAL	**35%**

Fuente: El autor

Grafica 25 Estado actual y esperado de los dominios

Fuente: El autor

Podemos observar la diferencia del estado actual en el que se encuentra la empresa en lo relacionado a seguridad informática, los controles que se establecieron dentro del proyecto los podemos identificar con el color amarillo y con el color verde los niveles esperados por estos, para la empresa Asmet Salud se definió un promedio entre el 80 – 100 %, cabe anotar que dos de estos dominios alcanzan el nivel esperado dentro del análisis de diseño del SGSI.

12. CONCLUSIONES

El diseño de un sistema de gestión de seguridad de la información permitió emparejar las amenazas existentes en la EPS Asmet Salud, los cuales exponen los activos de información a algún tipo de vulnerabilidad que afecte la disponibilidad, confidencialidad e integridad; y realizar una clasificación de estos de acuerdo a valores dados a los riesgos.

La clasificación de activos proporcionó información notable que permite afirmar que la clasificación de estos es independiente, ya que este tipo de clasificación se ajusta a las necesidades, para la EPS Asmet Salud se platearon criterios de clasificación de acuerdo con las necesidades de la EPS y con el perfil del recurso humano que labora en ella.

Se logra efectuar el análisis que le facultará a la empresa Asmet Salud la ejecución de un SGSI apoyado en el modelo ISO/IEC 27001:2013, trazando medidas utilizando fortalezas manejando temas relacionados con seguridad y minimizando al máximo la cantidad de debilidades a la que se encuentra expuesta la empresa ante cualquier ataque informático.

Se logró efectuar el análisis que otorgara la ejecución del SGSI apoyado por el modelo ISO/IEC 27001:2013, planteando soluciones en la protección de datos minimizando los diferentes peligros a que se ve expuesta la E.P.S. Los resultados arrojados de las vulnerabilidades encontradas indican que la empresa Asmet Salud cuenta con un nivel bajo en cuanto a medidas de seguridad, lo que permitió instaurar y demonstrar las estrategias en la protección de información, de igual forma se sugirieren algunas pautas para lograr blindar la organización ante ataques informáticos.

El diseño de un SGSI permitió identificar las debilidades existentes en la EPS Asmet Salud los cuales exponen los recursos de información a cualquier tipo de vulnerabilidad perjudicando la disponibilidad, confidencialidad e integridad; también permitió clasificar los riesgos, los cuales deben ser analizados, evaluados y controlados hasta llevarlos a un nivel aceptable.

La E.P.S. Asmet Salud posee debilidades en cuanto a políticas y controles de seguridad se habla que son significativas, por otro lado, las fortalezas son escasas en contenidos respectivos con la protección de la información, lo que representa que la empresa se encuentre vulnerable ante cualquier ataque informático.

Este proyecto permite detallar las utilidades que se pueden obtener en el momento de instalar un sistema de gestión de seguridad de la información apoyado en el modelo ISO/IEC 27001-2013 para cualquier sociedad, por medio en la etapa en diseño permite implantar documentación necesaria para realizar un mejoramiento

continuo, además de saber el estado de los controles de seguridad que se encuentran establecidos al interior de la empresa objeto de estudio, a su vez, se logra elaborar las diferentes normas para la protección de información.

Al mismo tiempo se logró saber las normas en las cuales hay falencias dentro de la EPS, políticas de seguridad que se encuentran, pero no están documentadas, clasificar activos con más falencias que demandan de mayor atención por los diferentes peligros a los que se ve expuesta la empresa, para lo cual se proponen distintos controles y políticas que se pueden establecer para minimizar cualquier impacto negativo en la presentación de los diferentes servicios.

13. RECOMENDACIONES

Con el propósito de mejorar, se recomienda a los altos administrativos de la EPS Asmet Salud que se tome el presente proyecto como una guía a la hora de tomar decisiones estratégicas que conllevan al cumplimiento con los controles, técnicas y políticas de protección que consiste con la implementación del diseño de un SGSI fundamentado en el modelo ISO/IEC 27001:2013, no solo para el departamento o área de sistemas si no que involucre a todos los funcionarios que a diario realizan funciones dentro de esta empresa.

La empresa requiere efectuar un orden de registros cuyo propósito de favorecer la protección de la información y dar consecución a las solicitudes establecidas en la norma ISO 27001:2013, es de vital importancia realizar capacitaciones en temas relacionados con la protección de la información, creando conciencia y sentido de pertenencia a los funcionarios de la EPS.

A su vez obtener mayor precisión a la hora de determinar las amenazas que pueden presentarse al interior o exterior de las oficinas y puedan afectar los activos, por otra parte, el compromiso que se debe adquirir a la hora de capacitar a los empleados en los contenidos respectivos con la protección de los datos, documentándoles e informándoles sobre los tipos de vulnerabilidades, como también las diferentes políticas y controles de seguridad que se pueden utilizar para salvaguardar todo tipo de información, considerando que es un tema que tiene que ver con todos y no solo con el personal de sistemas.

Por otra parte, se recomienda a la EPS suministrar información de seguridad informática a sus empleados en el uso diario de los activos tecnológicos que son empleados para cumplir con sus funciones y lograr buenas prácticas de seguridad minimizando riesgos que puedan poner en peligro los datos suministrados.

Es de suma importancia tener presente los resultados obtenidos en la gestión de amenazas y no ser ignorados, ya que a largo plazo estos pueden llegar a ocasionar daños que es a lo que el presente diseño de un SGSI quiere llegar a promover en las prácticas de seguridad con el fin de mantener un control sobre los mismos.

Por último, se recomienda seleccionar personal altamente capacitado para que tomen las riendas y lideren los diferentes procesos de seguridad, determinando la viabilidad y la factibilidad, de continuación con las diferentes políticas que se establecen en un SGSI.

14. BIBLIOGRAFÍA

Díaz, A.; Collazos, G.; Cortez Lozano, H.; Ortiz, L. y Herazo Pérez, G. 2011. Sistema para el control de gestión de seguridad de la información. Recuperado de: http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

DURANGO MARIN, José Alejandro. Ciclo PHVA institución universitaria escolme. Recuperado de http://www.escolme.edu.co/almacenamiento/oei/tecnicos/ppios_admon/contenido_u3_2.pdf

GIL FERNÁNDEZ, Raúl José. Sistematización de la gestión de riesgos de seguridad de la información en la red de la universidad Centroccidental "Lisandro Alvarado" (REDUCLA). Recuperado de: https://pide.wordpress.com/2011/06/08/sistematizacion-de-la-gestion-de-riesgos-de-seguridad-de-la-informacion-en-la-red-de-la-universidad-centroccidental-%E2%80%9Clisandro-alvarado%E2%80%9D-reducla/

NIETO MUÑOZ, Juan Pablo. Plan de implementación de la ISO/IEC 27001:2005. 2013. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23054/1/Nieto_WP2013_PlanImplementacionISO2007.pdf

RODRÍGUEZ CORREA, Jorge Leonardo. Diseño de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001 para laboratorios servicios farmacéuticos de calidad SFC LTDA. Recuperado de: http://repository.unad.edu.co/bitstream/10596/12598/1/1097035128.pdf

ROJAS VALDUCIEL, Halena. Trabajo Final De Máster. Plan de Implantación de SGSI según norma ISO/IEC 27001:2013. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/40297/7/hrojasvTFM1214presentaci%C3%B3n.pdf

Sistema de Gestión de la Seguridad de la Información. Recuperado de: http://www.iso27000.es/download/doc_sgsi_all.pdf

La norma ISO 27001:2013 ¿Cuál es su estructura? Recuperado de: https://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/

Política de atención integral en salud, MINSALUD. Recuperado de: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/modelo-pais-2016.pdf

ÁVILA FUNES, José Alberto. Confidencialidad de la información. Tomado de: http://www.innsz.mx/opencms/contenido/investigacion/comiteInvestigacion/confidencialidadInformacion.html

Belt Ibérica S.A. Confidencialidad, integridad y disponibilidad de la información. Tomado de: http://www.belt.es/expertos/HOME2_experto.asp?id=2245

Gestión de seguridad de la información, tomado de: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

ISO 27001: El método MAGERIT. Tomado de https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

Lloyd's Register. ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información. Tomado de: http://www.lrqa.es/certificaciones/iso-iec27001/

Blog especializado en Sistemas de Gestión de Seguridad de la Información. Norma ISO 27002: El dominio político de seguridad. Tomado de https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

ISOTools. ISO/IEC 27004. Evaluación de la Seguridad de la Información. Tomado de: https://www.isotools.cl/isoiec-27004/

Blog especializado en Sistemas de Gestión de Seguridad de la Información. ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información. Tomado de: https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

MINTIC. Ley 1273 de 2009. Tomado de: https://www.mintic.gov.co/portal/604/w3-article-3705.html

ICONTEC. Norma técnica NTC-ISO/IEC colombiana 27001. Tomado de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Congreso de la república. Ley 1288 de 2009. Tomado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1288_2009.html

Congreso de la república. Ley 1341 del 30 de julio de 2009. Tomado de: http://www.mintic.gov.co/portal/604/articles 3707_documento.pdf

MINTIC. Ley 1341 de 2009. Tomado de: https://www.mintic.gov.co/portal/604/w3-article-3707.html

Ley de delitos informáticos ley Nº 30096. Tomado de: http://www.derecho.usmp.edu.pe/cedetec/normas/Ley_Delitos_Informaticos_Ley_30096.pdf

Ley de Grooming. Tomado de: https://www.argentinacibersegura.org/noalgrooming/ley-de-grooming

Gaceta oficial de la república bolivariana de Venezuela. Ley especial contra los delitos informáticos. Tomado de: https://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

15. ANEXOS

AVAL PROYECTO DE GRADO

...cuida la salud de mi familia !

Timaná, 23 de Agosto de 2018

Señores
COMITE DE TRABAJO DE GRADO
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
Ciudad

Ref. AVAL PROYECTO DE GRADO

Por medio de la presente en nombre de la EPS Asmet salud se permite comunicarles que a concedido autorización y apoya el proyecto e grado denominado "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BAJO LA NORMA ISO 2701:2013 EN LA EPS ASMET SALUD" el cual será desarrollado por el estudiante de especialización en seguridad informática Jonathan Fernando Reyes Artunduaga con C.C. 1,024,461,092. Dicho proyecto tiene como objetivo desarrollar el DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BAJO LA NORMA ISO 2701:2013 con sus respectivos controles y procedimientos.

Para constancia se firma en Timaná el 23 de agosto de 2018

JORGE ELICER FAJARDO RODRIGUEZ
GO Asmet Salud EPSS
Cel 3112110493

ENCUESTA REALIZADA A LOS FUNCIONARIOS DE LA EPS ASMET SALUD

Anexo 1 Encuesta

PREGUNTAS	RESPUESTAS	
	SI	NO
¿En esta sede de Asmet Salud, existe un Sistema de Gestión de Seguridad Información?		
¿El talento humano recibe capacitación sobre temas de seguridad de la información?		
¿Existen políticas para el cambio de contraseñas?		
¿Recibe mantenimiento periódicamente el equipo de cómputo asignado para sus funciones?		
¿Realiza copias de la información?		
¿El computador asignado tiene instalado antivirus?		
¿el software que maneja la empresa para las funciones es legal?		
¿Se realiza mantenimiento a los equipos en la empresa?		
¿Cuenta con ventilación el lugar donde están los equipos PC?		
¿Los equipos de cómputo se encuentra asegurados mediante pólizas?		
¿Existe algún tipo de control a la hora de navegar en internet?		
¿Existe alguna política para el uso del correo electrónico?		
¿Es conveniente que Asmet Salud invierta en la ejecución de un SGSI?		

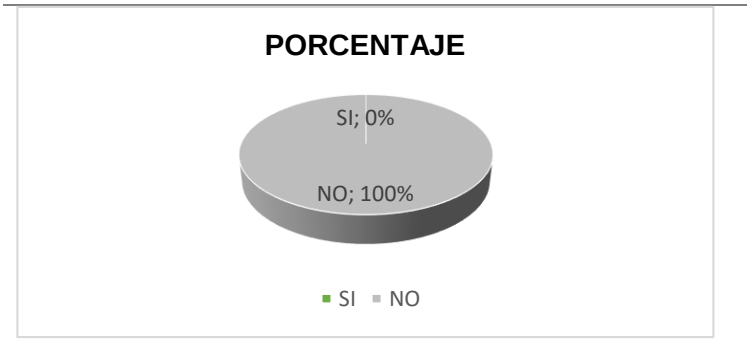
Fuente: El autor

RESULTADOS DE LA ENCUESTA

Para la presentación de los resultados de esta investigación, la encuesta practicada al personal de la empresa Asmet Salud, nos arroja los siguientes resultados:

Pregunta 1. ¿En esta sede de Asmet Salud, existe un Sistema de Gestión de Seguridad de la Información?

Figura 1 Pregunta 1



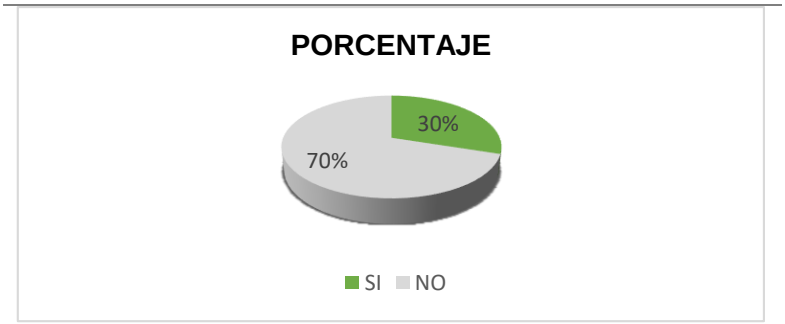
ITEM	ENCUESTADOS	PORCENTAJE
SI	0	0%
NO	10	100%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: al realizar la encuesta 10 empleados manifiestan que no existe un SGSI dentro de la empresa.

Pregunta 2. ¿El talento humano recibe capacitación sobre temas de seguridad de la información?

Figura 2 Pregunta 2



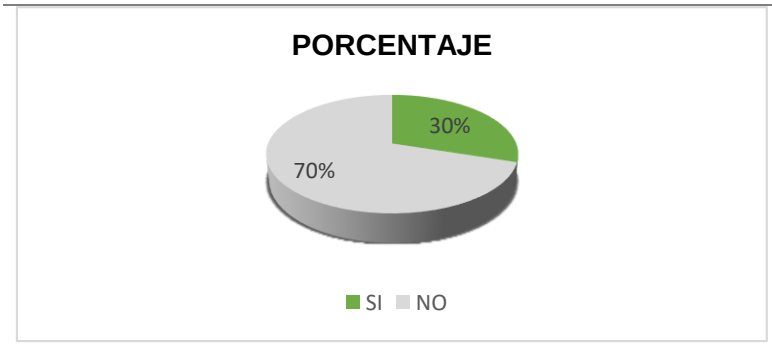
ITEM	ENCUESTADOS	PORCENTAJE
SI	3	30%
NO	7	70%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: al realizar la encuesta a los 10 funcionarios, 7 manifiestan que no son capacitados en temas de seguridad de la información y 3 manifiestan que la empresa si los ha capacitado en estos temas.

Pregunta 3. ¿Existen políticas para el cambio de contraseñas?

Figura 3 Pregunta 3



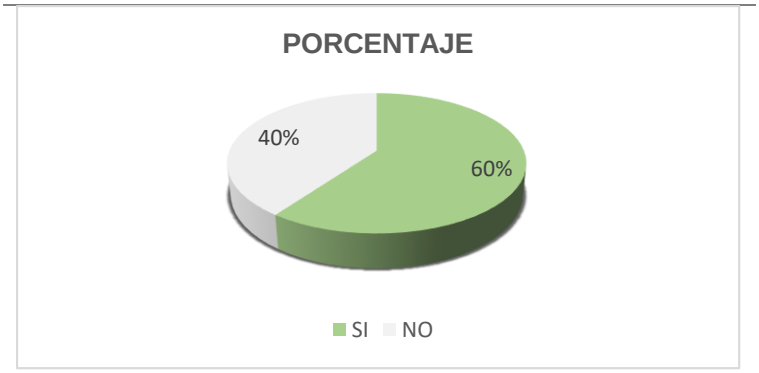
ITEM	ENCUESTADOS	PORCENTAJE
SI	3	30%
NO	7	70%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: al realizar la encuesta 10 empleados, 3 manifiestan que si hay políticas para el cambio de contraseña y 7 manifiestan que no la hay.

Pregunta 4. ¿Recibe mantenimiento periódicamente el equipo de cómputo asignado para sus funciones?

Figura 4 Pregunta 4



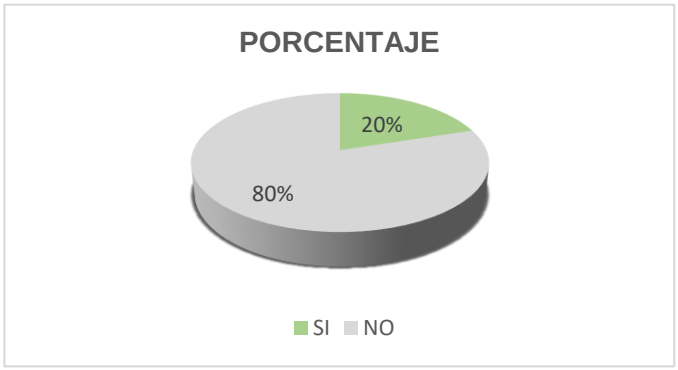
ITEM	ENCUESTADOS	PORCENTAJE
SI	6	60%
NO	4	40%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: al realizar la encuesta 6 de los 10 empleados manifiestan que si se realiza mantenimiento mientras 4 empleados refieren que no se realiza periódicamente.

Pregunta 5. ¿Realiza copias de la información?

Figura 5 Pregunta 5



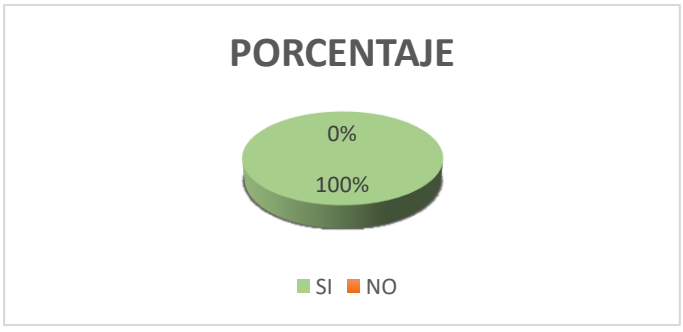
ITEM	ENCUESTADOS	PORCENTAJE
SI	2	20%
NO	8	80%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: al realizar la encuesta 8 empleados manifiestan que no realizan copias de seguridad mientras 2 empleados si las realizan.

Pregunta 6. ¿El computador asignado tiene instalado antivirus?

Figura 6 Pregunta 6



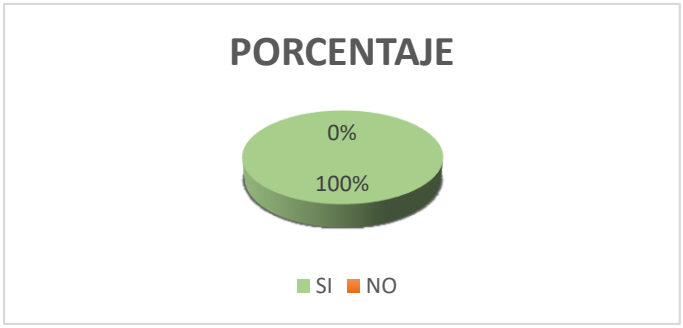
ITEM	ENCUESTADOS	PORCENTAJE
SI	10	100%
NO	0	0%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: después de realizar la encuesta se puede manifestar que todos los computadores de la empresa tienen antivirus.

Pregunta 7. ¿el software que maneja la empresa para las funciones es legal?

Figura 7 Pregunta 7



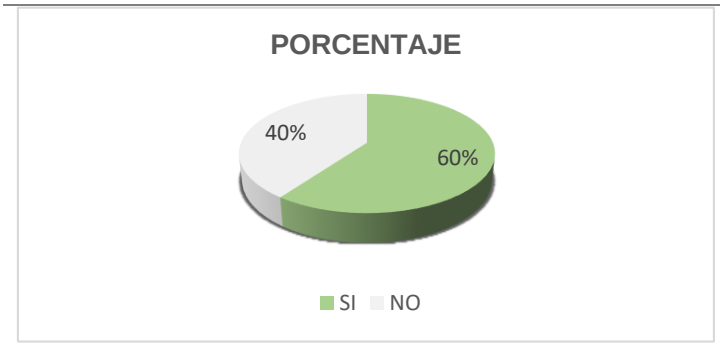
ITEM	ENCUESTADOS	PORCENTAJE
SI	10	100%
NO	0	0%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: los funcionarios de la empresa encuestados manifiestan que el software que manejan para la realización de las funciones es legal.

Pregunta 8. ¿Se realiza mantenimiento a los equipos en la empresa?

Figura 8 Pregunta 8



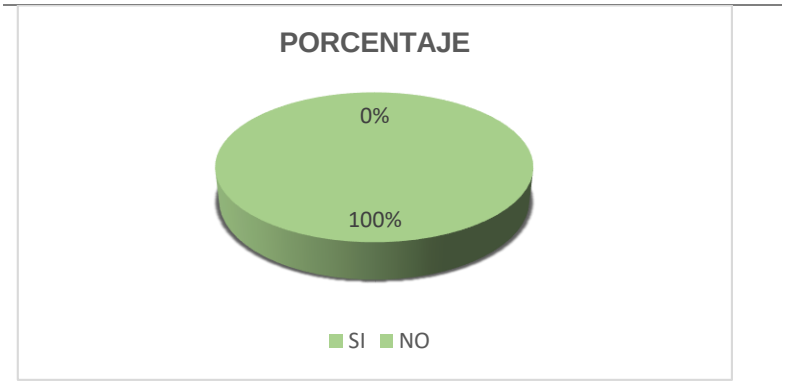
ITEM	ENCUESTADOS	PORCENTAJE
SI	7	70%
NO	3	30%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: al revisar las respuestas de la encuesta 7 empleados manifiestan que, si se les hace mantenimiento a los equipos, mientras 3 refieren que no.

Pregunta 9. ¿Cuenta con ventilación el lugar donde están los equipos PC?

Figura 9 Pregunta 9



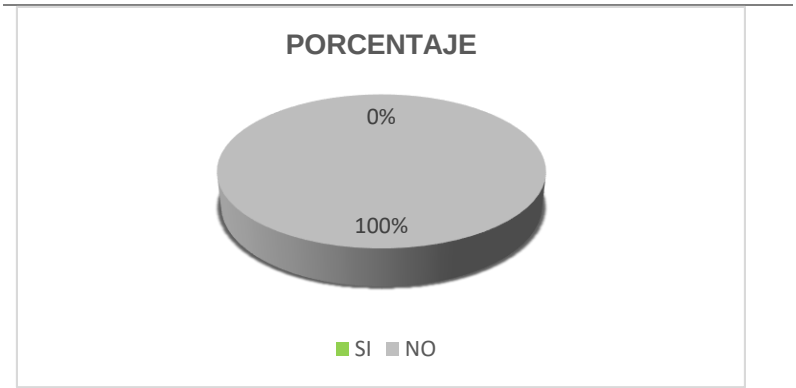
ITEM	ENCUESTADOS	PORCENTAJE
SI	10	100%
NO	0	0%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: todos los empleados que respondieron la encuesta manifiestan que si cuentan con ventilador en su puesto de trabajo.

Pregunta 10. ¿Los equipos de cómputo se encuentra asegurados mediante pólizas?

Figura 10 Pregunta 10



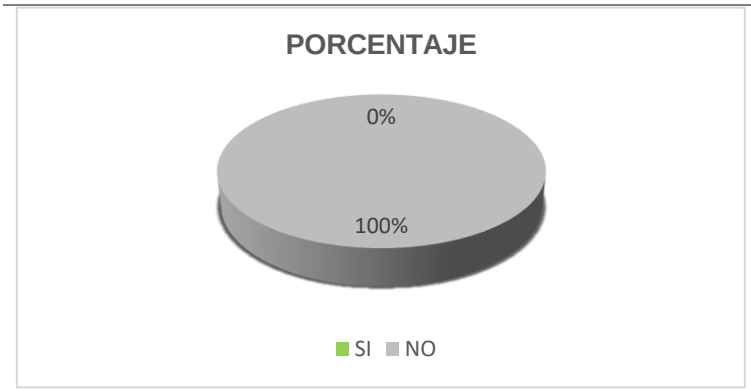
ITEM	ENCUESTADOS	PORCENTAJE
SI	10	100%
NO	0	0%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: el 100% manifiestan que los equipos no se encuentran asegurados.

Pregunta 11. ¿Existe algún tipo de control a la hora de navegar en internet?

Figura 11 Pregunta 11



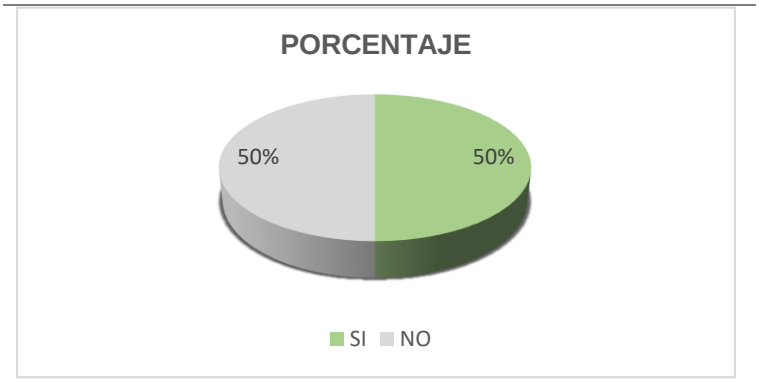
ITEM	ENCUESTADOS	PORCENTAJE
SI	0	0%
NO	10	100%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: en su totalidad, los funcionarios encuestados manifiestan que no hay control a la hora de ingresar a internet.

Pregunta 12. ¿Existe alguna política para el uso del correo electrónico?

Figura 12 Pregunta 12



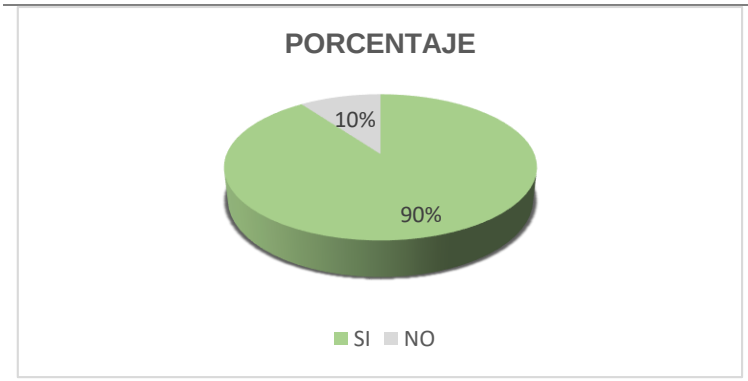
ITEM	ENCUESTADOS	PORCENTAJE
SI	5	50%
NO	5	50%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: la mitad de los encuestados manifiestan que si hay políticas para el uso del correo electrónico.

Pregunta 13. ¿Es conveniente que Asmet Salud invierta en la ejecución de un SGSI?

Figura 13 Pregunta 13



ITEM	ENCUESTADOS	PORCENTAJE
SI	9	90%
NO	1	10%
TOTAL	**10**	**100%**

Fuente: el autor

Interpretación: el 90% de los funcionarios encuestados manifiestan que es necesario que la empresa invierta en un SGSI.