DISEÑO DE POLÍTICAS DE ACUERDO AL ESTÁNDAR ISO 27001 DE SEGURIDAD DE LA INFORMACIÓN EN LA FUNDACIÓN INTERNACIONAL MARYOS

LORENA ASTRID CUERVO HUERTAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C, COLOMBIA
2020

DISEÑO DE POLÍTICAS DE ACUERDO AL ESTÁNDAR ISO 27001 DE SEGURIDAD DE LA INFORMACIÓN EN LA FUNDACIÓN INTERNACIONAL MARYOS

LORENA ASTRID CUERVO HUERTAS

PROYECTO DE GRADO

Asesor de proyecto:
Martin Cancelado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C, COLOMBIA
2020

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma Jurado

_____

Firma Jurado

Bogotá, 27 de mayo de 2020

DEDICATORIA

Dedico este trabajo a Dios por darme la sabiduría en la continuación de mis proyectos para salir cada día más adelante.

A mi Madre, Tía y Abuelos por inculcarme responsabilidad para superarme cada día y así mismo por ayudarme a cumplir mis sueños.

AGRADECIMIENTOS

Es trabajo fruto del esfuerzo dado por la Fundación Maryos con el apoyo de los doctores Marlen Huertas y Oscar Suarez que me ayudaron en el desarrollo del proyecto con su conocimiento.

Agradecimiento a los tutores y profesores que se esforzaron por detallarnos cada uno de los proyectos y por supuesto a la Universidad Nacional Abierta y Distancia por proporcionarme la oportunidad

CONTENIDO

Pág.

LISTADO DE TABLAS

Pág.

LISTADO DE ILUSTRACIONES

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

Con la evolución de la tecnología aumenta la necesidad de saber información de las diferentes empresas y compañías para poderla utilizar ya se en contra o venderla a los competidores. De acuerdo con lo anterior a la fundación maryos se dará una propuesta de diseño de políticas de seguridad de la información basadas en ISO 27001 el cual tendrá los procesos y controles de seguridad de cada una de las áreas con el fin de proteger la información contra personas externas e internas.
Para deducir lo anterior se tomó en cuenta la metodología margerit para identificar los activos y amenazas su respectiva probabilidad de daño.

Palabras claves: Seguridad de la información, ISO 27001, Margerit

ABSTRACT

With the evolution of technology, the need to know information from different companies and companies increases so that they can be used against themselves or sold to competitors. In accordance with the aforementioned, the Maryos Foundation will be given a proposal for the design of information security policies based on ISO 27001, which will have the security processes and controls of each of the areas in order to protect information against people. external and internal.

To deduce the above, the margerit methodology was taken into account to identify the assets and threats, their respective probability of damage.

Keywords: Information security, ISO 27001, Margerit

INTRODUCCIÓN

Actualmente las compañías suele manejar volúmenes de información por medio de correos electrónicos para realizar parte del proceso de comunicación interna y externa, lo cual hace que este flujo de datos sea sensible si llegase a estar en manos de personal ajeno a la empresa o en su defecto en quien no corresponde dentro de la misma, dejándose expuesta de manera pública por ende la convierte en importante para personas inescrupulosas que quieren hacerle daño a la misma, generando malestar en los procesos que se llevar a cabo en el día a día.

Es por este motivo que muchas empresas tienen como prioridad implementar políticas o técnicas de cifrado en su información general y más aún la transmitida por correo electrónico la cual comunica con el exterior de la empresa existiendo aquí el mayor riesgo de vulnerabilidad o sensibilidad en los datos intercambiados, en este contexto entra la aplicación fundamental del cifrado (utilización de llaves públicas o privadas, firmas digitales, apertura biométrica, entre otros) lo que puede garantizar que la comunicación se realice de manera satisfactoria y sin obstáculos entre el emisor y receptor de la misma, manteniendo la integridad de los datos que se quieren manejar.

Es importante que también se encuentren protegida las instalaciones de personas no autorizadas ya que se pueden llevar discos duros, cpu, usb con información de la Fundación Maryos.

En la parte de redes es recomendable tener firewall, a nivel de acceso a las diferentes aplicaciones se debe usar contraseña de 8 caracteres alfanuméricas y con un carácter especial en las redes y en los servidores utilizados.

Al realizar el diagnóstico de la Fundación Maryos se evidencio que carece de políticas de seguridad que proteja la información, por lo anterior se realizó un inventario de los activos tanto de software y hardware para analizar la evaluación de vulnerabilidades y amenazas con lo anterior se diseñaron políticas de seguridad donde se describen los procesos a llevar a cabo en las áreas de recursos humanos o administrativos, seguridad en el acceso a las instalaciones y software, la creación de usuarios con sus respectivos métodos de seguridad, a nivel de protección de la comunicación.

1. **OBJETIVOS**

1.2 OBJETIVO GENERAL

Diseñar políticas de protección de la información basándose en las normas ISO 27001:2013, manual de políticas y normas de seguridad de la información en la Fundación Maryos.

1.3 OBJETIVOS ESPECÍFICOS

1. Evaluar el estado la seguridad informática de la Fundación Maryos.
2. Diseñar políticas de seguridad informática de la Fundación Maryos.
3. Plantear manual de políticas de seguridad usando las normas ISO 27001 en la Fundación Maryos

2. PLANTEAMIENTO DEL PROBLEMA

La fundación Marys está en su inicio de creación con el objetivo de servir a la población más desfavorecida, como niños y ancianos ubicados en lugares apartados de la ciudad, que necesitan apoyo en el área de la salud y medidas de prevención que les permita mejorar estado de salud.

Existe una preocupación por la seguridad de la información en la Fundación Maryos, actualmente algunas fundaciones o empresas tienen pérdida significativa u uso indebido de la información y datos que les ocasiona mayores costos de recursos humanos y demoras en la atención al cliente externos e internos lo que repercute en el funcionamiento que desequilibran la estabilidad de la empresa y no proporciona un entorno seguro con los datos personales proporcionados.
La seguridad en la información es un proceso en el que se da cabida a un gran número de elementos como aspectos tecnológicos, recursos humanos, de gestión-organizacionales, económica, negocios, de tipo legal abarcando temas informáticos y de telecomunicaciones sino aspectos físicos, medioambientales, humanos

Dado lo anterior la Fundación Maryos debe manejar gran cantidad de información proveniente tanto de entidades y personas que apoyan la Fundación como el manejo de las bases de datos de las personas que requieren dicho apoyo, al igual debe llevar una contabilidad que le permita manejar su flujo de ingresos y gastos, para de esta manera proyectar los diferentes servicios la comunidad necesitada.
Teniendo en cuenta la razón social de la Fundación Maryos y sus objetivos, se hace necesario implementar un Sistema de Seguridad de la Información a niveles macro

y micro, utilizando la normatividad establecida en este campo, tales como las normas ISO 27001.

3. JUSTIFICACIÓN

Se evidencia que en la Fundación Maryos no tiene un control de políticas de seguridad de la información de acuerdo con lo informado por los fundadores ellos desean tener un diseño de políticas de calidad para implementarlo.

La seguridad en los sistemas de información es un tema de actualidad, por lo que en los últimos años se han realizado estudio de bases teóricas y el diseño e implementación de prácticas para tener mejor seguridad en la confidencialidad, integridad y disponibilidad de la Información.

La seguridad de los sistemas de información es indispensable para cualquier entidad o empresa, ya que se debe garantizar que la información esté Disponible en:buen estado y no estén alterados por factores externos, que genera pérdidas, y pongan en riesgo la viabilidad de la empresa. Las personas que trabajan en el mundo empresarial deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información en el complejo mundo de los negocios con el objetivo primordial de mantener sólido su futuro económico.

La Fundación Maryos es una entidad sin ánimo de lucro, en su inicio de creación tiene como propósito servir a la población más desfavorecida, como niños y ancianos ubicados (Garagoa, Chinavita, Chiquinquirá entre otros) en lugares apartados de la ciudad, que necesitan apoyo en el área de la salud y medidas de prevención que les permita mejorar sus condiciones y tener bienestar. Por esta razón la fundación debe manejar gran cantidad de información proveniente tanto de

entidades y personas que la apoyan como el manejo de las bases de datos de las personas que requieren dicho apoyo, por ser una entidad vigilada por el Estado debe llevar un control estricto de su contabilidad que le permita manejar su flujo de ingresos y gastos, para de esta manera proyectar los diferentes servicios la comunidad necesitada.

Es necesario implementar en la Fundación Maryos un Sistema de Seguridad de la Información a niveles macro y micro, utilizando la normatividad establecida en este campo, tales como las normas ISO 27001, así mismo crear un manual de políticas y normas de seguridad en donde se estructurará la seguridad organizacional, seguridad lógica, Seguridad física, seguridad legal.

Para lo anterior se realizará un inventario de los equipos que tiene la fundación, luego de lo anterior se realizara una evaluación de riegos para sí diseñar las políticas de seguridad para el mejoramiento de la seguridad de la fundación.

4. MARCO REFERENCIAL

4.1 MARCO CONTEXTUAL

El diseño del manual de políticas de calidad se realizará en la Fundación Maryos

4.1.1 Reseña histórica

La fundación maryos es una organización sin ánimos de lucro con el propósito de desarrollar actividades sociales y comunitarias principalmente relacionadas con el bienestar físico, intelectual y moral de la humanidad, así como para brindar apoyo a comunidades, organizaciones y grupos especiales necesidades sociales. La fundación maryos también ofrece actividades de capacitación e investigación en materia de salud.

Somos una fundación que desarrolla actividades sociales y comunitarias relacionadas con el bienestar de la humanidad, tanto físico, intelectual o moral, apoyo a comunidades, a colectividades, agrupaciones de personas vulnerables, realizamos actividades de capacitación, investigación a nivel nacional e internacional.

4.1.2 Valores institucionales

Misión

Somos una fundación que desarrolla actividades sociales y comunitarias relacionadas con el bienestar de la humanidad tanto físico, intelectual o moral, realizamos actividades de capacitación, investigación a nivel nacional e internacional

Visión

En 10 años ser reconocida a nivel nacional e internacional por sus actividades de bienestar a la comunidad e investigación.

4.1.3 Valores

Compromiso: comprometerse va más allá de cumplir una obligación, es poner en juego nuestras capacidades para sacar adelante todo aquello que se nos sea confiado.

- Responsabilidad: La responsabilidad es una obligación, ya sea moral o incluso legal de cumplir con lo que se ha comprometido.
- Humildad: Una personalidad sencilla a veces puede pasar inicialmente desapercibida, pero su fortaleza interior y su encanto es mucho más profundo y perdurable.
- Respeto: Hablar de respeto es hablar de los demás. Es establecer hasta donde llegan mis posibilidades de hacer o no hacer y donde comienzan las posibilidades de los demás. El respeto es la base de toda la convivencia en la sociedad.
- Aprender: El valor que nos ayuda a descubrir la importancia de adquirir conocimiento a través del estudio y la reflexión de las experiencias cotidianas.

- Honestidad: “Es una forma de vivir congruente entre lo que se piensa y la conducta que se observa hacia el prójimo, que junto a la justicia, exige en dar a cada quien lo que es debido” [1]

4.1.4 Organigrama fundación Maryos

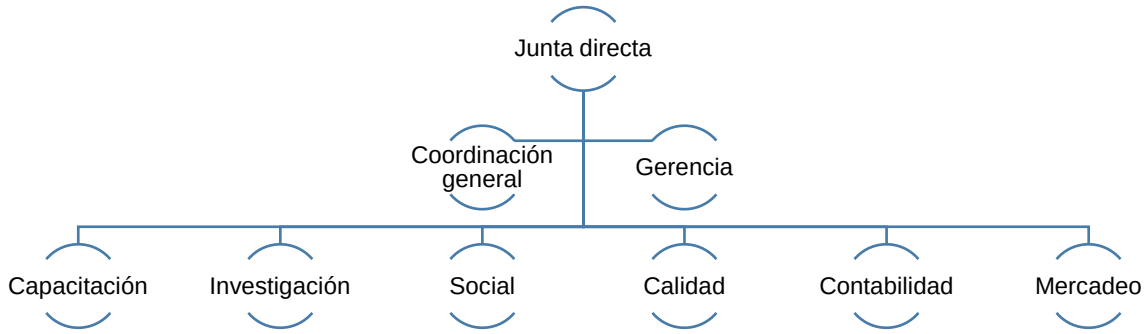

Ilustración 1 Organigrama Fundación Maryos

[1] Fundación Maryos,. [En línea]. *[Consultado* el 15 de septiembre de 2019] Nuestros Valores p. Disponible en internet: https://fundacionmaryos.org/valores/

4.1.5 Perfiles fundación Maryos

- Represéntate legal o general

  Oscar Suarez: Médico general, Especialista en gerencia y auditoria en salud, especialista en epidemiologia clínica, Especialista en anestesia y reanimación.

- Coordinación general:

  Marlen Huertas: Médico general, Especialista en gerencia y auditoria, especialista en epidemiologia general, Martes Internacional en geriatyria y envejecimiento.

- Revisor Fiscal

  Contador Público

- Contabilidad

  Contador publico

- Mercadeo

  Auxiliares de enfermería

- Investigación

  Epidemiólogos generales o clínicos

- Social

  Auxiliares de enfermerías, profesionales de cualquier área, estudiantes universitarios, personas de la comunidad, voluntarios

- Calidad

Auditores en salud, Ingenieros en sistemas, Ingenieros industriales

4.2 MARCO CONCEPTUAL

- **Confidencialidad:** Es la capacidad que se tiene para guardar o proteger la información con el fin de que las personas no autorizadas para el acceso la puedan utilizar de acuerdo con lo anterior se deben tener diferentes tipos de perfiles.
- **Integridad:** Se encarga que cada información tenga procesos como lo son modificación, creación y borrado el cual solo debe ser realizado por el personal autorizado, dando a entender que si no es un personal autorizado no puede realizar estos procesos.
- **Disponibilidad:** Consiste que tanto los activos o información esté disponible cuando sea necesaria o se vaya a usar por parte del hardware y el software para el usuario que la va a usar
- **Información:** Es la descripción de proceso que maneja un software o un hardware.
- **Activos:** Son todos los elementos de valor que sean importante para un elemento.
- **Amenazas:** Es una situación o proceso que puede dañar un activo.
- **Vulnerabilidad:** Es una debilidad de un sistema de información permitiendo que el intruso pueda afectar la disponibilidad, integridad y confidencialidad.

4.3 MARCO TEÓRICO

4.3.1 Seguridad de la información

Es una disciplina que se encarga que crea normas, métodos con el fin de obtener un sistema un sistema seguro y confiable para afrontar lo anterior se debe conocer los siguientes componentes:

- Elementos: son los que componen un sistema.
- Peligros: es todo lo que afecta el sistema
- Medidas: son los mecanismos de prevención.

Al juntar estos componentes son utilizados en el entorno de un sistema por lo cual se pueden evidenciar si se afectan o tienen fallos en los sistemas. Se debe tener en cuenta los sistemas operativos, la parte física y los fallos humanos.

Una política de seguridad son un conjunto de instrucciones que guían en los procesos, asimismo definiendo los criterios de seguridad para que sean implementados en las organizaciones o empresas con el fin de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico. [2]

[2] AGUILERA, Purificación, Seguridad informática. Editex, 2010

4.3.2 Tipos de seguridad

- Activa: se encarga de todas las prevenciones o defensas con el fin de reducir riesgos en los sistemas

- Pasiva: son todos los métodos que se establecen una vez ocurrido el ataque cibernético para así facilitar la recuperación del sistema.

4.3.3 Análisis de riesgos

Se encarga de encontrar los elementos de vulnerabilidad de un sistema determinando como una amenaza para el sistema, base de datos y sistemas operativos.

Principios

- Integridad: Se encarga de autenticación de la información al momento de ser solicitada por el personal autorizado por ende el sistema debe tener diseñado mecanismos que detecten si se produce un fallo.

- Confidencialidad: Toda información debe estar al alcance del personal o entidades autorizadas para prevenir se debe diseñar un control de acceso al sistema.

- Disponibilidad: la información de debe estar disponible a usuarios autorizados.[3]

[3] AGUILERA, Purificación, Seguridad informática. Editex, 2010

4.3.4 Elementos de estudio

Activos:
Son todos los componentes de un sistema y se clasifican de la siguiente manera:

- Datos: es toda la información almacenada en una base de datos
- Software: conjunto de aplicaciones instaladas en un equipo que se encargan de gestionar los distintos datos.
- Hardware: Se tratan de los equipos ya sean servidores, terminales y pc el cual se encarga del funcionamiento de las aplicaciones.
- Redes: Vía de comunicación y trasmisión de los datos ya sea metropolitanas o internet.
- Soportes: es donde la información queda almacenada.
- Instalaciones: son los lugares donde se guardan los equipos y sistemas de información
- Personal: son un conjunto de personas que se encargan de interactuar con un sistema.[4]

4.3.5 Amenazas

Es toda figura de distintos factores que quieren atacar un sistema de datos, redes o sistemas operativos.

Se clasifican de la siguiente manera:

- De interrupción: deshabilitar el acceso de la información.

[4] AGUILERA, Purificación, Seguridad informática. Editex, 2010

- De interceptación: son personas, programas y equipos no autorizados para no entrar al sistema.
- De modificación: son personas no autorizadas para modificar el sistema.[5]

Clasificación de amenazas

- Amenazas fundamentales: cual afecta directamente los principales básicos de la seguridad como lo son Integridad, disponibilidad, confidencialidad.

- Amenazas habilitadas de las primarias: son amenazas fundamentales como lo son: suplantación, virus entre otros.

- Amenazas subyacentes: son todas las amenazas que activan las amenazas fundamentales.

[5] ALEGRE, Maria, Seguridad informática ed.11 paraninfo. Editorial Paraninfo, 2011

4.3.6 ISO 27001:2013

Es un sistema de gestión de seguridad de la información la cual se basa la norma internacional que permiten a las organizaciones o empresas evalúen los riesgos, teniendo en cuenta los controles para mitigarlos teniendo procesos para mejorar el análisis de acuerdo con lo anterior se deben seguir los siguientes pasos[i6]:

[6] ISOTOOLS EXCELLENCE [En línea]. *[Consultado* el 04 de mayo de 2017], La norma ISO 27001. Disponible en https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

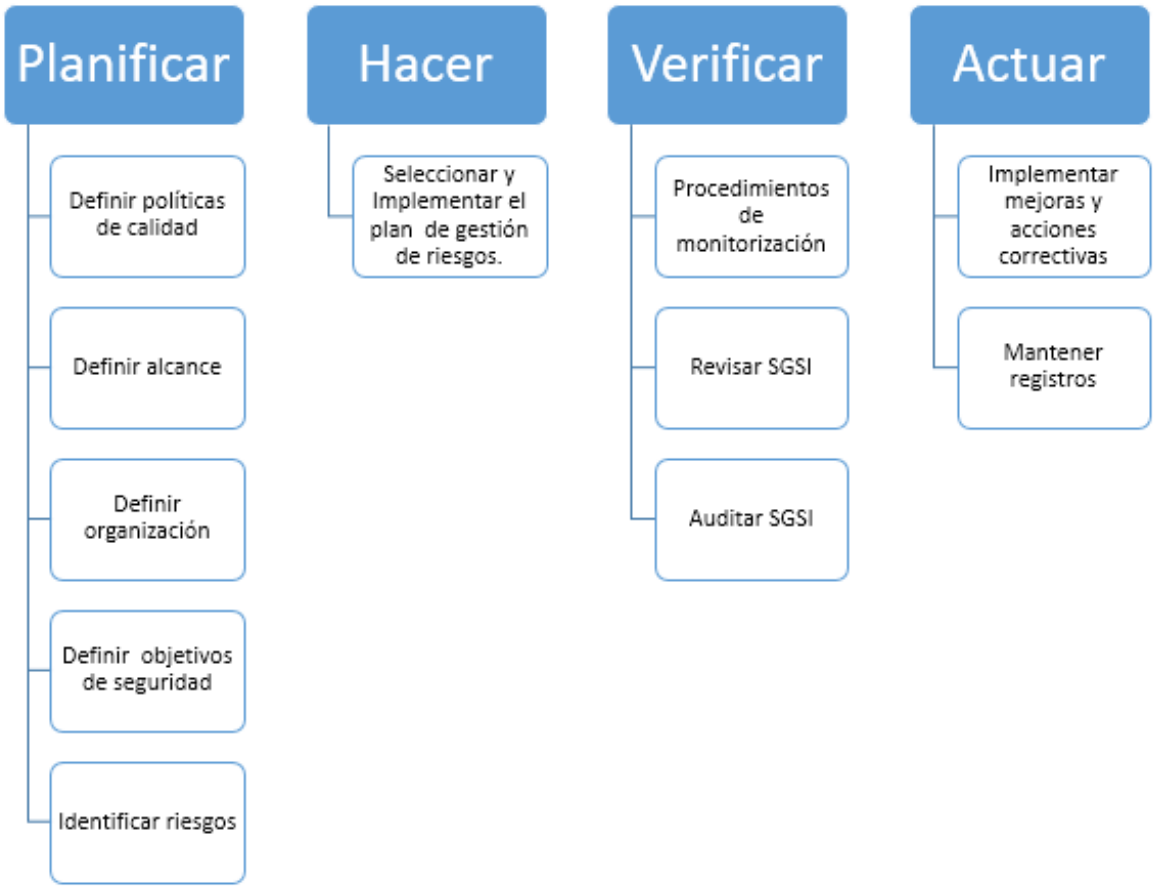

Ilustración 2 Pasos ISO 27001:2013

4.3.7 Margerit

Es una metodología de análisis y gestión de riesgos de los sistemas de información con el fin de minimizar los riesgos en las empresas públicas en las diferentes áreas. Para ello se deben seguir el siguiente método de análisis de riesgos se deben tener en cuenta los siguientes principios conocer e identificar los activos y su degradación con el tiempo, identificar las amenazas de los activos, identificar el daño de los diferentes activos.

En la descripción de un activo se debe tener en cuenta la información y el servicio que presta, entre los activos conocidos están los datos, servicios, aplicaciones informáticas, equipos informáticos, soporte, redes de comunicaciones, instalaciones y personas.

Los activos son dependientes de otros activos donde tienen las siguientes capas: activos esenciales que es la información, los servicios internos es la estructura de lo que compuesta el activo, el equipamiento informático aplicaciones o software utilizadas en dicho activo, el entorno se encarga de garantizar el equipamiento y mobiliario, servicios subcontratados por terceros, instalaciones físicas, el personal que son los usuarios, operadores, administradores, desarrolladores.[7]

Los activos se deben (Carvajal, 2014) (Geovanny, 2012) de la siguiente manera con la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad tanto de servicios y datos, en la seguridad se encuentra dividido coste reposición es todo lo relacionado con la instalación, costo de mano de obra, pérdida de ingresos, daños personales, activos pueden ser cuantitativos y cualitativos respectando lo siguiente homogeneidad y relatividad.

Para continuar con el análisis se deben identificar las amenazas que afectan a los diferentes activos, se tienen en cuenta origen natural como por ejemplo terremotos e inundaciones, del entorno se relaciona con la contaminación o fallos electrónicos,

defectos de aplicaciones, causadas por personas de forma accidental y deliberadamente. Las amenazas se determinan de degradación mide el daño causado y probabilidad las veces que se repite dicha amenaza. Para determinar el impacto potencial sobre el activo se debe conocer el valor y la degradación. Los impactos se dividen en impacto acumulado es el valor acumulado y las amenazas expuestas ya sean mayor o menor, otro de los impactos repercutido el cual se encarga de calcular el valor propio y las amenazas expuestas.[8]

Los riesgos se dividen en riesgos acumulados para cada activo por cada amenaza identificada y riesgo repercutido el cual se encarga de determinar las consecuencias.

Al continuar el análisis de riesgo es el de salvaguardar es tener todas las medidas necesarias para reducir los riesgos y protegerse de sí mismo, el cual se encarga de centrarse en el más valioso y se debe analizar los que no aplica los activos que no se deben proteger y los no se justifica, algunos de los efectos reducción de la probabilidad de la amenaza y limitando el daño causado. Entre los tipos de protección están la siguiente prevención (PR), disuasión (DR), eliminación (EL), minimización de impacto (IM), corrección (CR), recuperación (RC), monitorización (MN), detección (DC), concienciación (AW), y administración (AD).[9]

Para continuar con el análisis está el impacto residual que consiste en salvaguardar la madurez de los distintos procesos y el posible impacto el cual se denomina residual el cual se calcula sobre los activos inferiores o superiores

[8] AMUTIO, Miguel, [En línea]. *[Consultado* el 04 de mayo de 2017], MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 42 p. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

[9] AMUTIO, Miguel, [En línea]. *[Consultado* el 04 de mayo de 2017], MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 42 p. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

El siguiente paso a seguir es el riesgo residual en las cuales están las siguientes actividades levantar un modelo del valor del sistema, mapa de riesgos, conocimientos de la situación, evaluar el impacto posible y se deben caracterizar los activos identificándolos, dependencia, valoración de los activos, para ello hay que hacer las siguientes tareas caracterización de los activos, caracterización de las amenazas, caracterización de la salvaguardas, estimación de estado de los riesgos, caracterización de los activos, caracterización de las amenazas.[10]

Se deben tener en cuenta la documentación el cual se dividen en documentación intermedia que se encarga de las entrevistas, documentación auxiliar como lo son los planos e informes y evaluaciones. La documentación final modelo del valor, mapa de riesgos, declaración de aplicabilidad, evaluación de salvaguardas, los estados de los riesgos y para tener un mayor control debe tener en cuenta una lista.

Otro de los pasos del análisis es el proceso de gestión de riesgos la cual ayuda tomar decisiones de acuerdo con los siguientes factores gravedad del impacto, obligaciones de ley, reglamentos; otro es los conceptos el cual se encarga de determinar los impactos de los riesgos con los siguientes pasos la evaluación y tratamiento.

Para llevar un buen desarrollo del análisis los siguientes roles órganos de gobiernos quienes se encargan de la misión y los objetivos, dirección ejecutiva toman las decisiones para alcanzar los objetivos, dirección operacional son los responsables de lo operativo, para tener una mejor seguridad se asignaron los siguientes roles responsable de la información, responsable del servicio, responsable de la seguridad, responsable del sistema y administradores y operadores. Se debe realizar una matriz en donde se encontrará la asignación de tareas a los diferentes roles.

La documentación del proceso se encarga de la definición de los roles, criterios de valoración de la información y servicios, llevando un listo de control indicando e enumerado las actividades.

Para tener un mejor control en el análisis de riesgo se debe realizar un proyecto con los siguientes roles que son comité de seguimiento en donde su función resolver incidencias, asegura los recursos humanos, aprobar informes finales; equipo de proyecto su función son llevar a cabo las tareas relacionadas con el proyecto, recopilar, procesar y elaborar informes; grupos de interlocutores sus funciones son responsables del servicio y del personal. Para continuar con el alcance de proyecto se debe identificar activos esenciales, puntos de intercambios, proveedores externos. Para tener un mejor control debe crear un comité de seguimiento el cual aportara la documentación intermedia que consta de entrevistas y análisis de resultados y documentación final que consta de mapa de amenazas, informe de valoración e indicadores de impacto.[11]

Para continuar con el proceso se debe realizar un plan de seguridad que consta de los siguientes planes mejora de la seguridad, director de seguridad, estratégico de seguridad, adecuación, que le corresponde realizar las siguientes tareas identificación de proyectos de seguridad, planificación del proyecto, ejecución de plan para que funcione correctamente tiene una lista de actividades en donde consta la asignación de recursos, roles y responsabilidades, calendario de ejecución, indicadores del progreso.

Para realizar lo anterior se deben distinguir los diferentes activos. Los activos esenciales que se dividen en información y servicio los cuales constan de datos de interés vitales y para la administración pública. Los datos de carácter personal se denotan o se divulgan de acuerdo con la ley de cada país.

La arquitectura de un sistema consta de los datos que son los que ayudan a prestar un servicio que serán guardados en equipos en ficheros que serán utilizados para

la trasmisión; las claves criptográficas se encarga de proteger la información cifrando firmas digitales y claves; servicios es todo lo que satisface al usuario externos almacenando ficheros y servicios de directorio; aplicaciones informáticas son todas las actividades automatizadas para el desempeño transformando los datos para presentar un mejor servicio; equipamiento informático son todos los medios materiales, físicos para soportar los servicios, las redes de comunicación dedicado para prestar los servicios ya que son los medios de transportan los datos de un sitio a otro, soporte de información son dispositivos físicos, equipamiento auxiliar son todos los equipos para dar soporte, instalaciones es la infraestructura en donde se presta el servicio, el personal los que utilizan los sistemas de información. Donde cada parte está conformada por códigos los cuales contenían el paso a paso de la creación.

Las dimensiones de valoración son todos los atributos que hacen valioso un activo los cuales se utilizan para encontrar las consecuencias de las amenazas los activos, integridad de datos consiste que ningún activo ha sido modificado de no autorizada, confidencialidad de la información no se pone a disposición, ni se revela la información, autenticidad, trazabilidad.

Los criterios de valoración son todos los valores que se usan para todas las dimensiones para valorar criterios constan de listas de cada uno de los valores con distintos tamaños y divididos de acuerdo con el criterio. Se encuentran en escalas estándar donde esta una lista de información personal, obligaciones legales, seguridad, intereses económicos, interrupción de servicios, orden público, operaciones, administración y gestión, perdida y confianza, delitos e información clasificada.

Se encuentra las posibles amenazas como lo son desastres naturales, fuego que se activa en equipos informáticos, daños por agua, desastres naturales, desastres industriales, contaminación mecánica, contaminación electromagnética, averías de origen físico o lógico aplicaciones, corte del suministro eléctrico, condiciones inadecuadas de temperatura, fallos de servicios de comunicación, interrupción de los servicios, degradación de los soportes, emanación electromagnética.

Entre los errores y fallos no intencionados son todos los causados por las personas entre ellos se encuentran los errores de los usuarios, errores del administrador, errores de monitorización, errores de configuración, difusión de software dañino, errores de secuencia, destrucción de la información, fugas de la información, indisponibilidad del personal.

Ataques intencionados son causados por las personas que se combinan con los errores no intencionados entre estos ataque se encuentran manipulación de los registros de actividad, manipulación de la configuración, suplantación de identidad, abusos de privilegios, uso no previsto, software dañino, alteración de secuencias, acceso no autorizado, análisis de tráfico, repudio, interceptación de información en las redes de comunicación, divulgación de la información, manipulación de los equipos, robo, ataque destructivo, extorsión, ingeniera social, extorsión.[12]

Las salvaguardas los cuales le hacen el frente a las amenazas apareciendo tecnologías nuevas, evolucionan los posibles atacantes. La protección se divide en datos, claves criptográficas, servicios, aplicaciones, equipos, protección de las comunicaciones, protección de los puntos de interconexión, salvaguardas relativas al personal, continuidad de operaciones, externalización, adquisición y desarrollo.

Se encuentran distintas fichas en las que se busca información del nombre activo, porque, descripción, responsable.

Los análisis se pueden hacer mediante tablas para dar a conocer los elementos para analizar métodos para medir impacto de degradación desde muy bajo, bajo, medio, alto, muy alto. Otros de los medios son los grafico de radar representan las distintas variables como lo son los radios respectivos en donde el centro queda en valor cero.

[12] AMUTIO, Miguel, [En línea]. *[Consultado* el 04 de mayo de 2017], MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 42 p. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

4.4 MARCO LEGAL

- **Resolución 8430 de 1993 del Ministerio de Salud**: La cual se encarga de la protección de los datos a nivel de investigación humana en donde se empleará los registros basados en recolección y así mismo garantizando la confidencialidad de datos obtenidos.

- **Sistema de gestión ISO/IEC 27001 de Seguridad de la Información**: Proporciona un sistema que se encarga de identificar los riesgos y amenaza, confidencialidad, controles para la prevención de perdida de la información y mejora continua de lo implementado.

LEY 1273 DE 2009: Da a conocer las diferentes amenazas que se pueden evidenciar con respecto al daño o perdida de la información y su respectivo castigo.

4.5 **MARCO METODOLÓGICO**

4.5.1 Tipo de investigación

Investigación Aplicada

4.5.2 Metodología de investigación

Tipo de estudio**:** Para realizar el diseño de este trabajo de grado se utilizará la Descriptivo en la que corresponde al diagnóstico y diseño de las políticas de seguridad

Hipótesis: Es posible que con el manual de políticas de seguridad mejoren los procesos de seguridad.

Población en estudio: La población objeto de estudio corresponde a la Fundación Mayos entidad sin ánimo de lucro, ubicada en la ciudad de Bogotá D.C. con la que presta servicios a poblaciones de Boyacá.

4.5.3 Variables y su medición

- Variables: Las variables que se utilizaran en este estudio son nominales de infraestructura tecnológica, principios de seguridad como son confidencialidad, integridad, disponibilidad.

- Plan de recolección de datos

  - ✓ Se utilizará la información en físico y médicos magnéticos, sistemas de comunicación de la Fundación Mayos.
  - ✓ Recopilación documental

Plan de análisis

Los datos obtenidos se organizarán en tablas y gráficos e identificarán bajo los dominios de la Norma ISO/IEC 27001, elaboración de matriz de riesgos enfocad a la Norma ISO/IEC 27001, se realizará resultados de diagnóstico y plan de mejora.

3.2.8 Metodología de desarrollo

De acuerdo con los objetivo general y específicos los cuales se resolverán de la siguiente manera:

Objetivo 1

- Realizar investigación y de acuerdo con lo anterior definir las normas de seguridad de la información planteando un diseño

Objetivo 2

- Identificar las amenazas y vulnerabilidades que serán presentadas por medio de un cuadro
- Darles una valoración a las amenazas identificadas.
- Determinar impacto sobre los activos y riesgos de acuerdo con el análisis.
- Determinar causas que producen los riesgos.

Objetivo 3

- Definir los objetivos de políticas de calidad
- Elaborar políticas de Seguridad.

Objetivo 4

- Realizar un prototipo de un manual de políticas de seguridad información.

4.5.4 Recursos disponibles

Recursos humanos

- Representante Legal Fundación Maryos: Oscar Suarez

- Médico general especialista: Edith Marlen Huertas Martin
- Profesionales Fundación Maryos
- Voluntarios Fundación Maryos
- Profesional responsable del proyecto UNAD

5. MÉTODO DE ANÁLISIS DE RIESGOS

Según el descrito en la norma ISO 27001 en cual se debe utilizar Planear, hacer, verificar, actuar

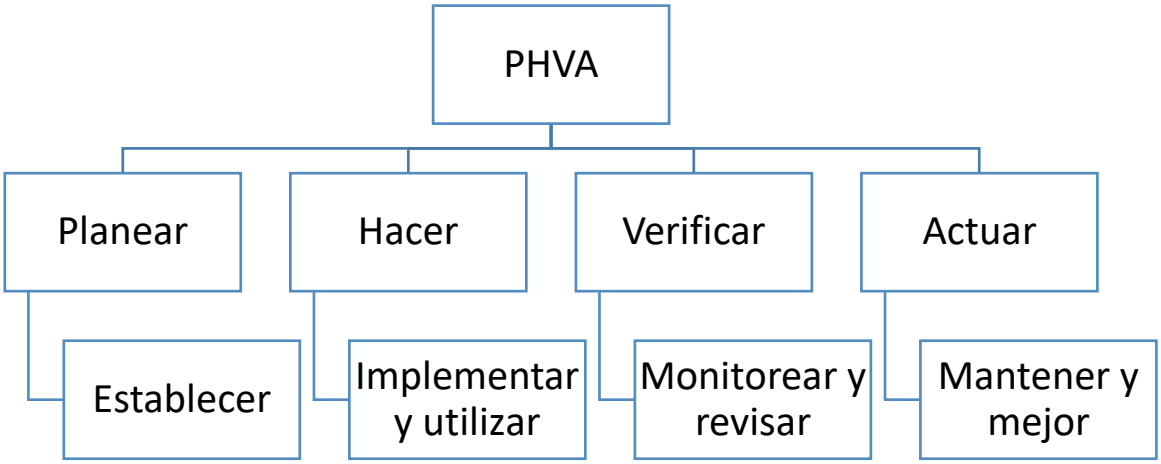

Ilustración 3 Análisis de riesgos

6. ALCANCE DEL SGSI

La fundación Maryos define el alcance para el área de tecnología inicialmente en procesos de la seguridad de la información para tener protegida información de la fundación teniendo en cuenta los usuarios que utilizan la información.

- Conocer los procesos y documentación utilizados para realizar el proceso en la Fundación Maryos por los colaboradores.
- Dar conocer las situaciones en los que se presentan los riesgos en la fundación
- La presentación de las actividades del resultado del diseño para mejorar los procedimientos
- Acompañamiento en proceso de diseño de las políticas y normatividad de seguridad de información
- Consolidación de la información

6.1 Diseño de políticas de seguridad

Definiciones

- Acuerdo de confidencialidad: Es el documento donde una persona externa manifiesta mantener confidencialidad de la información comprometiéndose a no dar a conocer la labor que se desarrolla de dentro de la fundación
- Análisis de riesgos: se encarga de identificar las variables de acuerdo a los criterios de evaluación para determinar la confidencialidad, integridad y disponibilidad de la información.
- Autenticación: Es el recurso que se encarga de comprobar la entidad para ingresar a un sistema.
- Centro de cableado: es el área donde se deben instalar los dispositivos que contenga los cables como por ejemplo materiales, paredes, piso, techos y provisión de alimentación eléctrica.
- Centro de cómputo: es la zona donde se almacena múltiples computadores la cuales se encuentran conectadas mediante un diagrama de red. El centro de cómputo debe cumplir estándares que ayudaran a los controles de acceso físico, paredes, pisos y techos.
- Derechos de autor: conjunto de normas y principios que regulan los derechos de la creación de una obra
- Disponibilidad: Es la garantía que tiene un usuario para el acceso a la información
- Integridad: es el estado completo de los activos.
- Perfiles del usuario: son grupos de usuarios que con permisos similares de necesidades de la información los cuales dan acceso a las diferentes aplicaciones
- Recursos tecnológicos: son los compuestos por un hardware y software por ejemplo como lo son servidores, equipos portátiles, dispositivos de comunicación

- SGSI: Sistema de Gestión de Seguridad de la Información
- Auditoria: encargada de verificar los procedimientos que se manejen en la fundación Maryos

7. IMPLEMENTACIÓN DE METODOLOGIA MARGERIT

Para realizar el análisis de los riesgos se tomaron en cuenta los procedimientos de la metodología margerit

7.1 Identificación de activos

De acuerdo con la información obtenida por la fundación Maryos se detallaron los siguientes activos:

Tipos de activos

Tabla 1 Tipos de activos

TIPO DE ACTIVO	DESCRIPCIÓN
Datos	Copias de respaldo, registro de actividad, información sobre programas de capacitación.
Servicios	Función que satisface una necesidad de los usuarios.
Hardware	Computadores, portátiles
Redes de comunicaciones	Routers
Instalaciones	Casa

Personal	Personal relacionado con los sistemas de información.
Sotfware	Conjunto de aplicaciones

Fuente: El autor

La fundación Maryos tienen en su inventario de activos informáticos los cuales se describen a continuación:

Tabla 2 Inventarios de activos Fundación Maryos

TIPO DE ACTIVO	ACTIVO	SERVICIO	SISTEMA OPERATIVO	CANTIDAD
Tangible	Modem	Provee el servicio de internet con		1
Tangible	Computadores de escritorio HP		Windows 8 de 64 bits	1
Tangible	Portátil		Windows 8 de 64 bits	1
Tangible	Impresora con scaner	Conectada al equipo principal		1
Tangible	Teléfonos IP	Comunicación con el exterior y receptor		1

Tangible	Celulares	Comunicación con el exterior y receptor	Android	3
Intangible	Servicio de internet	Navegación en internet UNE		1
Intangible	Servicio web	Sistema de información que muestra los servicios que presta la información	Pagina Publica	1

Fuente: El autor

Para continuar con el proceso de metodología Margerit se va utilizar como parte del proceso Libro II: Catálogo de Elementos del proceso para facilitar el proceso

Tabla 3 Activos

TIPO	NOMBRE DEL ACTIVO
SERVICIOS	1.[INTERNET] Conexión internet
	2.[TELEFONIA]
APLICACIONES	3.[SISTEMA OPERATIVO] Windows 8
	4.[OFICCE] oficce 2010
EQUIPO INFORMATICO	5.[PC] Un computador HP
	6.[PORTATIL]
	7.[IMPRESORA Y ESCANER] Conexión con cable
	8.[MODEM] acceso a internet de UNE

REDES DE COMUNICACIONES	9.[ADSL] Conexión para internet
	10.[WIFI] Conexión inalámbrica
INSTALACIONES	11.[OFICIANA] Fundación Maryos
PERSONAL	12.[MEDICOS] Creadores de la Fundación Maryos
	13.[SECRETARIA] Auxiliar para campañas de salud.

Fuente: El autor

7.2 valoración de activos

Para realizar este proceso se continuará tomando como guía Libro II: Catálogo de Elementos del proceso en el cual se tomaran en cuenta la disponibilidad, Integridad, Confidencialidad, Autenticidad para lo anterior se realizara una valorización

Convenciones

Tabla 4 Dimensiones

Dimensiones	
D	Disponibilidad
I	Integridad de datos
C	Confidencialidad de la salud
A	Autenticidad
T	Trazabilidad

Fuente: El autor

Tabla 5 Valoración según Margerit

VALOR		CRITERIO
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: El autor

Tabla 6 Dimensionamiento de activos

ACTIVOS	**DIMENSIONAMIENTO**				
SERVICIOS	**D**	**I**	**C**	**A**	**T**
1.[INTERNET] Conexión internet	7	7	7	7	7
2.[TELEFONIA]	5	5	5	5	5
APLICACIONES	**D**	**I**	**C**	**A**	**T**
3.[SISTEMA OPERATIVO] Windows 8	8		8	8	8
4.[OFICCE] oficce 2010	6	1			
EQUIPO INFORMATICO	**D**	**I**	**C**	**A**	**T**
5.[PC] Un computador HP	7	7	7		
6.[PORTATIL]	7				
7.[IMPRESORA Y ESCANER] Conexión con cable	5				
8.[MODEM] acceso a internet de UNE	9				
REDES DE COMUNICACIONES	**D**	**I**	**C**	**A**	**T**

9.[ADSL] Conexión para internet	2				
10.[WIFI] Conexión inalámbrica	2				
INSTALACIONES	**D**	**I**	**C**	**A**	**T**
11.[OFICIANA] Fundación Maryos	9				
PERSONAL	**D**	**I**	**C**	**A**	**T**
12.[MEDICOS] Creadores de la Fundación Maryos	10	10	10	10	10
13.[SECRETARIA] Auxiliar para campañas de salud.	7	5	7	5	

Fuente: El autor

7.3 Amenazas

De acuerdo con la metodología de Margerit el cual se demuestra que cada impacto determinado con cada una de las amenazas. Teniendo el conocimiento del valor de cada activo.

Tabla 7 Convenciones de amenazas

CODIGO	CONFIDENCIALIDAD	DESCRIPCION
C	Confidencial	Restringidas personas sin autorización
I	Uso Interno	Personal con acceso medio
P	Uso Público	Información dispuesta al público en general

CODIGO	INTEGRIDAD	DESCRIPCION		
N	Normal	Controles habituales para su protección		
B	Baja	Información que requiere controles mínimos para su protección		
CODIGO	DISPONIBILIDAD	DESCRIPCION		
MA	Muy Alta	Tiempo tolerable de interrupción menor a 3 horas	100%	
A	Alta	Tiempo tolerable mayor a 3 horas y menor a 5 horas	80%	
M	Media	Tiempo tolerable mayor a 5 horas y menor a 1 día	60%	
MB	Media Baja	Tiempo tolerable mayor a 2 día y menor a 3 días	40%	
B	Baja	Tiempo tolerable mayor a 4 días y menor a 6días	20%	

Tabla 8 Clasificación de amenazas

TIPO DE ACTIVO	VALOR DEL ACTIVO	CLASIFICACIÓN DE LA INFORMACIÓN	IMPACTO
Datos	MA	Nivel Confidencialidad: Confidencial Nivel Integridad: Normal Nivel Disponibilidad: Muy Alta	
Servicios	M	Nivel Confidencialidad: Uso público Nivel Integridad: Normal Nivel Disponibilidad: Muy Alta	
Hardware	M	Nivel Confidencialidad: Uso interno Nivel Integridad: Normal Nivel Disponibilidad: Muy Alta	
Redes de comunicaciones	M	Nivel Confidencialidad: Uso interno Nivel Integridad:	

		Normal Nivel Disponibilidad: Muy Alta	
Instalaciones	A	Nivel Confidencialidad: Uso publico Nivel Integridad: Normal Nivel Disponibilidad: Muy Alta	
Personal	A	Nivel Confidencialidad: Uso interno Nivel Integridad: Normal Nivel Disponibilidad: Muy Alta	
Sotfware	MA	Nivel Confidencialidad: Confidencialidad Nivel Integridad: Normal Nivel Disponibilidad: Muy Alta	

Fuente: Autor

Identificación de amenazas y vulnerabilidades

- La información de las diferentes actividades no se encuentra digitalizada la cual almacena en carpetas.
- No existe un formato donde se registre histórico de las actividades o formatos de la fundación Maryos
- No existe Back up de la información.
- No existe claves asignadas a los diferentes usuarios.
- En los contratos de los colaboradores no existe cláusulas de confidencialidad.
- No existe manual de procedimientos de seguridad de la información.

Tabla 9 Amenazas y vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Información	- Códigos maliciosos (virus informáticos). - Incumplimientos de las políticas de calidad. - Ataques Maliciosos. - Acceso no autorizado a las instalaciones y la sala de cómputo. - Hurto.	- Ingreso no controlado a la información de las aplicaciones o web. - Desinformación las políticas de seguridad de la información. - Documentación insuficiente. - Ausencia de copias de la información. - La descarga de software no autorizado.

		- El no monitoreo de los recursos la información usada.
Software	- Códigos maliciosos (virus informáticos). - Mal funcionamiento de software. - Usa de software sin ninguna licencia.	- Requerimientos inadecuados. - Ausencia de controles el software usado. - Fallas en los equipos. - La comunicación no es encriptado. - Ausencia de autenticación en las diferentes aplicaciones. - No hay copias de respaldo.
Hardware	- Mal funcionamiento del hardware. - Perdida de equipos.	- Requerimientos incompletos. - El no control de los activos dentro y fuera de las instalaciones. - Falta de mantenimientos de los equipos. - La no documentación de los equipos - Falta de autenticación
Soportes de la información	- Acceso forzado a la información.	- La no documentación de uso y administración. - Falta de autenticación

	- Robo de la información. - Dar a conocer información no autorizada. - El no cumplimiento de las políticas de seguridad. - Daño accidental por medio de incendios, agua, contaminación química, entre otros.	- El no control de los activos dentro y fuera de las instalaciones.
Redes de telecomunicaciones	- Mal funcionamiento. - Avería de origen o lógico. - Falla de los sistemas de comunicación (internet).	- Falta de mantenimiento d de los equipos. - La no documentación de uso y administración.
Personas	- Intrusos externos - Empleados - Contratistas. - Manipulación del sistema. - Espionaje. - Abusos de derechos - Hurto.	- Acceso no controlado a la información. - El no monitoreo a la actividad de los empleados o colaboradores. - El no tener acuerdos de confidencialidad - El no conocimiento de las políticas de información.

	- Error del uso del equipo.	- Desconocimiento de las normas legales. - El no cumplimiento de las políticas de procedimientos internos. - Falta de capacitación sobre seguridad de la información
Infraestructura	- Desastres naturales - Daño accidental - Fuego	- Acceso no controlado a la información. - El no control de los activos dentro y fuera de las instalaciones. - Ausencias de planes de emergencia y simulacros - Falta de servicios como los son internet, teléfono entre otro. - El no mantenimiento preventivo o correctivo

Fuente: Autor

7.3 Análisis y valoración de riesgos

De acuerdo con la metodología Margerit lo cual se les da un criterio valoraciones

Tabla 10 Valoración de las amenazas

VALORACIÓN DE LAS AMENZAS				
VALOR	NIVELES	OCURRENCIA	PROBABILIDAD	IMPACTO
MA	Muy Alto	A diario	100%	
A	Alto	Mensualmente	80%	
M	Medio	Una vez al año	60%	
B	Bajo	Poco frecuente	40%	
MB	Muy bajo	Muy poco frecuente	20%	

Fuente: Autor

De acuerdo con la anterior información se realizará la siguiente matriz:

Tabla 11 Matriz de amenazas

ACTIVOS	AMENAZAS	VALORACIÓN	RIESGO
	Códigos maliciosos (virus informáticos).	M	
	Incumplimientos de las políticas de calidad.	B	
	Ataques Maliciosos.	B	

Información	Acceso no autorizado a las instalaciones y la sala de cómputo.	M	
	Hurto	M	
Software	Códigos maliciosos (virus informáticos).	MA	
	Mal funcionamiento de software.	A	
	Usa de software sin ninguna licencia.	A	
Hardware	Mal funcionamiento del hardware.	M	
	Perdida de equipos.	M	
Soportes de la información	Acceso forzado a la información.	B	
	Robo de la información.	A	
	Dar a conocer información no autorizada.	M	
	El no cumplimiento de las políticas de seguridad.	M	

	Daño accidental por medio de incendios, agua, contaminación química, entre otros.	A	
Redes de telecomunicaciones	Mal funcionamiento.	M	
	Avería de origen o lógico.	M	
	Falla de los sistemas de comunicación (internet).	M	
Personas	Intrusos externos	B	
	Empleados	MB	
	Contratistas.	MB	
	Manipulación del sistema.	M	
	Espionaje.	MA	
	Abusos de derechos	MB	
	Hurto.	MB	
	Error del uso del equipo.	MB	
Infraestructura	Desastres naturales	B	
	Daño accidental	B	
	Fuego	B	

Fuente: Autor

8. DISEÑO DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

8.1 Políticas de seguridad recursos humanos

- Objetivos
  - ✓ Reducir la probabilidad de riesgos dados por error humano con el uso no apropiado con los activos informáticos y equipos.
  - ✓ Mantener informado a los empleados con respecto a todo el proceso de seguridad de la información.
  - ✓ Garantizar que los empleados tengan información con respecto a los riesgos y así mismo estar capacitados sobre las políticas de seguridad,

- Responsabilidades

  - ✓ El área de dirección se encargará de demostrar su compromiso con la seguridad de la información de acuerdo con los lineamientos de la fundación.
  - ✓ El área de talento humano debe realizar la verificación del personal que ingresa a la fundación Maryos.
  - ✓ El área de talento humano se debe encargar de que el personal firme cláusulas de confidencialidad y documentos las políticas de la seguridad de la información de los deben archivados de acuerdo con el cargo que ocupa.
  - ✓ El área de riesgos se debe encargar de diseñar y ejecutar una capacitación sobre la seguridad de la información para que el personal sobre el uso de la protección de la información.

- ✓ Los personales de la fundación deben dar cumplimiento a las políticas y normas de seguridad informática y asistir a las capacitaciones.

- Administradores

  - ✓ Establecer roles y responsabilidades a nivel directivo y operativo relacionados con la seguridad de la información.
  - ✓ Proponer actividades y capacitaciones de acuerdo con la seguridad de la información.
  - ✓ Facilitar el entendimiento de las políticas de seguridad a todos los funcionarios de la fundación.

- Administradores y soporte

  - ✓ El personal encargado deberá asignar los recursos de acuerdo de infraestructura física y personal provisto gestionar seguridad.

- Comité seguridad

  - ✓ El comité de seguridad deberá actualizar las políticas de seguridad cada vez que surja un cambio en el análisis de riesgos y en la clasificación de la información y presentarlo a la junta directiva para su aprobación.
  - ✓ El comité de seguridad de interpretar los incidentes presentados de acuerdo con la seguridad de la información y así mismo escalarlo con las autoridades pertinentes
  - ✓ El comité de seguridad es el encargado de supervisar el cumplimiento de las políticas de seguridad

- Encargado de los riesgos

    - ✓ Se encargará de dar lineamiento para gestionar la seguridad de la información y definirá el establecimiento de controles técnicos, físicos y administrativos.
    - ✓ Monitoreara de manera periódica el cumplimiento de las políticas de seguridad.

- Todos los usuarios

    - ✓ Tienen la responsabilidad de cumplir las políticas, normas, procedimientos relacionados a la seguridad informática.

De acuerdo con los anteriores roles o participantes deberán revisar y actualizar las políticas de acuerdo con los cambios que ocurran.

8.2 Políticas de seguridad control de acceso

- Objetivo

    - ✓ Garantizar el acceso seguro a la información de en los diferentes aplicativos que maneja la Fundación Maryos

- Gestión de contraseñas

    - ✓ Para obtener una mayor seguridad en los diferentes equipos y aplicaciones por los cuales cada usuario de debe tener una contraseña la cual estará asociada al usuario de red y ir, que le permitirá el acceso al equipo, acceso al correo electrónico y a las diferentes aplicaciones.

- ✓ Para obtener autorización de la creación, eliminación y modificación debe tener un formulario en el cual debe ir la firma del jefe inmediato.
- ✓ El usuario debe tener un perfil de acuerdo con el cargo al cual está ingresado debe estar en una lista de usuarios con los respectivos permisos y la persona que lo autoriza.
- ✓ El área encargada de recibir el formato de autorización y para la creación de los usuarios es el área de tecnología.
- ✓ Cuando un usuario ya no está trabajando en la fundación el jefe inmediato debe enviar un formato de retiro del usuario al área encargada

- Uso de contraseñas

- ✓ La contraseña establecida debe cumplir con los siguientes parámetros:
  - Debe contener nueve caracteres alfanuméricos
  - Debe iniciar con una letra mayúscula y continuar con las tres letras siguientes.
  - Debe contener cuatro números.
  - Debe contener un carácter especial.
- ✓ Las contraseñas deben ser cambiadas cada tres meses en las diferentes aplicaciones y usuarios de red.

8.3 Políticas de seguridad de usuarios

- Objetivo

- ✓ Asegurar el adecuado uso de los usuarios de acuerdo con los privilegios en las diferentes aplicaciones.

- Creación de usuarios

  Para realizar la creación de una cuenta de usuario de acuerdo con lo siguiente:

  - ✓ Autenticación de la identidad del usuario que se conecta en la red.
  - ✓ Controlar el acceso a la red y aplicaciones que se usan.
  - ✓ Realizar seguimiento al uso de la cuenta.
  - ✓ Tener una lista de usuarios de acuerdo los diferentes privilegios
  - ✓ Debe existir un súper usuario administrador con el cual se pueda hacer la creación, modificación y eliminación de los usuarios.
  - ✓ Debe tener una plataforma tecnológica en la cual se puedan realizar las diferentes actividades.

Los cuales deben tener los siguientes tipos de usuarios:

- ✓ Súper usuario: deben estar creados por defecto de acuerdo con el aplicativo que se está instalando de acuerdo con las políticas de seguridad los cuales deben ser usados en situaciones de emergencia el cual debe ser autorizada.
- ✓ Usuarios administradores: debe ser usado por el encargado de seguridad para asimismo administrar las aplicaciones el cual se encarga de monitorear el área de sistemas.
- ✓ Usuarios avanzados: son los usuarios que requieren acceso a los usuarios privilegiados, los cuales pueden tener permisos de modificación en ninguno de los aplicativos
- ✓ Usuarios finales: su principal función es realizar consultas para las aplicaciones.

8.4 Políticas de seguridad comunicaciones

- Objetivo

  - ✓ Garantizar que los diferentes medios de comunicación sean seguros y apropiados para la protección de la Fundación Maryos

- Protección contra el software malicioso

  - ✓ Los sistemas de información deben estar protegidos con freeware o antivirus para evitar el ingreso de virus que tomen el control o infecten e información no deseada en los diferentes medios comunicación como lo son el correo electrónico, USB, discos externos.
  - ✓ Verificar que constantemente se actualice automáticamente freeware o antivirus.
  - ✓ Mantener actualizada las bases de datos con las diferentes alertas de seguridad

- Copias de seguridad

  - ✓ La información o data utilizada debe constar con una copia de respaldo la cual debe ser guardada en la ruta apropiada para esta información.
  - ✓ Cuando empleado renuncie o sea despedido debe quedar una copia de su disco duro en la ruta acordada.

- Instalación de software

  - ✓ Las instalaciones de software que se realicen deben estar aprobadas por el área de seguridad.

- ✓ Debe tener un inventario del software autorizados para el uso e instalación de los mismos.
- ✓ No se permite la instalación software que viole las leyes de propiedad intelectual.

8.5 Políticas de seguridad móvil

- Objetivo

  - ✓ Controlar el ingreso al sistema o aplicaciones para evitar perdida de la información

- Equipo móvil

  - ✓ Para la conexión de un equipo móvil el empleado debe constar con un usuario de red y una contraseña asignada.

- Auditoria

  - ✓ Los diferentes sistemas o recursos deben estar en seguimiento y auditados

- Acceso remoto

  - ✓ Para la conexión remota el empleado debe constar con un usuario de red y una contraseña asignada y autorización por escrito.

8.6 Políticas de seguridad base de datos

- Objetivo

  - ✓ Garantizar de los derechos de habeas Data con el fin de tener mejor privacidad, el buen nombre, legalidad quien esté utilizando tanto interna como externamente

- Definiciones

  - ✓ Autorización: Consentimiento previo.
  - ✓ Base de datos: conjunto de información o datos personales utilizados para una actividad determinada.
  - ✓ Dato personal: información asociada a varias personas.

- Principios específicos

  - ✓ Principio de legalidad: Uso, captura y tratamiento de datos personales cuando se encuentren en estado vigente.
  - ✓ Principio de libertad: toda información o utilización de datos se debe tener en cuenta el consentimiento y autorización de quien corresponda dicha información.
  - ✓ Principio de transparencia: la utilización de la información, datas personales sin restricción alguna.
  - ✓ Principio de acceso: sin autorización previa no se puede divulgar por ningún medio de comunicación.
  - ✓ Principios de seguridad: Los datos e información será protegida mediante recursos técnicos como lo son protocolos de seguridad asimismo evitando la modificación, pérdida y consulta.

- ✓ Principio de confidencialidad: el personal que tenga acceso a la información deberá comprometerse a conservar, mantener y a no divulgar dicha información.

- Tratamientos de datos

  - ✓ Es necesario para salvaguardar la información ya sea del titular, física o jurídica para ello los representantes legales deberán otorgar una autorización.
  - ✓ Por parte de la Fundación Maryos la cual es un organismo si ánimo de lucro con el fin de proporcionar seguridad de protección de información tantos a los colaboradores y a los que se les proporciona ayuda.
  - ✓ Se usará con fines estadísticos y científicos en donde los datos utilizados se debe suprimir la identidad de los titulares.

- Autorización del titular

  Para la utilización de los datos e información se debe tener autorización previa para cualquier medio de consulta.

  - ✓ La autorización no será necesaria cuando:
    - Datos de naturaleza pública.
    - Temas de urgencia médica o sanitaria.
    - Información relacionada con el registro civil de las personas.

  - ✓ Deberes de los responsables de la data o información:
    - Garantizar el derecho habeas data
    - Realizar copias con previa autorización de los titulares
    - Informar al titular el uso de los datos.

- Exigir al que realice el tratamiento de datos

✓ Base de datos FUNDACIONMARYOS

- Colaboradores.
- Pacientes.
- Donaciones.
- Proveedores.
- Cursos

- Finalidad

✓ La base de datos tiene como finalidad usar los datos para prestar un mejor servicio y tener mayor conocimiento de los pacientes y cursos dados la cual debe estar actualizada para así mismo tener mejores procesos.

✓ La base de datos FUNDACIONMARYOS es un conjunto de información que compete a los pacientes atendidos, las personas colaboradoras (médicos, odontólogos, cirujanos, psicólogos entre otros), también se deben tener en cuenta los cursos de salud que proporcionar un mejor servicio.

8.7 Políticas de seguridad correo electrónico

- Objetivo

✓ Mejorar la seguridad tanto del emisor y receptor de mensajes e información enviada o recibida por medio de correo electrónico.

- Principios específicos

- ✓ El personal que utiliza el correo electrónico no debe dar a conocer la clave o contraseña las claves las cuales son de uso personal e intransferible, terceras sin previa autorización del área de tecnología
- ✓ Las contraseñas utilizadas deben contener una letra, números y caracteres especiales.
- ✓ Al realizar a la autenticación se debe especificar el rol asignado.
- ✓ El cambio de clave se debe hacer cada 3 meses.

8.8 Políticas de seguridad equipos

- Objetivo

  - ✓ Mejorar la seguridad de los equipos físicos y el uso de los mismos.

- Principios específicos

  - ✓ Los equipos donde se guarda y almacena la cual debe monitorearse el funcionamiento, por el cual se puedan realizar mantenimientos preventivos y correctivos.
  - ✓ Cuando el empleado haya sido retirado de la fundación Maryos se realizará el procedimiento de borrado o eliminación segura.
  - ✓ Se restringe las copias de archivos por medios removibles mediante dispositivos USB y unidades ópticas de grabación.

8.9 Políticas de seguridad claves de acceso

- Objetivo

  - ✓ Mejorar el uso de contraseñas para los diferentes accesos

- Principios específicos

  - ✓ Las claves o contraseñas deben contener mínimo 6 caracteres alfanuméricos.
  - ✓ Cada contraseña o clave utilizada deben ser diferentes a las utilizadas anteriormente.
  - ✓ La contraseña debe cumplir los requisitos como los son: caracteres mayúsculos, minúsculas las cuales debe ser 6 dígitos y alfanuméricos.

8.10 Políticas de seguridad de centro de datos y cableado

- Objetivo

  - ✓ Garantizar seguridad y protección de los centros datos y cableado.

- Principios específicos

  - ✓ Prohibido Fumar en el centro datos y cableado.
  - ✓ Prohibido Introducir alimentos o bebidas.
  - ✓ Prohibido el porte de armas de fuego, corto punzantes o similares.
  - ✓ Prohibido Mover, desconectar equipo de cómputo sin autorización previa.
  - ✓ Prohibido Modificar la configuración del equipo sin autorización previa.
  - ✓ Prohibido Afectar software instalado en los equipos sin autorización

8.11 Políticas de seguridad de respaldo de información

- Objetivo

  - ✓ Garantizar medios de respaldo asegurar la información del sistema después de una falla.

- Principios específicos

  - ✓ Al realizar una restauración o copia de respaldo debe estar autorizada previamente.
  - ✓ Semanalmente o mensual los administradores de plataformas deberán realizar un Backus.
  - ✓ Los administradores de las plataformas deberán verificar la correcta ejecución de los procesos.
  - ✓ Cuando al cumplir el periodo de guardado se deberá utilizar el procedimiento de eliminado o borrado.

8.12 Políticas de seguridad de redes sociales

- Objetivo

  - ✓ Garantizar la protección de usuarios de redes sociales y la mensajería instantánea

- Principios específicos

- ✓ Usuarios creados en las redes sociales creados con el usuario de Fundación Maryos como lo son twittee, Facebook, YouTube LinkedIn, blogs, instagram entre otros. Por ende, el personal encargado de la utilización deberá garantizar la fiabilidad y confiabilidad.
- ✓ La información compartida por redes sociales deberá ser autorizada por los jefes inmediatos.
- ✓ No se deberá utilizar el nombre o usuario de la fundación Maryos para difamar o afectar la imagen al responder comentarios en contra de la filosofía o pensamiento de la institución.

8.13 Políticas de seguridad de redes

- Objetivo

  - ✓ Garantizar la protección de los sistemas de amenazas externas e internas

- Principios específicos

  - ✓ Al crear un nuevo usuario tanto en el aplicativo o sistema se debe hacer firmar un documento que conste que conoce las políticas y procedimientos de seguridad.
  - ✓ No se debe dar usuarios o cuentas a personas que no trabajan en la Fundación Maryos.
  - ✓ No se deben compartir las contraseñas.
  - ✓ Cuando se genera un nuevo usuario, la contraseña solo debe ser válida hasta la primera sesión.
  - ✓ Las contraseñas predeterminadas que vienen en los routers y switchs sean cambiarse inmediatamente.

- ✓ Para realizar acceso remoto se debe contar con autorización del jefe inmediato.
- ✓ Las contraseñas deben tener 8 caracteres alfanuméricos.
- ✓ Se debe contar con antivirus actualizados y firewall el cual nos va a permitir mayor protección.

CONCLUSIONES

De acuerdo al análisis realizado a los diferentes activos de información en la Fundación Maryos se evidenciaron vulnerabilidades y amenazas que generan impacto de riesgo medio que puede ocasionar perdida de la información con lo anterior se diseña las políticas de la seguridad de la información con lo cual se desea mejorar, ya que la fundación se encuentra en etapa de creación de mejora continua para así mismo evitar la pérdida de la información para ello se tomó como referencia la ISO 27001: 2013 describe como se debe gestionar la información de una organización la cual proporciona una estructura medir los controles de riesgos y vulnerabilidades. Asi mismo proporcionar una mejora continua en los diferentes procesos usados.

Al realizar el respectivo análisis del estado en el que se encontraba la fundación Maryos se encontró que actualmente no tiene políticas de seguridad implementadas lo cual se sugirió un diseño para evitar riesgos ya que puede ocasionar perdida de la información y es importante para proporcionar calidad de los servicios prestados.

En el análisis del inventario de los activos se encontró que poseen los principales activos los cuales tienen riesgos altos con pérdida de la información lo cual ayudo realizar un análisis de vulnerabilidades y riesgos en donde se encontró que la Fundación maryos tiene un nivel alto de riesgo de pérdida de información y se delimitaron cuáles son los riesgos que afectan que se debe tomar para realizar la mejora pertinente.

Para realizar la mejora se sugirió un diseño con las principales políticas de seguridad en donde se proporcionó información sobre cómo deben funcionar entre ellas están la de recursos humanos, bases de datos, comunicación, redes sociales

entre otros, donde se evidencia como se conforma cada una de ellas para que sean tomadas en cuenta.

BIBLIOGRAFÍA

27001ACADEMY; ¿Qué es norma ISO 27001?. [Sitio web]. España: Antonio Jose Segovia *[Consulta:* 04 de mayo de 2017]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001.

AGUILERA. Purificación. Seguridad informática. Editorial Editex. Madrid: Editorial Editex 2010 ISBN 978-84-9771-761-8

ALEGRE, Maria. Seguridad informática. Editorial Paraninfo. Madrid:Editorial Paraninfo 2011 ISBN 978-84-9732-818-8

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS; Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [Sitio web]. España: Secretaria de estados de administración publicas *[Consulta:* el 04 de mayo de 2017]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

BACA, Gabriel, Introducción a la seguridad informática. Grupo Editorial Patria, 2016RAPHAEL, Rault, Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defens (3ª edición). Ediciones ENI, 2015

ICONTEC; Norma técnica ntc-iso/iec colombiana 27001 [Sitio web]. Bogotá D.C: INCONTEC *[Consulta:* el 04 de mayo de 2017]. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Geovanny, M. L. (2012). Análisis y Gestión de Riesgos Implementando la Metodología MAGERIT: AGR-MAGERIT.

Welivesecurity by ESET; Metodología práctica para gestionar riesgos [Sitio web]. España: Gutierrez Camilo *[Consulta:* el 04 de mayo de 2017]. Disponibles en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/.

ISOTOOLS EXCELLENCE; La norma ISO 27001 [Sitio web]. Isotools Excellence *[Consulta:* el 04 de mayo de 2017]. Disponible en: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

KOUNS, Jake. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams. John Wiley & Sons, 2011

ROYAL P. FISHER. Seguridad en los sistemas informáticos. Ediciones Díaz de Santos. Madrid: Díaz de Santos S.A. 1988. ISBN 84-86251-95-8

FUNDACIÓN MARYOS; Fundacion [Sitio web]. Fundación Maryos *[Consulta:* el 04 de mayo de 2017]. Disponible en: https://fundacionmaryos.org/

ANEXOS

ANEXO A

RESUMEN ANÁLITICO RAE

Título del documento	DISEÑO DE POLITICAS DE ACUERDO AL ESTANDAR ISO 27001 DE SEGURIDAD DE LA INFORMACION EN LA FUNDACIÓN INTERNACIONAL MARYOS
Autor	LORENA ASTRID CUERVO HUERTAS
Fuente Bibliográfica	27001ACADEMY; ¿Qué es norma ISO 27001?. [Sitio web]. España: Antonio Jose Segovia *[Consulta:* 04 de mayo de 2017]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001. AGUILERA. Purificación. Seguridad informática. Editorial Editex. Madrid: Editorial Editex 2010 ISBN 978-84-9771-761-8 ALEGRE, Maria. Seguridad informática. Editorial Paraninfo. Madrid:Editorial Paraninfo 2011 ISBN 978-84-9732-818-8 MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS; Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [Sitio web]. España: Secretaria de estados de administración publicas *[Consulta:* el 04 de mayo de 2017]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html BACA, Gabriel, Introducción a la seguridad informática. Grupo Editorial Patria, 2016RAPHAEL, Rault, Seguridad informática - Hacking Ético:

Conocer el ataque para una mejor defens (3ª edición). Ediciones ENI, 2015

ICONTEC; Norma técnica ntc-iso/iec colombiana 27001 [Sitio web]. Bogotá D.C: INCONTEC *[Consulta:* el 04 de mayo de 2017]. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Geovanny, M. L. (2012). Análisis y Gestión de Riesgos Implementando la Metodología MAGERIT: AGR-MAGERIT.

Welivesecurity by ESET; Metodología práctica para gestionar riesgos [Sitio web]. España: Gutierrez Camilo *[Consulta:* el 04 de mayo de 2017]. Disponibles en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/.

ISOTOOLS EXCELLENCE; La norma ISO 27001 [Sitio web]. Isotools Excellence *[Consulta:* el 04 de mayo de 2017]. Disponible en: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

KOUNS, Jake. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams. John Wiley & Sons, 2011

ROYAL P. FISHER. Seguridad en los sistemas informáticos. Ediciones Díaz de Santos. Madrid: Díaz de Santos S.A. 1988. ISBN 84-86251-95-8

	FUNDACIÓN MARYOS; Fundacion [Sitio web]. Fundación Maryos *[Consulta:* el 04 de mayo de 2017]. Disponible en: https://fundacionmaryos.org/
Resumen	Con la evolución de la tecnología aumenta la necesidad de saber información de las diferentes empresas y compañías para poderla utilizar ya se en contra o venderla a los competidores. De acuerdo con lo anterior a la fundación maryos se dará una propuesta de diseño de políticas de seguridad de la información basadas en ISO 27001 el cual tendrá los procesos y controles de seguridad de cada una de las áreas con el fin de proteger la información contra personas externas e internas. Para deducir lo anterior se tomó en cuenta la metodología margerit para identificar los activos y amenazas su respectiva probabilidad de daño.
Palabras Claves	Seguridad de la información, ISO 27001, Margerit

Descripción del Problema de Investigación

Se evidencia que en la Fundación Maryos no tiene un control de políticas de seguridad de la información de acuerdo con lo informado por los fundadores ellos desean tener un diseño de políticas de calidad para implementarlo.

La seguridad en los sistemas de información es un tema de actualidad, por lo que en los últimos años se han realizado estudio de bases teóricas y el diseño e implementación de prácticas para tener mejor seguridad en la confidencialidad, integridad y disponibilidad de la Información.

La seguridad de los sistemas de información es indispensable para cualquier entidad o empresa, ya que se debe garantizar que la información esté Disponible en:buen estado y no estén alterados por factores externos, que genera pérdidas, y pongan en riesgo la viabilidad de la empresa. Las personas que trabajan en el mundo empresarial deben recibir instrucciones claras y definitivas que los ayuden a

garantizar la seguridad de la información en el complejo mundo de los negocios con el objetivo primordial de mantener sólido su futuro económico.

La Fundación Maryos es una entidad sin ánimo de lucro, en su inicio de creación tiene como propósito servir a la población más desfavorecida, como niños y ancianos ubicados (Garagoa, Chinavita, Chiquinquirá entre otros) en lugares apartados de la ciudad, que necesitan apoyo en el área de la salud y medidas de prevención que les permita mejorar sus condiciones y tener bienestar. Por esta razón la fundación debe manejar gran cantidad de información proveniente tanto de entidades y personas que la apoyan como el manejo de las bases de datos de las personas que requieren dicho apoyo, por ser una entidad vigilada por el Estado debe llevar un control estricto de su contabilidad que le permita manejar su flujo de ingresos y gastos, para de esta manera proyectar los diferentes servicios la comunidad necesitada.
Es necesario implementar en la Fundación Maryos un Sistema de Seguridad de la Información a niveles macro y micro, utilizando la normatividad establecida en este campo, tales como las normas ISO 27001, así mismo crear un manual de políticas y normas de seguridad en donde se estructurará la seguridad organizacional, seguridad lógica, Seguridad física, seguridad legal.

Para lo anterior se realizará un inventario de los equipos que tiene la fundación, luego de lo anterior se realizara una evaluación de riegos para sí diseñar las políticas de seguridad para el mejoramiento de la seguridad de la fundación. .

Objetivos

OBJETIVO GENERAL

Diseñar políticas de protección de la información basándose en las normas ISO 27001:2013, manual de políticas y normas de seguridad de la información en la Fundación Maryos.

OBJETIVOS ESPECÍFICOS

1. Evaluar el estado la seguridad informática de la Fundación Maryos.
2. Diseñar políticas de seguridad informática de la Fundación Maryos.
3. Plantear manual de políticas de seguridad usando las normas ISO 27001 en la Fundación Maryos.

Referentes Teóricos

Metodología MARGERIT

Es una metodología de análisis y gestión de riesgos de los sistemas de información con el fin de minimizar los riesgos en las empresas públicas en las diferentes áreas. Para ello se deben seguir el siguiente método de análisis de riesgos se deben tener en cuenta los siguientes principios conocer e identificar los activos y su degradación con el tiempo, identificar las amenazas de los activos, identificar el daño de los diferentes activos.

En la descripción de un activo se debe tener en cuenta la información y el servicio que presta, entre los activos conocidos están los datos, servicios, aplicaciones informáticas, equipos informáticos, soporte, redes de comunicaciones, instalaciones y personas.

Los activos son dependientes de otros activos donde tienen las siguientes capas: activos esenciales que es la información, los servicios internos es la estructura de lo que, compuesta el activo, el equipamiento informático aplicaciones o software utilizadas en dicho activo, el entorno se encarga de garantizar el equipamiento y mobiliario, servicios subcontratados por terceros, instalaciones físicas, el personal que son los usuarios, operadores, administradores, desarrolladores.

ISO/ IEC 27001 (La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) tomado

Referencias Conceptuales

- **Confidencialidad:** Es la capacidad que se tiene para guardar o proteger la información con el fin de que las personas no autorizadas para el acceso la puedan utilizar de acuerdo con lo anterior se deben tener diferentes tipos de perfiles.
- **Integridad:** Se encarga que cada información tenga procesos como lo son modificación, creación y borrado el cual solo debe ser realizado por el personal autorizado, dando a entender que si no es un personal autorizado no puede realizar estos procesos.
- **Disponibilidad:** Consiste que tanto los activos o información esté disponible cuando sea necesaria o se vaya a usar por parte del hardware y el software para el usuario que la va a usar
- **Información:** Es la descripción de proceso que maneja un software o un hardware.
- **Activos:** Son todos los elementos de valor que sean importante para un elemento.
- **Amenazas:** Es una situación o proceso que puede dañar un activo.
- **Vulnerabilidad:** Es una debilidad de un sistema de información permitiendo que el intruso pueda afectar la disponibilidad, integridad y confidencialidad.

Resultados

Se realizó un diagnóstico de vulnerabilidades y amenazas analizando su respectivo porcentaje de riesgo un diseño de acuerdo con lo anterior se diseñó políticas de seguridad de la información en cada uno de los procesos de la Fundación Maryos.

Conclusiones

De acuerdo al análisis realizado a los diferentes activos de información en la Fundación Maryos se evidenciaron vulnerabilidades y amenazas que generan impacto de riesgo medio que puede ocasionar perdida de la información con lo

anterior se diseña las políticas de la seguridad de la información con lo cual se desea mejorar, ya que la fundación se encuentra en etapa de creación de mejora continua para así mismo evitar la pérdida de la información para ello se tomó como referencia la ISO 27001: 2013 describe como se debe gestionar la información de una organización la cual proporciona una estructura medir los controles de riesgos y vulnerabilidades. Asi mismo proporcionar una mejora continua en los diferentes procesos usados.

Al realizar el respectivo análisis del estado en el que se encontraba la fundación Maryos se encontró que actualmente no tiene políticas de seguridad implementadas lo cual se sugirió un diseño para evitar riesgos ya que puede ocasionar perdida de la información y es importante para proporcionar calidad de los servicios prestados.

En el análisis del inventario de los activos se encontró que poseen los principales activos los cuales tienen riesgos altos con pérdida de la información lo cual ayudo realizar un análisis de vulnerabilidades y riesgos en donde se encontró que la Fundación maryos tiene un nivel alto de riesgo de pérdida de información y se delimitaron cuáles son los riesgos que afectan que se debe tomar para realizar la mejora pertinente.

Para realizar la mejora se sugirió un diseño con las principales políticas de seguridad en donde se proporcionó información sobre cómo deben funcionar entre ellas están la de recursos humanos, bases de datos, comunicación, redes sociales entre otros, donde se evidencia como se conforma cada una de ellas para que sean tomadas en cuenta.