DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA - SGSI PARA LA FUNDACIÓN SABEMOS CUIDARTE EN LA CIUDAD DE POPAYÁN

SAUL AQUILINO BAUTISTA SARRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
POPAYÁN
2018

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA - SGSI PARA LA FUNDACIÓN SABEMOS CUIDARTE EN LA CIUDAD DE POPAYÁN

SAUL AQUILINO BAUTISTA SARRIA

Trabajo de grado como requisito para optar el título de

Especialista en Seguridad Informática

Ing. YINA ALEXANDRA GONZÁLEZ SANABRIA

Asesor del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA

POPAYÁN

2018

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Ciudad y Fecha de entrega

DEDICATORIA

A mi Madre que siempre me apoya en todas las actividades que emprendo en mi vida. A mi Esposa y mis hijos por toda su compresión durante el tiempo que me llevo realizar mi carrera y este proyecto y a Dios por brindarme salud para culminar con éxito esta nueva etapa.

AGRADECIMIENTOS

A todos los Funcionarios de la Fundación Sabemos Cuidarte por su colaboración en el desarrollo del presente proyecto y a los Docentes de la Universidad Abierta y a Distancia UNAD por sus enseñanzas, acompañamiento y orientación.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

1. INTRODUCCION

Se hace muy difícil, por no decir que imposible, negar el ritmo tan acelerado y los avances tan significativos que se han tenido, en el factor del tiempo, en el tema relacionado a las Tecnología de la Información y lo que esto conlleva a nuestra sociedad. Se puede decir que estas Tecnologías están presentes en todas las actividades de nuestras vidas, algunos de los ejemplos que se pueden visualizar son: en la educación muchas universidades hacen su proceso de registro para sus matrículas usando aplicaciones web; en el comercio se han incrementado sustancialmente los pedidos y el pago por medios electrónicos; en las Entidades del Gobierno se pueden adelantar algunos trámites accediendo únicamente a su página web y en el sector salud se está dejando de lado las historias clínicas elaborados en papel y diligenciadas a mano por historias clínicas sistematizadas.

Los cambios o avances en las Tecnologia de la información han generado una transformación en la manera como se debe ver el presente y en el cómo afrontaremos el futuro en términos del proteger el activo más valioso que tienen las Entidades y que es considerada la fuente esencial de todo sistema de Información: la Información.

El presente trabajo es un proyecto aplicado sobre los activos, la valoración de los posibles riesgos y la proyección de algunas medidas para mejorar la Seguridad a nivel informático de la Fundación Sabemos Cuidarte, que es una Entidad del sector salud, que presta sus servicios a varias Entidades Promotoras de Salud (EPS) y que atiende a los usuarios directamente en la casa (atención domiciliaria) en la Ciudad de Popayán y en algunos Municipios aledaños.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DEFINICIÓN DEL PROBLEMA.

Se hace indiscutible que hoy en día el activo más importante que tienen las Organizaciones es “La Información” y por tal motivo es indispensable que se tomen las medidas necesarias para cuidar, proteger, salvaguardar y evitar la fuga de tan preciado activo.

La Fundación Sabemos Cuidarte tiene serios problemas con la seguridad de la información ya que no cuenta con un inventario de los equipos de cómputo y su licenciamiento, no se cuenta con planes de mantenimiento preventivo, las claves de acceso a la red inalámbrica se han convertido en públicas, no se cuenta con un procedimiento establecido para la realización de las copias de seguridad y de recuperación de información, no se realiza un proceso periódico de revisión de las actualizaciones del sistema operativo, se cuenta con antivirus libres configurados en su opción más básica; en parte todos estos inconvenientes se presentan porque no existe una persona responsable de esta actividades y no se cuentan con políticas de seguridad de información entre otras.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de un Sistema de Gestión de Seguridad Informática permitirá mejorar la seguridad en los procesos de manejo de información y la seguridad del sistema de la Fundación Sabemos Cuidarte?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad Informática en la Fundación Sabemos Cuidarte.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar el inventario del hardware y software utilizados actualmente en la prestación de servicios en la Fundación Sabemos Cuidarte.
- Identificación de riesgos en el manejo de la seguridad de la información existentes en la Fundación Sabemos Cuidarte.
- Definir las políticas de seguridad de la información para la Fundación Sabemos Cuidarte.
- Realizar la divulgación del contendio del presente trabajo a la Gerencia de la Fundación Sabemos Cuiadarte una vez revisado y aprobado el presente documento.

4. JUSTIFICACIÓN

Es impresionante la velocidad con la cual la tecnología y las telecomunicaciones avanzan cada día, facilitando las actividades que se realizan en los diferentes espacios, es así como hoy por hoy se puede realizar cualquier tipo de transacción sin necesidad de diligenciar un solo papel y todo gracias al computador y el mundo de las telecomunicaciones.

Actualmente la gran mayoría de empresas y personas utilizan las diferentes alternativas tecnologías que proporciona el mercado, lo que implica tomar conciencia de los peligros que se corren al no identificar y establecer medidas básicas de protección relacionada con la seguridad de la información, evitando así ser víctima de ataques, pérdida o robo de la información.

Por lo expuesto anteriormente y partiendo de la base que la Fundación Sabemos Cuidarte utiliza de manera recurrente el computador para realizar las actividades en cumplimiento de su misión, transacciones electrónicas relacionadas con pagos e informes a presentar a las Entidades de Control, utilización de software de aplicación entre otros, es pertinente iniciar un proceso de diseño del Sistema de Gestión de Seguridad Informática, que permita garantizar la custodia de la información, sus controles y la mitigación de los riesgos derivados del uso inadecuado de las diferentes herramientas tecnológicas utilizadas para el desarrollo de sus funciones.

5. AREA Y LINEA DE INVESTIGACIÓN

El presente proyecto se enmarca dentro del área de la Ingeniería de Sistemas y está enfocado al diseño de un Sistema de Gestión de Seguridad Informática (SGSI), los sistema de gestión establecen unos lineamientos que son de tipo genérico y por lo tanto son aplicables a todo tipo de organización sin importar su objeto social, la empresa debe hacer un proceso de adaptación de estos "requisitos" a sus necesidades especificadas, de esta manera se pueden obtener muchos beneficios como: la identificación y manejo de riesgos, procesos de mejora continua, garantía de continuidad y disponibilidad del servicio, mejorar la percepción de los clientes y de esta manera poder posesionarse comercialmente en el mercado de la Ciudad.

El presente trabajo es un proyecto aplicado, el cual tiene como característica principal la aplicación de manera práctica de los conocimientos bases. Se pretende el poder identificar los posibles riesgos, a nivel informático, a los cuales puede estar expuesta la Fundación Sabemos Cuidarte y plantear las posibles medidas o soluciones a las mismas y de esta manera disminuir o mitigar dichos riesgos.

6. ALCANCE Y DELIMITACIÓN DEL PROYECTO

El Sistema de Gestión de Seguridad Informática a diseñar durante el periodo 2016-2017 en la Fundación Sabemos Cuidarte con sede en la Ciudad de Popayán Departamento del Cauca, se aplicará a todos los procesos responsables del manejo de la información y a los sistemas utilizados con el fin de garantizar la eficaz y eficiente prestación del servicio.

7. MARCO REFERENCIAL

7.1 ESTADO DEL ARTE

La tesis de grado llamada “Diseño de un Sistema de Gestión de seguridad de la información para el laboratorio clínico Confesalud IPS de la Ciudad de Ocaña”, elaborado por Rodríguez Andrea y Sumlabe Karen, publicado en octubre de 2014, como opción de grado de la Universidad Francisco de Paula Santander Ocaña; documento en el cual el sistema de gestión de seguridad de la información es una herramienta que ofrece a las organizaciones un modelo de trabajo como utilidad para diseñar, implementar y mejorar el desempeño en sus labores, protegiendo y resguardando la información como activo primordial y necesario en el ejercicio de sus actividades. El fin principal por el cual se diseña el sistema de gestión de seguridad de la información, es con el propósito de cuidar la confiabilidad, la disponibilidad y la integridad de la información procesada y guardada por el laboratorio clínico Confesalud Ips Ltda. (Rodriguez & Sumlabe, 2014).

La tesis de grado llamada “Modelamiento de proceso basado en el grupo de normas internacionales ISO/IEC 27000 para gestionar el riesgo y seleccionar controles en la implementación del sistema de gestión de seguridad de la información”, elaborado por Reina Elkin y Morales José, publicado en 2014 de la Universidad Tecnológica de Pereira, documento en el cual se demuestra que es indispensable para cualquier compañía garantizar que sus procesos de gestión de la información sean lo suficientemente efectivos, confiables y organizados, de tal manera que se pueda prestar un servicio o entregar un producto con calidad. Para esto las compañías deben valerse de las metodologías y modelos aprobados internacionalmente que promueven una gestión de la información con seguridad, haciéndose indispensable implementar los procesos y procedimientos necesarios para alcanzar este objetivo. Un Sistema de Gestión de Seguridad de la Información (SGSI) es una herramienta que le permite a una compañía realizar una completa gestión de los riesgos que se presentan en la producción, procesamiento, almacenamiento y análisis de la información, buscando mantener siempre las características de Confidencialidad, Integridad y Disponibilidad con las que esta debe contar. La implementación de un SGSI en cualquier compañía conlleva realizar una serie de actividades que deben ceñirse a lo señalado por el grupo de normas ISO/IEC 27000, siendo la ISO/IEC 27001 la que establece los requisitos para la certificación, pero teniendo en cuenta las recomendaciones y mejores prácticas descritas en las demás. (Reina & Morales, 2014).

El proyecto de grado llamado “Diseño de las Politicas de control de Riesgos de la seguridad de la Información para la sede central de la Gobernación del Putumayo”, trabajo elaborado y presentado por Leyda Liliana Cordoba Araujo y Wilson Camilo Delgado Trujillo, Estudiantes de la Especialización en Seguridad Informatica de la Universidad Nacional Abierta y a Distancia – UNAD, en el año 2016, este documento presenta de manera adecuada el proceso que se puede seguir para la elaboración del diagnostico de las vulnerabilidades que se tienen en los sistemas de información de la Gobernación; se realiza la inspección de la infraestructura tecnologica,se evaluan los riesgos y se proyectan las posibles politicas y/o procedimientos que permiten la prevención, el control o la mejora en terminos de seguridad de la información.

Se revisa otro proyecto de grado denominado “Modelo para la implementación del Sistema General de Seguridad informatica y protocolos de Segurida Informatica en la Oficina TIC de la Alcaldia Municipal de Fusagasuga, basado en la gestión del Riesgo Informatico”, trabajo elaborado y presentado por Ana Milena Pulido Barreto y Jenith Marsella Mantilla Rodriguez, estudiantes de la Especialización en Seguridad Informatica de la de la Universidad Nacional Abierta y a Distancia – UNAD, en el año 2016, en este documento se puede observar como apartir de los lineamientos y requerimientos que hacen las Entidades de Orden Nacional, la Alcaldia hace un proceso de revisión de los riesgos informaticos y utilizando la estrategia del Planear, Hacer, Verificar y Actuar; que es la estrategia que se usa o aplica para la implementación de los Sistema de Gestión de Calidad.

7.2 MARCO TEORICO

Con el fin de poder llevar a cabo esta propuesta se hace necesario investigar y documentarnos en temas relacionados como: que es la seguridad informática y la seguridad de la información; profundizar sobre las metodologías existentes para la identificación y la gestión del riesgo, Normas Internacionales como la ISO 27001 la cual describe cómo gestionar la seguridad de la información en un Empresa, poder identificar y clasificar las posibles vulnerabilidades o amenazas informáticas y por último los documentos que permiten realizar una adecuada estructuración del sistema de gestión de seguridad informática con sus respectiva etapas.

A continuación se procede a brindar información general de cada uno de los temas aquí consignados:

7.2.1. ¿Qué es la Seguridad Informática?

La Seguridad Informática se considera una disciplina o el área que se encarga de proyectar, elaborar o diseñar normas, procesos, procedimientos, métodos o técnicas que están orientadas o dirigidos a proveer, lo que se puede denominar, “condiciones seguras y confiables”, para el proceso de los datos en los diferentes sistemas informáticos.

En otras palabras, la Seguridad Informática busca prevenir el uso No autorizado de los sistemas informáticos (pero ¿Qué son los sistemas informáticos? los Sistemas Informáticos se pueden definir como el conjunto de partes debidamente interrelacionados que almacenan y procesan la información).

7.2.2. ¿Qué es la Seguridad de la Información?

La seguridad de la información se establece como la capacidad que tienen los sistemas informáticos de resguardar y proteger la información que manejan o utilizan, buscando siempre garantizar los principios de confidencialidad, disponibilidad, integridad y autenticación.

Con relación a las Metodologías existentes para la identificación y la gestión de los riesgos informáticos se tiene:

7.2.2.1 Octave (Operationally Critical Threat, Asset and Vulnerability Evaluation) esta metodología revisa o estudia la infraestructura de la información y hace énfasis especial en la manera como las Empresas usan dicha infraestructura. En todas las organizaciones es indispensable que sus empleados o funcionarios tomen conciencia de la importancia que tienen todos los activos que están interrelacionados con la información y de la necesidad de protegerlos de la mejor manera posible.

La Metodología Octave establece tres (03) fases para su proceso de evaluación:

- La construcción de perfiles de amenazas basadas en los activos.
- La identificación de las posibles vulnerabilidades de la infraestructura.
- El desarrollo de estrategias y planes de seguridad.

7.2.2.2 Magerit está metodología fue diseñada por el Consejo Superior de Administración Electrónica y nació al identificar la creciente "dependencia" de las Organizaciones y de la Sociedad en general del manejo de la información mediante el uso de la tecnología.

La metodología Magerit para la revisión y análisis de los riesgos plantea las siguientes etapas:

- Planificación.
- Análisis de Riesgos.
- Gestión de los Riesgos.
- Selección de Salvaguardas.

7.2.2.3 Mehari esta metodología fue desarrollada y puesta en el "mercado" en el año de 1995 por el Club Francés de la Seguridad de la Información – CLUSIF. Mehari mediante el uso del sistema de auditorías busca detectar las posibles vulnerabilidades, realizar el análisis de todas las situaciones de riesgo y por ultimo plantear conclusiones en base a los contenidos identificados.

La metodología Mehari está conformada por tres módulos:

- La Evaluación o análisis de los riesgos.
- La evaluación de la seguridad la cual está enfocada en el análisis de las vulnerabilidades.
- El análisis de las amenazas.

7.2.2.4 NIST SP 800 – 30 esta metodología fue diseñada por el Instituto Nacional de Estándares y Tecnología – NIST de los Estados Unidos. Para lograr el éxito en la implementación de esta metodología se hace necesario que toda la organización participe en el proceso.

La metodología NIST SP 800 – 30 está compuesta por nueve pasos:

- La Caracterización del sistema.
- La identificación de las amenazas.
- La identificación de las vulnerabilidades.
- El Análisis de los controles.

- La Determinación de Probabilidades.
- El Análisis del impacto.
- La Determinación de los riesgos.
- La Recomendaciones de control.
- La Documentación de los resultados.

7.2.2.5. Coras (Construct a Platform for Risk Analysis of Security Critical Systems) esta metodología fue desarrollada por SINTEF, que es un grupo de investigación de origen Noruego. Está basada principalmente en la elaboración de modelos y para ello plantea siete pasos:

- Presentación.
- Análisis de Alto Nivel.
- Aprobación.
- Identificación de Riesgos.
- Estimación de Riesgos.
- Evaluación de Riesgos.
- Tratamiento de los Riesgos.

7.2.2.6. Cramm (CCTA Risk Analysis and Management Method) esta metodología fue desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones – CCTA y la cual está orientada a grandes industrias y entidades gubernamentales especialmente en Europa y en ella se incluyen tres etapas:

- La Identificación general de los objetivos de seguridad (en esta etapa se incluye l identificación y posterior evaluación de todos los activos hardware y software, como también la valoración de los datos o información y el impacto de estos sobre la organización)
- El Análisis de Riesgos (en esta etapa se deben identificar las amenazas que pueden afectar el sistema, las posibles vulnerabilidades que explotan dichas amenazas y la posibilidad que se tienen de que dichos riesgos se puedan materializar).
- La Identificación y selección de las medidas de seguridad (la Metodología Cramm cuenta con una librería en la cual se encuentran aproximadamente unas tres mil (3.000) medidas de seguridad planteadas).

7.2.2.7. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité que significa "expresión de las necesidades e identificación de los objetivos de seguridad") esta metodología es de origen Francés y pasa de ser de una metodología de identificación de riesgos a convertirse en una verdadera herramienta para el diseño del proyecto. Para su desarrollo se plantean cinco fases:

- El Estudio del Contexto.
- El Estudio de los Eventos Peligrosos.
- El Estudio de los Escenarios de Amenazas.
- El Estudio de los Riesgos.
- El Estudio de las Medidas de Seguridad.

7.2.2.8. ISO 27000 Las normas de la “gran familia” ISO 27000 tienen sus orígenes en Entidades Británicas, aproximadamente en el año de 1995, cuando para la fecha se publican recomendaciones relacionadas con las buenas prácticas de seguridad que deben seguir la Empresas, cinco (5) años después aparece la primer norma ISO relacionada con el tema y se denominó ISO/IEC 17799:2000, la cual a su vez cinco (5) años más tarde sería renombrada como la norma ISO 27002:2005. (El Portal de ISO 27001 en Español)

La serie 27000 relacionada con la Seguridad de la Información, es la serie que se encuentra asignada dentro de los estándares ISO/IEC y dentro de las cuales tenemos:

- ISO 27000: Publicada en mayo de 2009. Contiene la descripción general y el vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman. (Wikipedia, 2016)

- UNE-ISO/IEC 27001: esta norma en su contenido describe cómo gestionar la seguridad de la información al interior de las empresas, es de aclarar que estas normas son “genéricas” y por lo tanto son adaptables a cualquier tipo de empresa que las quiera implementar.

- ISO/IEC 27002: esta norma establece lo que se puede denominar el catálogo de las buenas prácticas en términos de seguridad informática, además se debe recalcar que en esta norma hay establecidos un total de

114 controles, aunque no es necesario cumplirlos todos si es necesario e indispensable revisarlos todos.

- ISO/IEC 27003: esta norma establece los lineamientos base para la implementación de los Sistemas de Gestión de la Seguridad de la Información – SGSI.

- ISO 27004: esta norma está muy asociada y va muy de la mano de la norma ISO 27003, ya que contiene los parámetros necesarios para medir, de la mejor manera posible, los resultados que se obtienen del implementar un SGSI.

- ISO 27005: esta norma brinda una serie de estándares para la gestión de los riesgos que se pueden identificar en términos de la seguridad de la información y riesgos que deben ser revisados y tratados en la implementación o mantenimiento de los SGSI.

- ISO 27006: esta norma contiene la guía base que deben seguir y aplicar todas las entidades o entes certificadores, porque en ella están consignados los puntos claves que se deben auditar dentro de los SGSSI.

7.3 MARCO CONCEPTUAL

En el marco conceptual se tiene las siguientes definiciones:

- **Amenaza**: aquel evento o situación que puede comprometer la integridad, la disponibilidad y/o la confidencialidad de la información que manejamos dentro de la entidad.
- **Riesgo**: es la probabilidad que tiene una amenaza de dejar de ser solo una amenaza y de convertirse en una realidad, estos riesgos se pueden catalogar en tres niveles bajos, medios y altos; esta calificación se suministra dependiendo del número de eventos presentados en un periodo de tiempo determinado.
- **Política**: son lineamientos institucionales, las cuales son establecidas para mitigar y/o prevenir los efectos de las amenazas y las cuales deben ser socializadas, entendidas y puestas en práctica por todo el personal de la organización.
- **Procedimiento**: es el paso a paso de cómo se debe ejecutar una tarea o actividad y el cual debe estar debidamente documentado y socializado; se

recomienda que su estructura sea muy sencilla, entendible y de fácil comprensión.

- **SGSI**: esta sigla corresponde a la abreviatura de Sistemas de Gestión de Seguridad de la Información.
- **Confidencialidad:** consiste permitir el acceso de la información única y exclusivamente a las personas o procesos que están debidamente autorizados.
- **Disponibilidad:** consiste en que se debe asegurar que el uso y el acceso de la información se realice en el momento oportuno y de manera confiable.
- **Integridad**: la información debe estar debidamente protegida de proceso de adulteración o modificación, como también de borrado o eliminación de la misma por personal o por proceso no validados o autorizados.
- **ISO**: esta sigla corresponde a la Organización Internacional de Normalización.
- **Seguridad de la Información**: consiste en garantizar la confidencialidad, integridad y disponibilidad de la información.

7.4 MARCO LEGAL

Dentro de la normatividad aplicable para el servicio de Atención Domiciliaria prestado por la Fundación Sabemos Cuidarte se relacionan las siguientes normas:

Protección de la Información y de los Datos Ley 1273 del 5 de enero de 2009 del Congreso de Colombia por 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. Creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.¨

Protección de datos personales Ley Estatutaria 1581 de 2012 del Congreso de Colombia Por la cual se dictan disposiciones generales para la protección de datos personales.

Fortalecimiento del Sistema General de Seguridad Social en salud Ley 1438 de 2011 del Congreso de Colombia ¨Por medio de la cual se reforma el sistema general de seguridad social en salud y se dictan otras disposiciones¨.

7.5 MARCO CONTEXTUAL

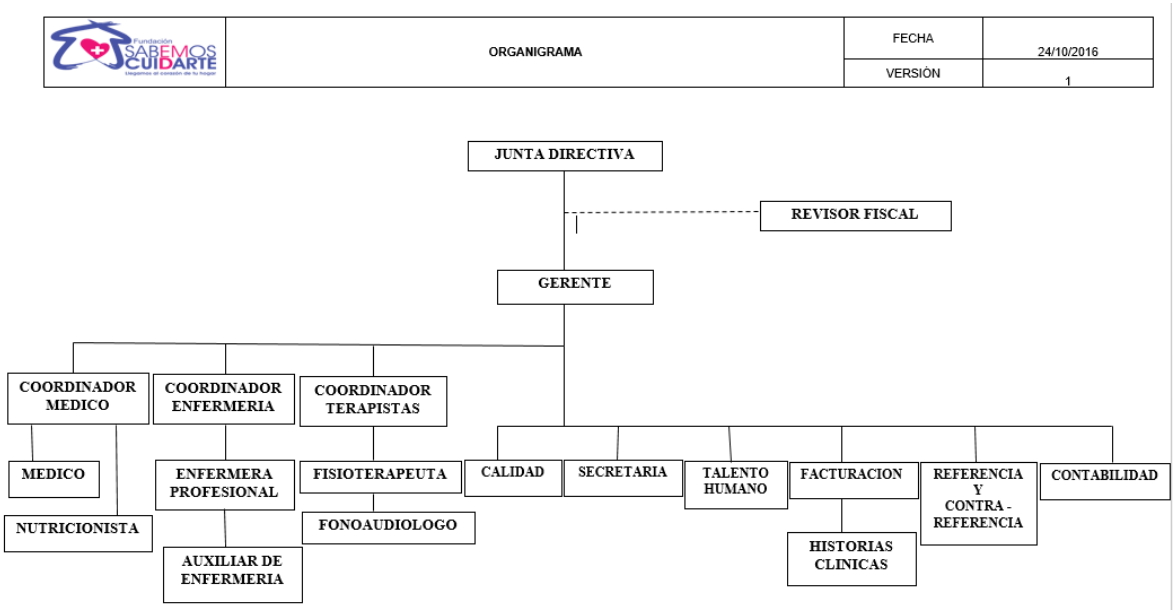
La Fundación Sabemos Cuidarte es una IPS de atención domiciliaria, que presta servicios de Valoración por Medico General, Nutricionista y Enfermera Jefe; además servicios de terapia física, terapia de fonoaudiología, terapia ocupacional, servicio de auxiliar de enfermería para aplicación de medicamentos o el servicio de auxiliar de enfermería por turnos, tiene convenios con varias Empresas Promotoras de Salud (EPS) y presta sus servicios a los usuarios de los Municipios de Popayán, Piendamo y Timbio en el Departamento del Cauca.

Administrativamente la fundación está conformada por los siguientes cargos:

- Gerente
- Coordinadora de Terapias Físicas, Fonoaudiología y Ocupacionales
- Coordinadora del Servicio de Auxiliar de Enfermería
- Auxiliar de coordinación del servicio de auxiliar de enfermería
- Un contador
- Un auxiliar contable
- Un auxiliar de archivo
- Una secretaria
- Un auxiliar administrativo
- Una persona responsable del proceso de talento humano
- Una persona responsable del proceso de facturación

La estructura organica y la línea de mando de la Fundación se puede observar en su respectivo Organigrama (ver figura 1. Organigrama).

Figura 1. Organigrama



Fuente: Fundación Sabemos Cuidarte

Activos informáticos de la Fundación Sabemos Cuidarte

En la actualidad se cuentan con nueve (09) computadores de los cuales siete (07) son de escritorio y dos (02) son portátiles, los equipos cuentan con sistemas operativos como Windows vista y Windows 7, todos los equipos cuentan con Microsoft office, algunos usuarios tienen habilitado Skype, se cuenta con un aplicativo de facturación y se cuenta con un aplicativo contable, se establece que existen varios tipos de antivirus instalado en los equipos.

Los procesos que manejan la información son:

- Existe un sistema de información al usuario.
- Proceso de facturación
- Proceso Contable
- Proceso de gestión y tramites de solicitudes de servicios con las EPS
- Proceso de auditoría de historias clínicas.
- Proceso de almacenamiento de Historias Clínicas.

7.5.1 MISIÓN

La misión que tiene establecida la Fundación es:

“Prestar asistencia médica y terapéutica domiciliaria y demás servicios complementarios, con el fin de mejorar la calidad de vida de nuestros usuarios y su satisfacción”.

7.5.2 VISIÓN

La visión que tiene establecida la Fundación es:

“Constituirse para el 2017, como una empresa líder en servicios de salud en el ámbito domiciliario en el Departamento del cauca, con compromiso social, mediante una atención integral y oportuna a nuestros usuarios; brindando de esta forma una mejor calidad de vida”.

7.5.3 POLÍTICA DE CALIDAD

La política de calidad que tiene establecida la Fundación es:

“Hacer de la Fundación Sabemos Cuidarte una entidad reconocida a nivel Departamental en la prestación de Servicios Médicos y Terapéuticos a nivel domiciliario, mejorando la calidad de vida de las personas por medio de un equipo interdisciplinario, idóneo, que permita satisfacer las necesidades y expectativas de nuestros clientes y usuarios, con atención oportuna, servicios de calidad, e interactuando con su entorno familiar, mejorando continuamente para su satisfacción y el crecimiento de la organización”.

7.5.4 OBJETIVOS DE CALIDAD

La Fundación tiene establecido un proceso de Calidad y dentro de este proceso se tienen establecidos los siguientes objetivos de calidad:

- Prestar un servicio de forma confiable y eficaz, cumpliendo con todos los requisitos exigidos por ley.
- Satisfacer las necesidades y expectativas de nuestros clientes a través de una atención oportuna y con calidez.

- Fomentar y capacitar, al talento humano de la organización para lograr servicios de alta calidad.
- Contar con un grupo humano que cumpla los perfiles y las competencias necesarias para la atención de los usuarios.
- Manejar la información de manera oportuna y confiable.
- Mejoramiento continúo.

7.5.5 VALORES

La Fundación tiene establecido una serie de valores institucionales, los cuales sirven de lineamiento para el actuar de todos sus funcionarios, estos valores son:

- Responsabilidad
- Eficiencia
- Solidaridad
- Igualdad
- Principios éticos
- Confidencialidad y respeto
- Honestidad

8. METODOLOGIA DE DESARROLLO

Para el desarrollo del presente proyecto se utilizara el ciclo de Mejoramiento Continua PHVA (Planear, Hacer, Verificar y Actuar), teniendo en cuenta que es una de las estrategias más seguidas en la implementación de Sistemas de Gestión de Calidad y considerando que la Fundación Sabemos Cuidarte dentro de su estructura organizacional tiene establecida una Área de Calidad que trabaja bajo es lineamiento, de esta manera se mantiene y se trabaja bajo una misma línea u orientación dentro de la Entidad.

8.1 METODOLOGIA POR FASES

El presente trabajo es un proyecto aplicado y para poder llevarlo acabo se opta por la utilización de una metodología por fases teniendo en cuenta que se plantea una secuencia de pasos que se deben seguir para poder alcanzar los objetivos propuestos.

8.2 UNIVERSO Y MUESTRA

Para el diseño del Sistema de Gestión de Seguridad Informática, se establece como muestra al 100% de los procesos responsables del manejo de la información y a los sistemas utilizados en la Fundación Sabemos Cuidarte con sede en la Ciudad de Popayán Departamento del Cauca.

9. INSTRUMENTOS DE RECOLECCION

Para la recolección de la información se establecen los siguientes instrumentos de recolección:

Observación Directa y Entrevista: se establece una agenda de trabajo con cada uno de los colaboradores de la Fundación y en compañía de ellos se hace el levantamiento de la información del equipo de cómputo con el cual trabaja y acompañado de preguntas estratégicas que permitan identificar el uso de las tecnologías de la información.

Establecer la estructura de la documentación: como la entidad trabaja en la implementación de un Sistema de Gestión de la Calidad, los documentos que se generen de este proceso serán acorde a lo establecido por la Fundación en este tema.

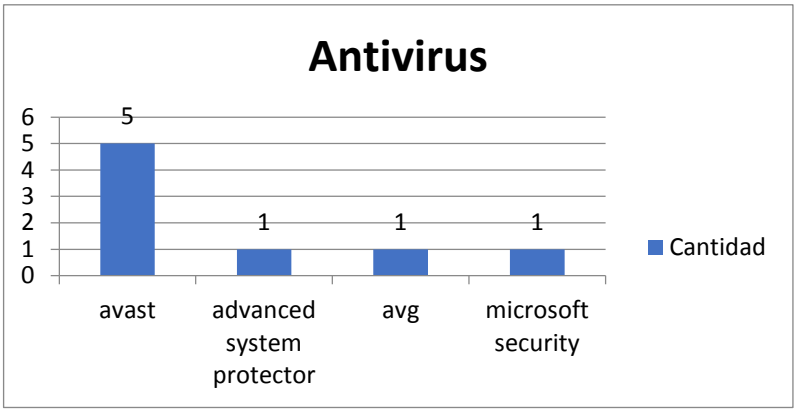
De acuerdo a la necesidades y el ambiente de trabajo se aplicaran las siguientes Técnicas para la recopilación de la información, con estas técnicas es posible identificar la situación actual de la Organización, identificar posibles problemas y oportunidades de mejora.

- **Entrevista**: es una interacción verbal, que consiste en obtener información sobre hechos, actividades o personas. En aquellos momentos en que se interactúa con los funcionarios se procede a realizar preguntas que permitan identificar nuevos riesgos y/o corroborar información obtenida previamente
- **Observación**: Consiste en examinar e investigar alguna situación, hecho, fenómeno, con el fin de recolectar datos o información para describir lo que se está detallando. Se debe solicitar a la Gerencia la autorización para acceder a los equipos de cómputo de la Fundación y de esta manera poder observar las condiciones generales de los equipos y tomar evidencia fotográfica de los hallazgos encontrados.
- **Revisión de registro:** Es buscar el historial de lo que ha sucedido anteriormente. En este caso se procede a solicitar copia de los soportes que nos permitan evidenciar de alguna manera la información que nos suministran.

Como consecuencia del proceso de recolección de información se presentan algunos de datos, asi:

- Antivirus: se identifican cinco (05) equipos con antivirus Avast Free, un equipo con antivirus AVG, un equipo con microsft security y un equipo con advanced system protector (ver Figura 2. Antivirus).

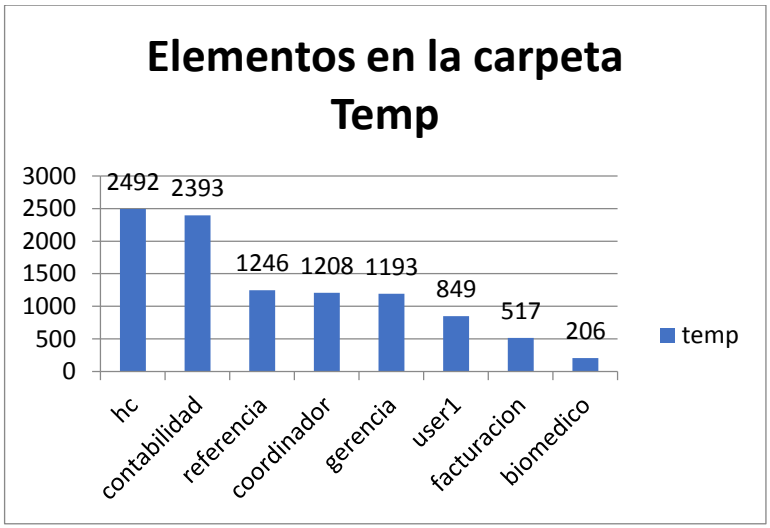
Figura 2. Antivirus



Fuente: Fundación Sabemos Cuidarte

- Elementos en la Carpeta Temp: se pudo identificar que el equipo de historias clínicas fue el equipo con la mayor cantidad de elementos en dicha carpeta con un total de 2492 elementos y el equipo con el menor número de elementos en dicha carepra es el de diomedico con un total de 206 elementos (ver Figura 3. Elementos en carpeta temp).

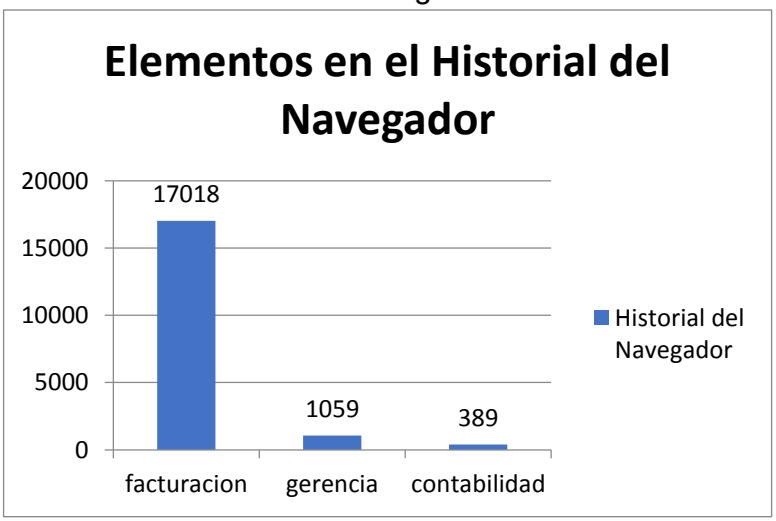
Figura 3. Elementos en carpeta Temp



Fuente: Fundación Sabemos Cuidarte

- Elementos en el historial del navegador: se pudo identificar que el equipo de facturación tenían 17018 elementos en el historial del navegador y contabilidad solamente tenía 389 elementos en dicho historial (ver Figura 4. Elementos en el historial del navegador).

Figura 4. Elementos en el historial del navegador



Fuente: Fundación Sabemos Cuidarte

- Mantenimiento preventivo: al realizar la consulta a los funcionarios responsables del equipo de cómputo sobre la periodicidad de los mantenimientos preventivos se obtuvo de manera general la misma respuesta “a los equipos de cómputo no le hacen mantenimiento

preventivo, solamente los revisan cuando se dañan o presentan algún problema que nosotros no podamos solucionar".

9.1 METODOLOGIA DE DESARROLLO

Para el desarrollo del presente proyecto se ejecutaran las siguientes etapas:

- **Etapa 1.** Establecer diagnostico frente a los requisitos de la ISO 27001. Se realizará con los responsables el levantamiento de la información evaluando el grado de cumplimiento de cada requisito en la Fundación Sabemos Cuidarte, incluyendo la identificación de las necesidades de protección del sistema informático objeto de análisis (caracterización del sistema informático. Identificación de las amenazas y estimación de los riesgos. Evaluación del estado actual de la seguridad).
- **Etapa 2:** Definir el plan de acción para el diseño del sistema de seguridad informática: En esta etapa se establecerá cronograma de trabajo incluyendo actividades, productos, fechas de ejecución, así como los responsables de la actividad.
- **Etapa 3**: Diseño del Sistema de Seguridad que garantice minimizar los riesgos identificados en la primera etapa. Definir las políticas de seguridad. Definir las medidas y procedimientos a implementar, según las actividades aprobadas en el plan de acción establecido.

10. DESARROLLO METODOLOGICO

10.1 DIAGNOSTICO SITUACIONAL DE LA ENTIDAD

Para elaborar el diagnóstico de la situación actual de la Entidad se hace necesario hacer un proceso de revisión de cada uno de los diferentes componentes y luego de esto se puede proyectar un diagnostico por cada uno de ellos.

10.1.1 REVISIÓN DEL ORGANIGRAMA

Al revisar la estructura orgánica de la Fundación se puede evidenciar que la entidad tiene una falencia muy significa en el hecho de que no cuenta dentro de ella con un funcionario que maneje el tema de los sistemas de información y los funcionarios del área administrativa tienen unos conocimientos muy básicos en el tema (ver Figura 1. Organigrama).

10.1.2 REVISIÓN PÁGINA WEB DE LA ENTIDAD

La Fundación tiene habilitado el siguiente Enlace:

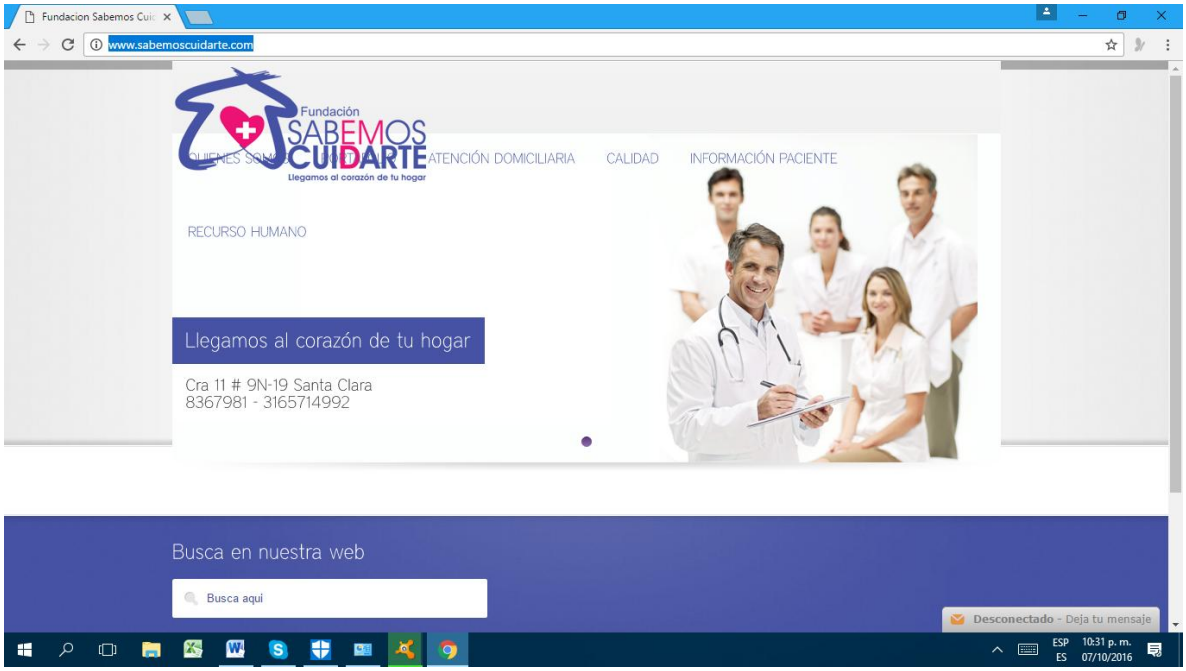
http://www.sabemoscuidarte.com/

Al realizar el proceso de navegación dentro de la página web se puede evidenciar lo siguiente:

- El logo de la entidad no permite visualizar algunas de las opciones del menú de inicio.
- La Información se encuentra sin actualizar en este momento la sede se encuentra ubicada en otra dirección.
- El slogan de la Entidad se encuentra a la mitad de la pantalla (ver Figura 5. Pagina de Inicio).
- El menú inicio está conformado por las siguientes opciones: Quienes Somos, portafolio, atención domiciliaria, calidad, información paciente, recurso humano. Pero al acceder a cualquiera de los enlaces estos no se

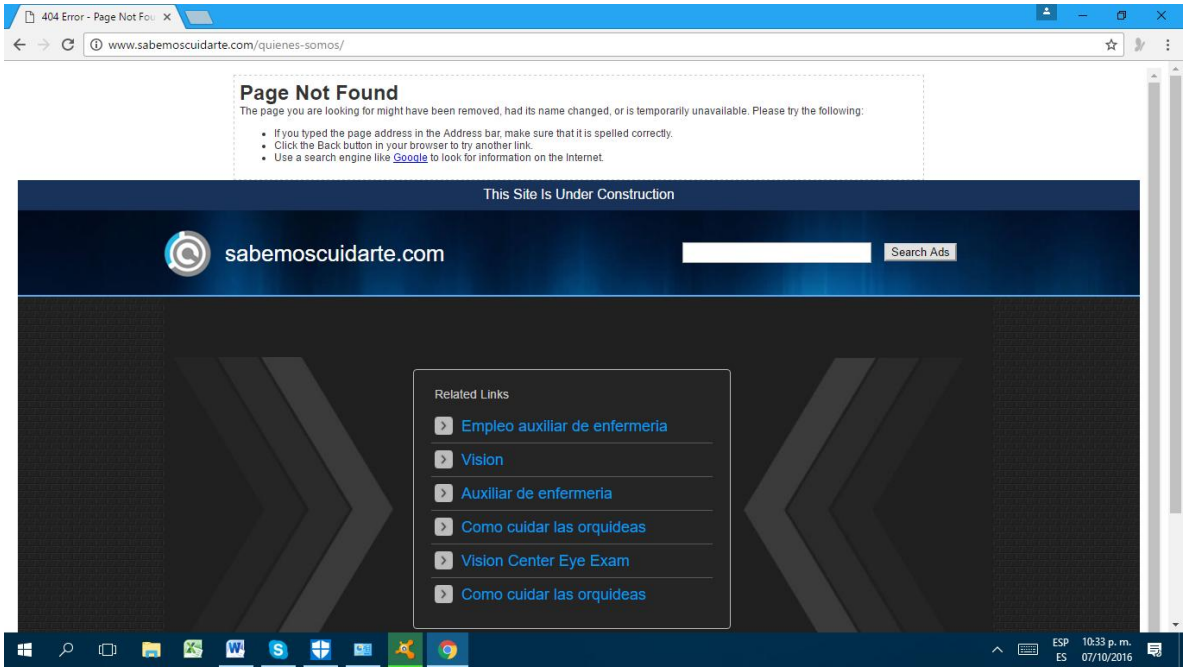
encuentran funcionales y se presenta un error (ver Figura 6. Error de página web).

Figura 5. Pagina de inicio



Fuente: Fundación Sabemos Cuidarte

Figura 6. Error de página web



Fuente: http://www.sabemoscuidarte.com/

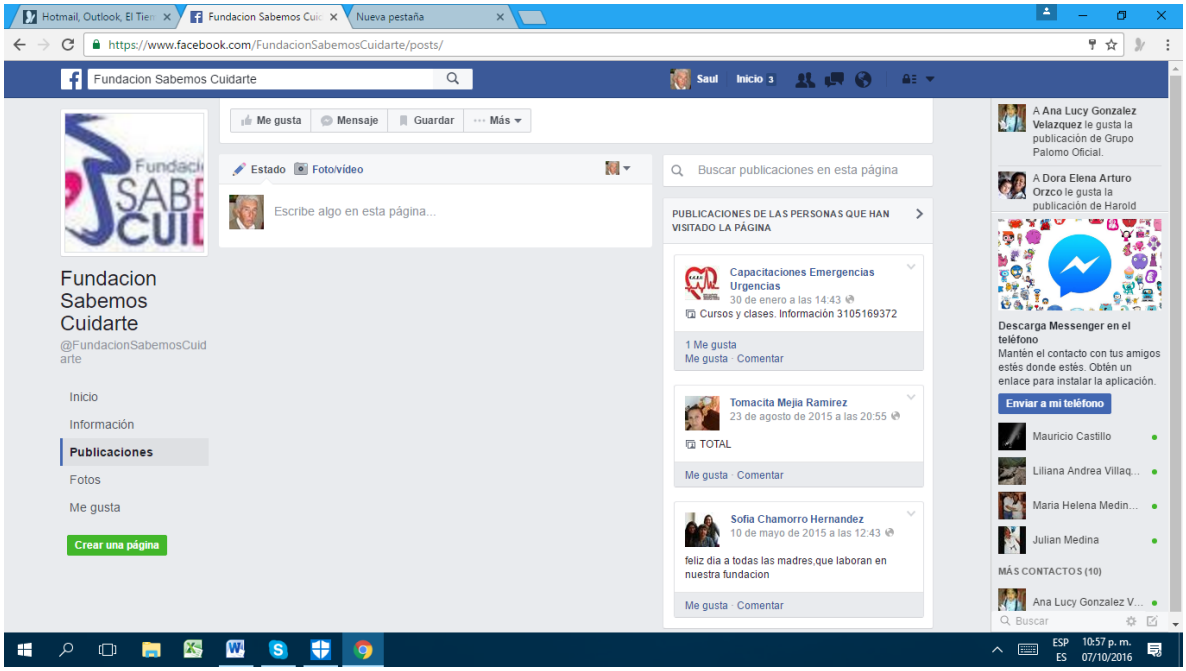
Se realiza contacto con el proveedor del servicio de la página web (Ipage) y se logra que esta quede funcional pero se observa que la página tiene mucha información desactualizada, empezando por sus datos de contacto, por lo que se hace necesario hacer un proceso de revisión, ajuste y actualización de la misma.

10.1.3 REDES SOCIALES

La Fundación tiene presencia en la red social Facebook (ver Figura 7. Facebook) pero se puede determinar que no se realiza ningún proceso de revisión o actualización de la información que se tiene, como tampoco se observa que se realice procesos de retroaliementación a los comentarios planteados por los usuarios.

En “Publicaciones” no se observan publicaciones de la entidad y en publicaciones de las personas que han visitado la entidad la última fue realizada el 30 de enero de este año, anterior hay una publicación del 23 de agosto de 2015 y del 10 de mayo de 2015, con lo cual se puede deducir que la entidad no le da uso a esta red social.

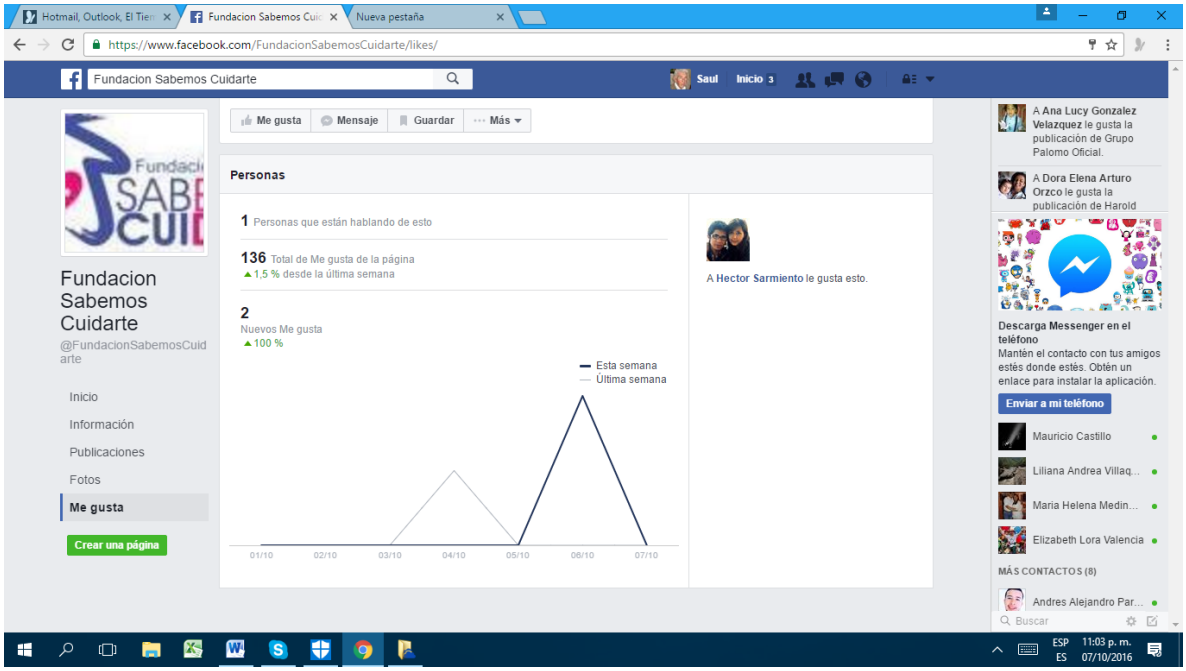
Figura 7. Facebook



Fuente: Fundación Sabemos Cuidarte

De igual manera se puede verificar en las estadísticas de “Me gusta” que entre los días del 3 al 5 se obtiene uno y entre el 5 y el 7 se obtienen 2 me gustan (ver Figura 8. Estadisticas de Facebook).

Figura 8. Estadísticas de Facebook



Fuente: Fundación Sabemos Cuidarte

10.1.4 PUNTOS DE RED

Al consultar al Gerente de la Fundación sobre la existencia de los planos de identificación de los puntos de red, se pudo establecer que la Entidad no cuenta con dicha información, como consecuencia de lo anterior se procede a realizar el trabajo del levantamiento y elaboración de dichos planos los cuales por cuestión de seguridad y de prevención se toma la determinación de no incluirlos dentro del presente trabajo. Pero dicha información será entregada al Gerente de la Fundación para su respectiva custodia.

Como consideración general se puede decir que se presento una falla en la numeración de los puntos de red, al detectar algunos “saltos” en su consecutivo; se establecio que ocho (08) puntos de red no se encuentran debidamente etiquetados.

Ademas se puede evidenciar que la Fundación tiene instalados demasiados puntos de red para el número de equipos de cómputo que se tienen en uso, además se evidencia una deficiencia en el hecho de que la Entidad no cuenta con

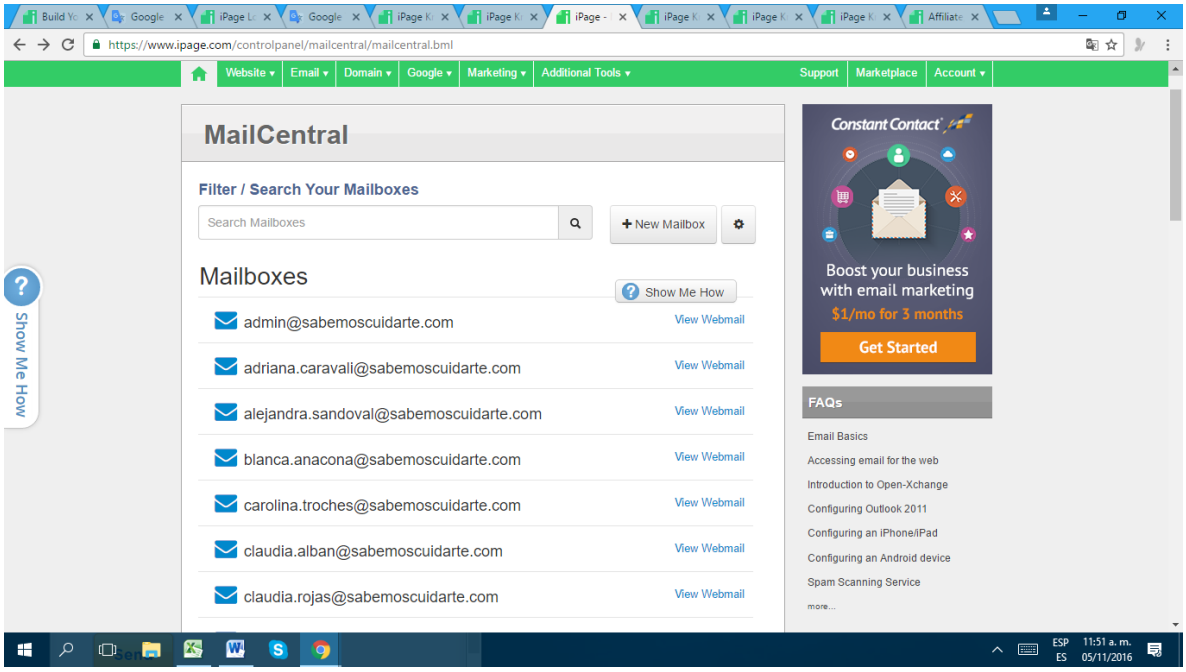
un sistema de respaldo en caso de que falle el fluido eléctrico (ups – planta de energía).

10.1.5 CORREOS ELECTRÓNICOS

En la entrevista y en la revisión de los equipos se puede evidenciar el mal uso que se da al sistema de correos electrónicos, se identifican las siguientes debilidades:

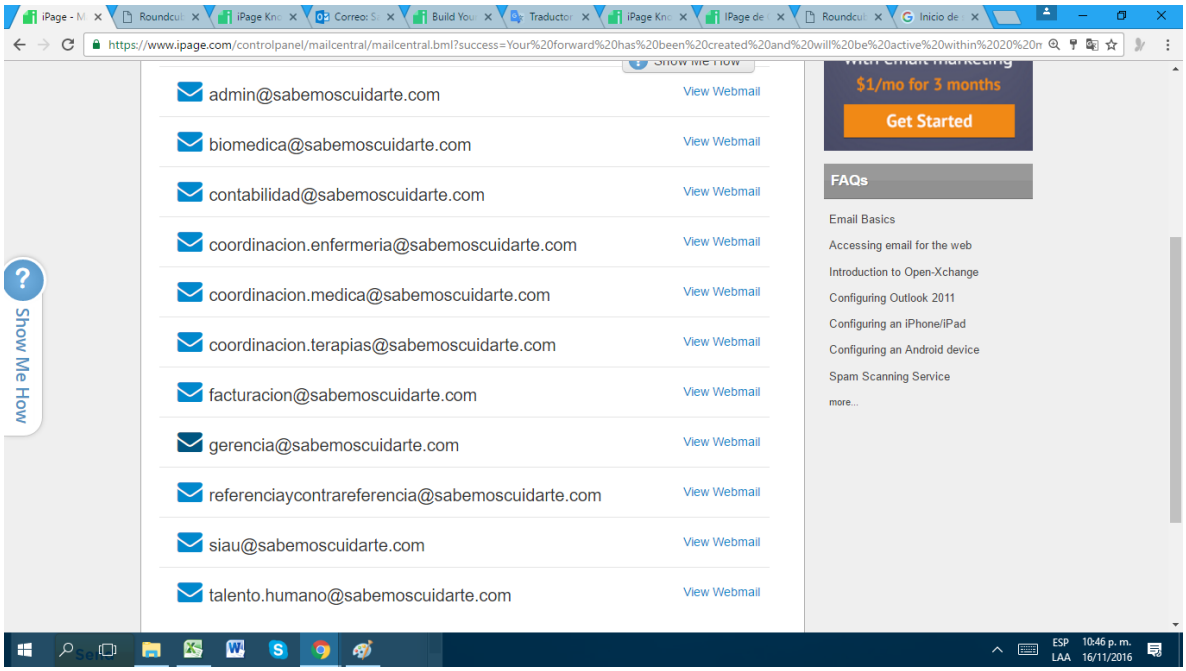
- Se utiliza una única cuenta fscuidarte@hotmail.com que es donde llega casi el 100% de la información de la entidad y la persona que administra esta cuenta redirección los casos al funcionario(s) responsable(s) que son su cuentas de correos personales (ver anexos de las hojas de vida de los equipos de computo).
- Se evidencia el uso de las cuentas personales de los funcionarios para actividades de la empresa.
- Con el proveedor Ipage se tiene creadas aproximadamente 50 cuentas de correo institucionales, pero se puede comprobar que absolutamente nadie de la entidad conocía o sabia de las mismas y además muchas de estas cuentas pertenecen a ex funcionarios de la entidad. (ver Figura 9. Cuentas de correo electrónico de Ipage viejas).
- Se gestiona con Ipage las claves de acceso al portal y se evidencia que estas cuentas fueron creadas pero nunca fueron utilizadas, por consiguiente y con autorización de la Gerencia se procede a eliminarlas y a crear nuevas cuentas pero con el nombre de la dependencia y se plantea la sugerencia que la Entidad empieza a utilizar estas cuentas (ver figura 10. Cuentas de correo electrónico nuevas).

Figura 9. Cuentas de correo electrónico de Ipage viejas



Fuente: Ipage

Figura 10. Cuentas de correo electrónico nuevas



Fuente: Ipage

10.2 HOJAS DE VIDA DE LOS EQUIPOS

Con la autorización de la Gerencia se procede a realizar la revisión de los equipos y se entrevista al Funcionario que lo utiliza donde se puede identificar entre otras las siguientes situaciones:

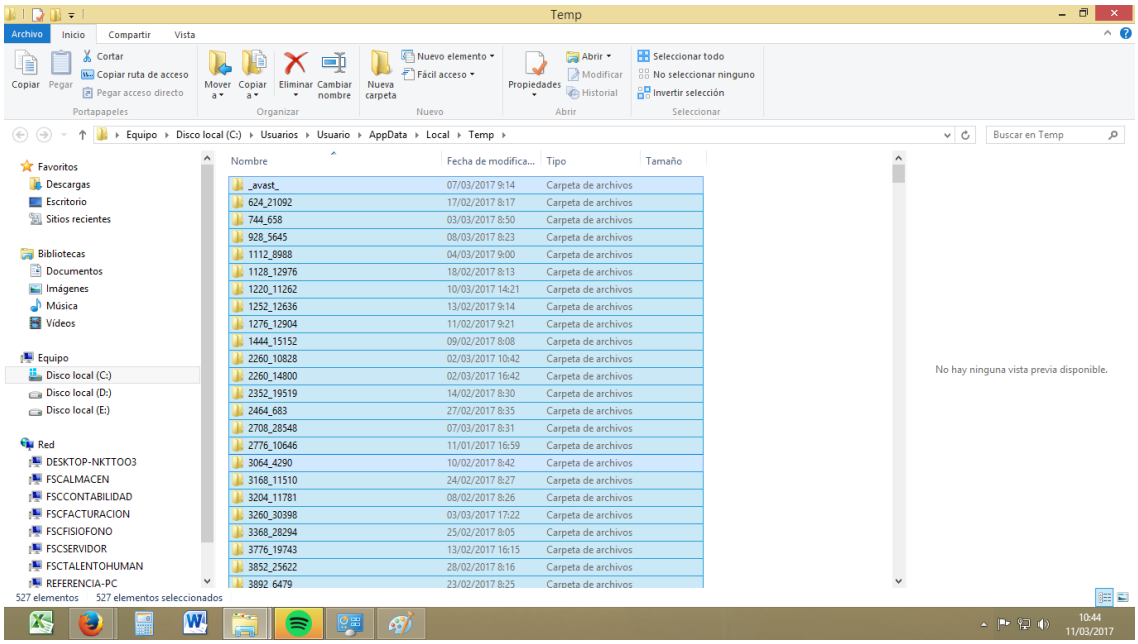
- Los equipos al ser prendidos no tiene asignado usuario y por consiguiente tampoco una clave de acceso, lo cual es muy delicado porque cualquier persona lo puede prender y extraer la información ahí contenida.
- No se observa una estandarización de los nombres de los equipos.
- No se tiene establecido un plan de mantenimiento de los equipos, ya que al preguntarles a los funcionarios que si sabían o se habían dado cuenta de cuando había sido la última vez que le habían hecho mantenimiento al equipo la respuestas fueron “la verdad no sé” y a la pregunta desde el momento en que tu entraste a trabajar a la Fundación y hasta la Fecha te has dado cuenta que a tu equipo le han hecho mantenimiento, la respuesta fue “No”.
- Al preguntar por las copias de seguridad de la información la respuesta fue “de vez en cuando vienen con un disco duro externo y hacen las copias”, al preguntar por la periodicidad de las mismas la respuesta fue “muy de vez en cuando” y al preguntar quién hacia las copias y donde se guardaba el disco duro las respuestas fueron “las hace el Gerente y creo que el guarda el disco en su escritorio”.
- Al preguntar por la clave de acceso al internet se pudo determinar que esta clave es de “acceso público” ya que todos los funcionarios la conocían.
- Al preguntar y al acceder al servicio de internet se pudo determinar que no existe ningún tipo de restricciones y los funcionarios pueden acceder a todo tipo de páginas web.
- Al preguntar si se tiene algún formato de hoja de vida de los equipos de cómputo se pudo determinar que no existe, se procede a diseñar y poner en consideración de la Gerencia un formato, el cual es aprobado y es utilizado para realizar el levantamiento de las hojas de vida de los equipos.

Las hojas de vida de los equipos de cómputo de la Fundaciòn pueden ser revisadas en los anexos del prsente documento.

Algunos datos que se pueden considerar relevantes al momento de realizar el “levantamiento” de la información de los equipos de cómputo:

- Talento Humano: el uso principal de este equipo es llevar un control en un archivo en Excel de los cuadros de turnos del personal, un control en términos de contratación de personal y la expedición de certificados laborales (ver Anexo 1. Hoja de vida equipo Talento Humano), al realizar la revisión del contenido de la carpeta Temp de este equipo se pudo identificar que dicha carpeta contenia un total de 527 elementos (ver Figura 11. Información carpeta temp equipo de talento humano).

Figura 11. Información carpeta temp equipo de talento humano

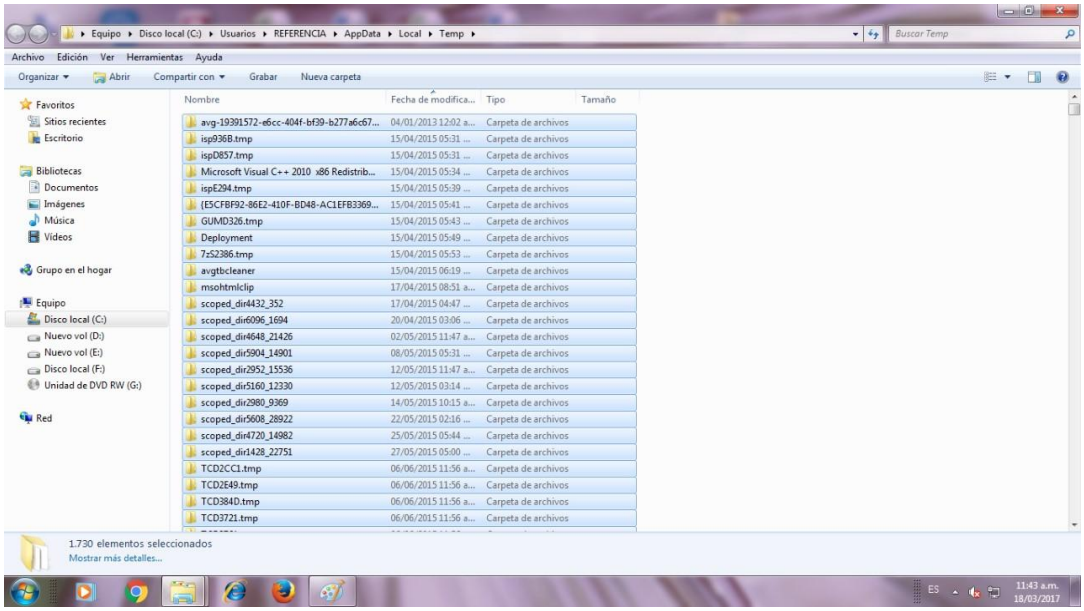


Fuente: Fundación Sabemos Cuidarte

- Referencia: el uso de este equipo esta dado para la recepción y envio de correos electrónicos en procesos de referencia y contrareferencia de pacientes, la elaboración y radicación de comités técnicos científicos (ver Anexo 2. Hoja de vida equipo referencia), al realizar la revisión del contenido de la carpeta Temp de este equipo se pudo identificar que dicha

carpeta contenia un total de 1730 elementos (ver Figura 12. Información carpeta temp equipo de referencia).

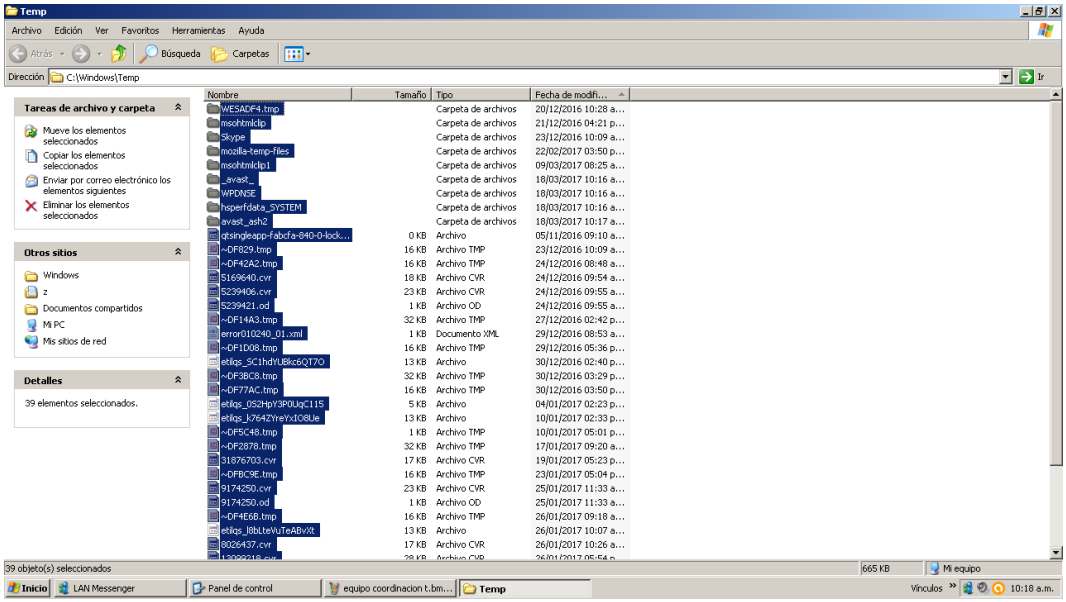
Figura 12. Información carpeta temp del equipo de Referencia



Fuente: Fundación Sabemos Cuidarte

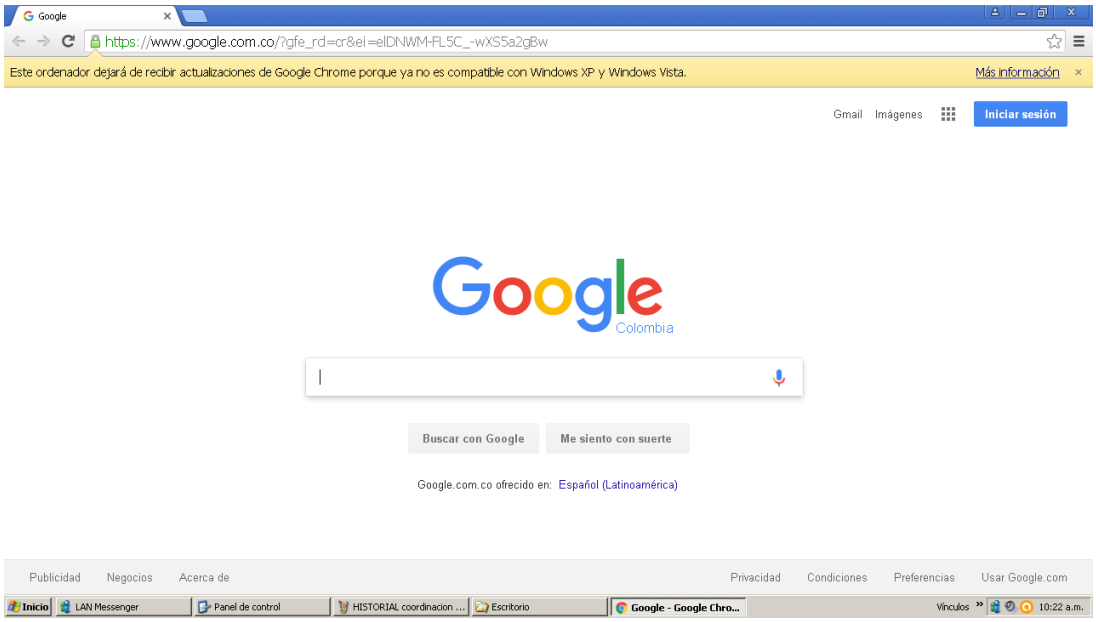
- Coordinación de Terapistas: el uso principal de este equipo es llevar un control en un archivo en Excel de los cuadros de turnos del personal de terapistas, un control en términos de contratación y un control en términos de los pagos realizados y pendientes por realizar a los Terapistas (ver Anexo 3. Hoja de vida equipo coordinación de terapista), al realizar la revisión del contenido de la carpeta Temp de este equipo se pudo identificar que dicha carpeta contenia un total de 39 elementos (ver Figura 13. Información temp del equipo de coordinación de terapistas), como también se pudo determinar la obsolencia del navegador utilizado bajo el sistema operativo Windows xp (ver Figura 14. Error en navegador del equipo coordinación de terapistas).

Figura 13. Información temp del equipo de coordinación de terapistas



Fuente: Fundación Sabemos Cuidarte

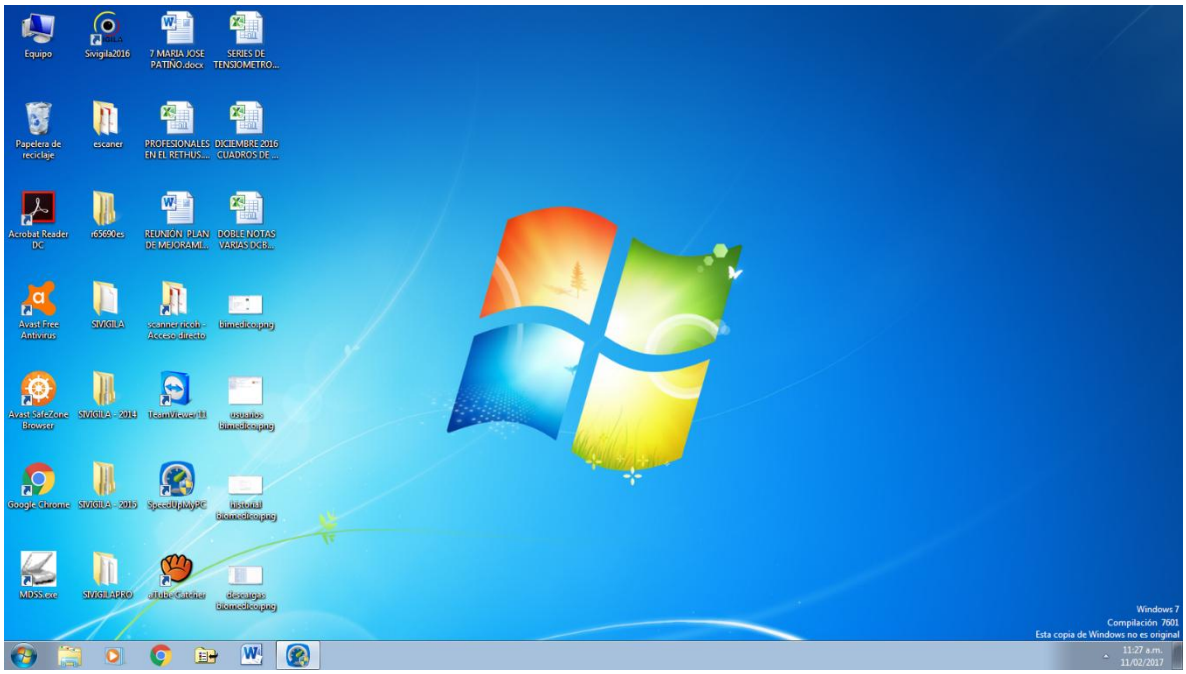
Figura 14. Error en navegador del equipo coordinación de terapistas



Fuente: Fundación Sabemos Cuidarte

- Biomédico: este equipo es utilizado principalmente para llevar un registro y control de las hojas de vida de los equipos biomédicos con los cuales cuenta la Fundación (ver Anexo 4. Hoja de vida equipo Biomedico), de este equipo lo que mas llama la atención es el mensaje que se observa en el escritorio y cual esta asociado con la NO originalidad de la licencia del sistema operativo (ver Figura 15. Error en licenciamiento de Windows 7).

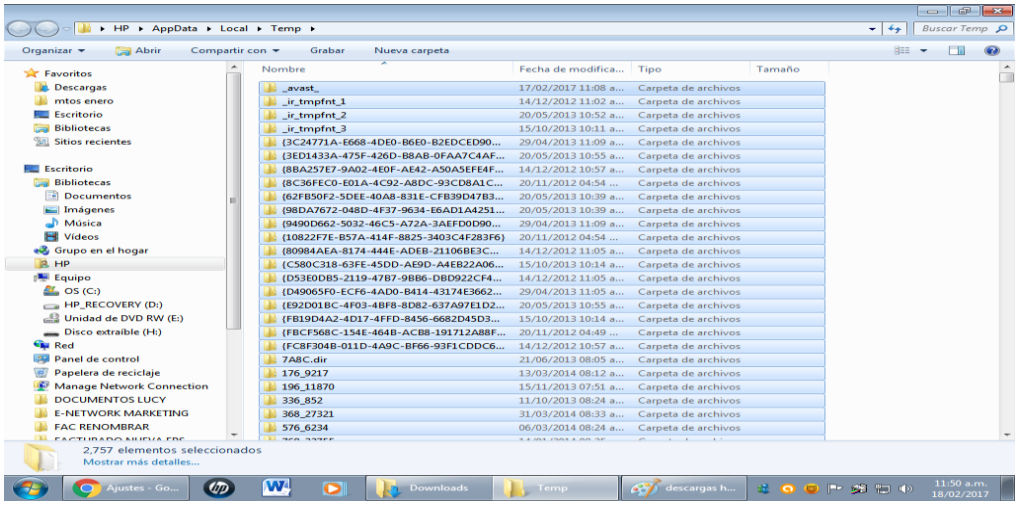
Figura 15. Error en licenciamiento de Windows 7



Fuente: Fundación Sabemos Cuidarte

- Historias Clínicas: este equipo es utilizado principalmente para llevar un registro y control de todas las historias clínicas de los pacientes que son atendidos por parte de la Fundación (ver anexo 5. Hoja de vida equipo HC), al realizar la revisión del contenido de la carpeta Temp de este equipo se pudo identificar que dicha carpeta contenia un total de 2757 elementos (ver Figura 16. Información carpeta temp equipo HC).

Figura 16. Información carpeta temp equipo HC



Fuente: Fundación Sabemos Cuidarte

- Coordinación de Enfermería: el uso principal de este equipo es llevar un control en un archivo en Excel de los cuadros de turnos del personal de auxiliares de enfermeria, un control en términos de contratación y un control en términos de los pagos realizados y pendientes por realizar a los auxiliares de enfermeria (ver Anexo 6. Hoja de vida equipo coordinación de enfermeria).

- Contabilidad: el uso principal de este equipo es el registro de la información contable de la Fundación (ver Anexo 7. Hoja de vida equipo contabilidad). Se pudo evidenciar que el aplicativo Delta utilizado para el registro de la información contable de la Entidad maneja un sistema de control de acceso con usuario y contraseña.

- Facturación: el uso principal de este equipo es realizar el proceso de facturación de los servicios prestados a los usuarios de las EPS con las cuales se tiene contrato (ver Anexo 8. Hoja de vida equipo facturación). Se pudo evidenciar que el aplicativo EMRIPs utilizado para el proceso de

Facturación de la Entidad maneja un sistema de control de acceso con usuario y contraseña.

- Gerencia: el uso principal de este equipo es la revisión permanente del sistema de correos electrónicos, además es utilizado en algunas ocasiones para realizar transacciones en línea con la Entidad Financiera y la expedición de algunos certificados (ver Anexo 9. Hoja de vida equipo gerencia).

10.3 LICENCIAMIENTO

La Entidad cuanta en este momento con los siguientes CD Originales en cuanto a licenciamiento:

Tabla 1. Licenciamiento de software

Nombre	Tipo		Serie	Observación	
OFFICE HOGAR Y ESTUDIANTES 2010	ORIGINAL		7WFJK-XXXXX-VKMCF-XXXXX-FVTPJ	3 EQUIPOS DOMESTICOS, PROHIBIDO SU USO EN ACTIVIDADES COMERCIALES	
OFFICE HOGAR Y PEQUEÑA EMPRESA 2010	ORIGINAL	6000139879-7-995285-SLOU		LICENCIA PARA USO NO COMERCIAL EN UN MAXIMO DE 3 EQUIPOS PERSONALES	
OFFICE HOGAR Y PEQUEÑA EMPRESA 2010	ORIGINAL	6000139879-7-995285-SLOU	BW2HW-XXXXX-9RC6X-XXXXX-DTHQ3	LICENCIA PARA USO NO COMERCIAL EN UN MAXIMO DE 3 EQUIPOS PERSONALES	
WINDOWS 7 PROFESIONAL	ORIGINAL		XXXXX-PY3JH-6J6H6-XXXXX-8DB4H	NA	
WINDOWS 7 PROFESIONAL	ORIGINAL		XXXXX-MGQX7-BTYTR-XXXXX-H9WXH	NA	

DELTA	ORIGINAL		01-XXXXX-C-2XXX4	NA

Fuente: Fundación Sabemos Cuidarte

En el momento los equipos de cómputo ubicados en Historias Clínicas y Enfermera Jefe son los únicos que cuentan con el sticker que garantizan la originalidad de sus sistemas operativos, los demás equipos no cuentan con este sticker y al consultar si se tienen las licencias disponibles de alguna otra manera y ninguno de los funcionarios da razón al respecto.

Además llama la atención que al revisar la información del licenciamiento del office en las cajas con la información de las licencias de las cajas ninguna de ella coinciden.

10.4 RACK DE COMUNICACIONES

Al realizar la inspección del rack de comunicaciones de la Fundación se obtiene la siguiente información:

En el momento se cuenta con una Router marca Arris TG-862 (ver Figura 17. Router) el cual tiene en otras las siguientes características:

Interfaces

- Interfaz RF: conector F.
- Interfaces de datos: Ethernet base-T 4 x 10/100/1000 (conector RJ-45).
- Interfaz de voz: 2 líneas; RJ-14 ("línea 1/2"), RJ-11 ("línea 2").
- Interfaz USB; USB 2.0.

Wi-Fi

- 802.11b/g/n.
- Radio 802.11n 2x2 de 2.4GHz.
- Opciones WPA2™ personales y para empresas, WEP de 64/ 128 bits y autenticación de seguridad inalámbrica MAC.
- WMM® QOS, y WMM Power Save.

Figura 17. Router

Fuente: Fundación Sabemos Cuidarte

Dentro del rack se pueden visualizar dos Switch así:

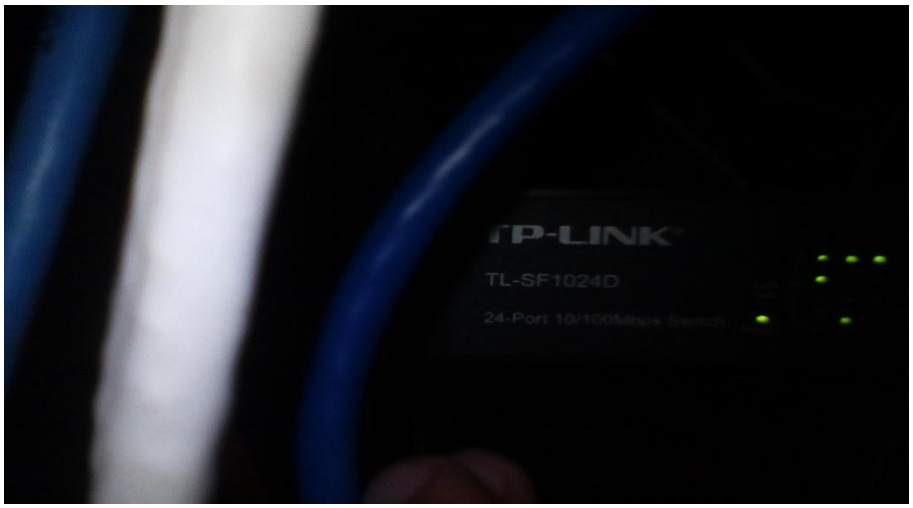
- Marca TP LINK de 16 puertos modelo TL-SG1016 (ver Figura 18. Switch 16 puertos).

Figura 18. Switch 16 puertos

Fuente: Fundación Sabemos Cuidarte

- Marca TP LINK de 24 puertos modelo TL-SF1024D (ver Figura 19. Switch 24 puertos).

Figura 19. Switch 24 puertos

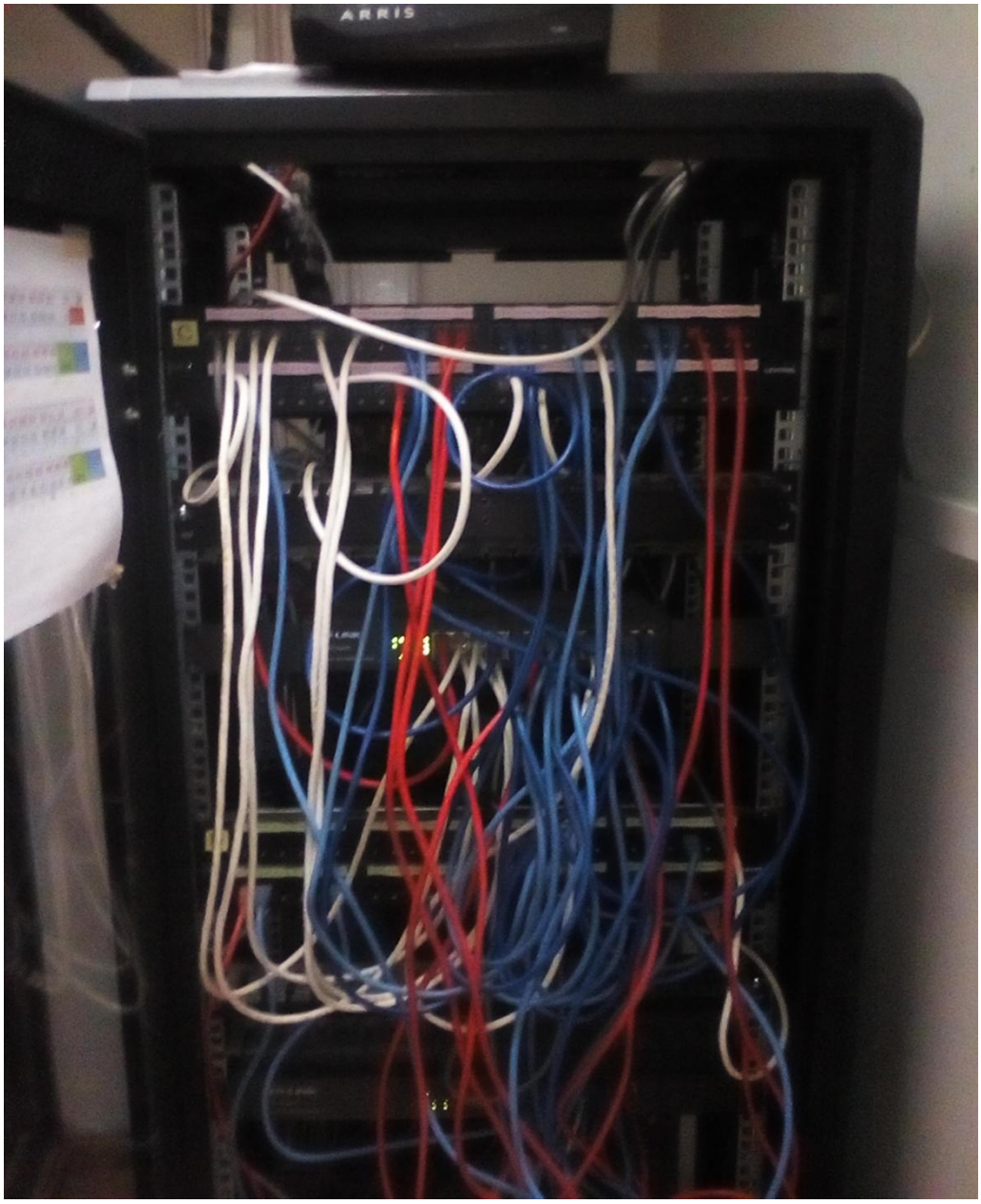


Fuente: Fundación Sabemos Cuidarte

Estos equipos y todo su cableado se encuentra dentro de un armario metálico (ver figura 20. Rack), el cual al momento de la revisión se encuentra sin llave y la ubicación del mismo es un sitio abierto al público, muy cerca de un baño público,

lo que se convierte en un riesgo ya que cualquier persona podría acceder al cableado y/o a los equipos aquí instalados.

Figura 20. Rack



Fuente: Fundación Sabemos Cuidarte

Además como se puede observar en la Figura anterior no se maneja un estándar en los colores del cableado, por ejemplo: los azules para habilitar los puntos de datos y los rojos para puntos de voz. Esta puede ser una buena opción teniendo

en cuenta que dentro de la organización no existe un funcionario con conocimientos en el área de sistemas y con un simple estándar como el planteado puede darse orientaciones que en un determinado momento los lleve a la solución de algún pequeño problema.

10.5 REDES ELECTRICAS

Aunque la Fundación cuenta con todo un tendido en canaleta metálica para su red de datos y energía regulada, se evidencia que hacen falta que la Entidad realice una inversión en términos en equipos de respaldo en términos de fluido eléctrico, como por ejemplo UPS y baterías o una planta electrica, teniendo en cuenta que en el momento no se cuentan con ellas y cuando el fluido eléctrico se va se corren dos riesgos muy significativos la perdida de información y/o el daño de los equipos.

Además preocupa el hecho de que algunas de las cajas del sistema de cableado de datos y/o de energía se encuentran sueltos, inseguros y otros hasta pegados con cinta (ver Figura 21. Tomacorrientes).

Figura 21. Tomacorrientes

Fuente: Fundación Sabemos Cuidarte

Otra situación que llama mucho la atención es que todos los equipos de cómputo se conectan a la red regulada de energía mediante los denominados “cortapicos” o “multitomas” (ver Figura 22. Cortapicos).

Figura 22. Cortapicos

Fuente: Fundación Sabemos Cuidarte

10.6 ANÁLISIS DE LA INFORMACIÓN

- No fue posible realizar la identificación del Proveedor y la fecha de compra de los equipos de cómputo, al requerir esta información al funcionario que se desempeña como Auxiliar Contable no fue posible su identificación en el sistema de información.
- La Entidad inicialmente no contaba con hojas de vida de los equipos de cómputo, se diseña y se recolecta la información de los equipos de cómputo.

- No es posible establecer la fecha del último mantenimiento de los equipos de cómputo, con lo cual se puede determinar que la Entidad no cuenta con un cronograma o programa de mantenimientos preventivos. Al requerir esta información al funcionario que se desempeña como Auxiliar Contable no fue posible su identificación en el sistema de información y al realizar la pregunta al funcionario responsable del equipo la respuesta generalizada fue “de lo que llevo aquí nunca le han hecho mantenimiento preventivo al equipo, solamente cuando se daña o molesta”.
- Por la falta de mantenimiento se pueden observar que existen muchos archivos almacenados en la carpeta de temporales, de igual manera sucede al revisar el historial del navegador (ver Figura 3. Elementos en carpeta Temp y ver Figura 4. Elementos en el histaorial del navegador).
- Llama mucho la atención que existen varios antivirus instalados en los equipos (avg, avast, Microsoft security), en su versión Free, lo cual ofrece una protección básica, motivo por el cual existen problemas de virus en algunos equipos (vert Figura 2. Antivirus).
- Con relación al licenciamiento del software utilizado en la entidad se tiene lo siguiente:
    - Sistema Operativo: solamente dos (2) equipos tienen la etiqueta o sello que garantizan la originalidad y se encuentran adheridas a la CPU, además se cuentan con dos (2) cd originales de Windows 7 profesional.
    - Office: todos los equipos cuentan con office instalado, pero llama la atención que los cd originales hacen referencia a office 2010 e instalado se encuentra office 2007, además existe una licencia que para la entidad no sirve ya que la etiqueta está marcada para Hogar y Estudiantes.
    - Delta: cuenta con su licencia, pero se debe revisar el tema de la actualización para dar cumplimiento a los requerimientos de presentar la información según las Normas Internacionales - NIIF
    - EMRIPS: no fue posible determinar si este software está debidamente licenciado.
    - Windows XP: existe un equipo que a la fecha está funcionando con Windows xp, sistema operativo al cual el soporte sin Service Pack finalizó el 30 de septiembre de 2004, el Soporte de Service Pack 1 finalizó el 10 de octubre de 2006 y el soporte de Service Pack 2 se retiró el 13 de julio de 2010, 6 años después de su disponibilidad general.

- Kmspico: existe un equipo en el cual se identificó este programa el cual es utilizado para hacer activaciones de software no original (ver Anexo 1. Hoja de Vida equipo Talento humano).
- Spotify: en algunos equipos de cómputo se encontró instalado este programa el cual sirve para la reproducción de música en línea (ver Anexo 1. Hoja de Vida equipo Talento humano)..

- Según la información obtenida la Entidad no ha hecho procesos de depreciaciones de sus activos como tampoco de dar de baja contablemente los activos que han sido dados de baja.

- No se puede establecer o identificar que la Entidad y/o sus funcionarios realizan procesos de copias de seguridad de la información.

10.7 INVENTARIO CONSOLIDADO

Una vez recolectada y analizada toda la información correspondiente al inventario hardware y software de la Fundación Sabemos Cuidarte se presente un informe consolidado del mismo de la siguiente manera:

Tabla 2. Inventario Consolidado

Dependencia	Tipo	Cantidad	Conexión	Finalidad
GERENCIA	PORTATIL	1	INALAMBRICA	Revisión correo electrónico Algunos pagos en línea Revisión de informes
REFERENCIA	DE MESA	1	ALAMBRICA	Revisión correo electrónico Reporte del sivigila Radicar mipres Revisar informes
REFERENCIA	IMPRESORA	1	ALAMBRICA	Impresión de mipres
COORDINACION DE TERAPISTAS	DE MESA	1	ALAMBRICA	Revisión correo electrónico Revisar informes
BIOMEDICO	DE MESA	1	ALAMBRICA	Revisión correo electrónico Inventario de equipos biomédicos
HISTORIAS CLINICAS	DE MESA	1	ALAMBRICA	Revisión correo electrónico Inventario físico de HC
COORDINACION DE ENFERMERIA	PORTATIL	1	INALAMBRICA	Revisión correo electrónico Revisar informes

Dependencia	Tipo	Cantidad	Conexión	Finalidad
CONTABILIDAD	DE MESA	1	ALAMBRICA	Registro de información contable Elaborar formatos DIAN Revisión correo electrónico Revisión informes
FACTURACION	DE MESA	1	ALAMBRICA	Elaborar la facturación para las diferentes EPS Revisión correo electrónico Revisar informes
TALENTO HUMANO	DE MESA	1	ALAMBRICA	Revisar correo electrónico Publicar vacantes Revisar informes
IMPRESORA RICOH MULTIFUNCIONAL		1	ALAMBRICA	Es una impresora para toda la entidad también usada para escanear también usada para fotocopiar

Fuente: Fundación Sabemos Cuidarte

10.8 IDENTIFICACION DE ACTIVOS

Los activos identificados son:

Tabla 3. Identificación de Activos

Tipo de activo	Activo
[D] Datos/Información	[int] datos de gestión interna
	[password] contraseñas ,aplicación web
	[auth] datos de validación de credenciales
[SW] Software	[BROWSER] Navegador web
	[APP] Aplicación web
	[OFFICE] Ofimática
	[AV] Anti virus
	[OS] Sistema operativo
[HW] Equipamiento informático	[IPPHONE] teléfono
	[PC] Computadores de mesa

Tipo de activo	Activo
	[PC] Computadores portátiles
	[PRINT] Impresora de soporte
	[LAN] Cableado red de área local
	[SWITCH] Switch
[COM] Redes de comunicaciones	[WIFI] red inalámbrica
	[INT] Internet
	[PSTN] Red telefónica
	[LAN] Red local
[Media] Soportes de información	[NON_ELECTRONIC] no electrónicos
	[PRINTED] Material impreso. informes
[L] Instalaciones	[OFI] Oficina
[P] Personal	[UI] Usuarios internos

Fuente: Fundación Sabemos Cuidarte

10.9 VALORACION DE LOS ACTIVOS

La tabla de valores para la valoración de los activos es:

Tabla 4. Valoración de los Activos

Nivel	Criterio
10	Alto
9	Alto
8	Alto
7	Alto
6	Medio
5	Medio
4	Medio

3	Bajo
2	Bajo
1	Bajo
0	Depreciable

Fuente: Fundación Sabemos Cuidarte

Las Dimensiones Establecidas son:

Tabla 5. Dimensiones

Sigla	Dimensión
[D]	Disponibilidad
[I]	Integridad de Datos
[C]	Confidencialidad de los datos
[A]	Autenticidad de los usuarios e información
[T]	Trazabilidad de los datos y del servicio

Fuente: Fundación Sabemos Cuidarte

Ahora se presenta una valoración de los activos por cada una de las dimensiones.

Tabla 6. Valoración de activos por Dimensión

	Dimensiones				
Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servicios internos					
Internet	[9]			[9]	[9]
Aplicaciones					
Aplicación web	[8]			[8]	[7]
Antivirus					[8]
Sistema Operativo					[8]

Sistema de Información	[9]	[9]	[9]	[9]	[9]
Equipos					
Medios de Impresión					[6]
Computadores de escritorio					[8]
Modem					[8]
Computadores portátiles					[8]
Comunicaciones					
Telefonía	[8]	[7]			[7]
Red WIFI					[8]
Internet		[9]	[9]		
Soportes de Información					
Documentación digital de procesos		[8]	[8]		
Documentación digital del Sistema de Información		[8]	[8]		
Informes en digital y físico		[8]	[8]		
Equipamiento Auxiliar					
conexión wi-fi	[7]				
Instalaciones					
Oficina			[8]		
Personal					
Gerente			[8]		
Coordinador Terapistas			[8]		

Coordinador de Enfermería			[8]		
Auxiliar de Talento Humano			[7]		
Auxiliar de Referencia			[7]		
Biomédico			[7]		
Auxiliar de Historias Clínicas			[7]		
Auxiliar de Contabilidad			[7]		
Auxiliar de Facturación			[7]		

Fuente: Fundación Sabemos Cuidarte

10.10 CARACTERIZACION E IDENTIFICACION DE LAS AMENAZAS

Teniendo en cuenta la información contenida en la Metodología Magerit y en donde se clasifican las amenazas en:

Tabla 7. Amenazas

Sigla	Descripción
[N]	Desastres Naturales
[I]	De origen Industrial
[A]	Ataques Intencionados
[E]	Errores y fallos no intencionados

Fuente: Metodología Magerit [1]

En primera medida se identifican las posibles amenazas a los cuales se pueden ver abocados los activos así:

[1] Magerit Versión 3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de Elementos. Disponible en el enlace https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WhtV40rXbIU

Tabla 8. Amenazas por Activos

Activos	Amenazas
Computadores portátiles	[N.2] Daños por agua
	[I.8] Fallo de servicios de comunicaciones
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperaturas o humedad
	[I.10] Degradación de los soportes de almacenamiento de la información
	[E.14] Escapes de información.
	[E.23] Errores de mantenimiento, actualización de equipos hardware
	[E.25] Pérdida de equipos
	[A.22] Manipulación de programas.
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.23] Manipulación de los equipos.
	[I.6] suministro eléctrico
Computadores de mesa	[N.2] Daños por agua
	[I.8] Fallo de servicios de comunicaciones
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperaturas o humedad
	[I.10] Degradación de los soportes de almacenamiento de

Activos	Amenazas
	la información
	[E.14] Escapes de información.
	[E.23] Errores de mantenimiento, actualización de equipos hardware
	[E.25] Pérdida de equipos
	[A.22] Manipulación de programas
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[I.6] suministro eléctrico
	[A.23] Manipulación de los equipos.
Sistema de Información	[E.1] Errores de los usuarios
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades del programa (software)
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)
	[A.7] Uso no previsto
	[A.24] Denegación de servicios
	[A.11] Acceso no autorizado
	[A.6] Abuso de privilegios de acceso
Antivirus	[E.8] Difusión de software dañino

Activos	Amenazas
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)
Sistema Operativo	[I.5] Avería de origen físico o lógico
	[E.1] Errores de los usuarios
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)
	[A.7] Uso no previsto
Aplicación web	[E.1] Errores de los usuarios
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades del programa (software)
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)
	[A.7] Uso no previsto
	[A.24] Denegación de servicios
	[A.11] Acceso no autorizado
	[A.6] Abuso de privilegios de acceso
Impresoras	[I.5] Avería de origen físico o lógico

Activos	Amenazas
	[I.7] Condiciones inadecuadas de temperaturas o humedad
	[E.23] Errores de mantenimiento, actualización de equipos hardware
	[I.6] suministro eléctrico
	[A.11] Acceso no autorizado
Router	[N.1] Fuego
	[N.2] Daños por agua
	[I.6] suministro eléctrico
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperaturas o humedad
	[A.11] Acceso no autorizado
	[A.4] Errores de configuración
Telefonía	[A.11] Acceso no autorizado
	[I.6] suministro eléctrico
Red WIFI	[I.4] Fallo de servicios de comunicaciones
	[E.8] Errores de re-encaminamiento
INTERNET	[I.8] Fallo de servicios de comunicaciones
	[E.15] Alteración de la información
Documentación digital de	[A.11] Acceso no autorizado
	[E.15] Alteración de la información

Activos	Amenazas
procesos.	[A.15] Modificación de la información
	[A.25] Robo de la información
Documentación digital del Sistema de Información.	[A.11] Acceso no autorizado
	[E.15] Alteración de la información
	[A.15] Modificación de la información
	[A.25] Robo de la información
Informes en digital y físico	[A.11] Acceso no autorizado
	[E.15] Alteración de la información
	[A.15] Modificación de la información
	[A.25] Robo de la información
Oficina	[N.1] Fuego
	[N.2] Daños por agua
	[.*] Desastres naturales.
	[A.27] Ocupación enemiga
Gerente	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Coordinación de Terapistas	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social

Activos	Amenazas
Coordinación de Enfermería	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Auxiliar Talento Humano	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Auxiliar de Referencia	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Biomédico	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Auxiliar de Historias clínicas	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Auxiliar de contabilidad	[E.28] indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería Social
Auxiliar de Facturación	[E.28] indisponibilidad del personal
	[A.29] Extorsión

Activos	Amenazas
	[A.30] Ingeniería Social

Fuente: Fundación Sabemos Cuidarte

10.11 VALORACION DE LAS AMENAZAS

Para poder realizar el proceso de valoración de las amenazas se hace indispensable establecer una tabla que nos permita realizar la posible medición del daño:

Tabla 9. Medición del daño

Valor	Descripción	
100%	MA	Muy alta
80%	A	Alta
50%	M	Media
20%	B	Baja
10%	MB	Muy baja

Fuente: Metodología Magerit.[2]

Luego debemos determinar la frecuencia con la cual se puede presentar el daño:

Tabla 10. Frecuencia del daño

Valor	Descripción		
100	MF	Muy frecuente	A diario
10	F	Frecuente	Mensualmente

[2] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro i – Método. Disponible en el enlace https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

1	N	Normal	Una vez al año
1/10	P	Poco	Cada varios años
1/100	MP	Muy poco frecuente	Siglos

Fuente: Metodología Magerit [2].

Una vez establecida esta información se procede a cuantificar el posible daño y lo que esto le puede producir a la Entidad en el caso de que se presente, para ello se elaboraba una tabla que contiene la valoración de las amenazas:

Tabla 11. Valoración de las amenazas

Activos	**Amenazas**	**frecuencia**	**D**	**I**	**C**	**A**	**T**
Computadores portátiles	[N.2] Daños por agua	MP	A				
	[I.8] Fallo de servicios de comunicaciones	P	A				
	[I.5] Avería de origen físico o lógico	N	A				
	[I.7] Condiciones inadecuadas de temperaturas o humedad	P	A				
	[I.10] Degradación de los soportes de almacenamiento de la información	P	A	M	M		
	[E.14] Escapes de información.	P	A	M	M		
	[E.23] Errores de mantenimiento, actualización de equipos hardware	N	A				
	[E.25] Pérdida de equipos	P	A				

Activos	Amenazas	frecuencia	D	I	C	A	T
	[A.22] Manipulación de programas.	P	A		M		
	[A.6] Abuso de privilegios de acceso	P	A	M	M		
	[A.7] Uso no previsto	P	A	M	M		
	[A.23] Manipulación de los equipos.	P	A		M		
	[I.6] suministro eléctrico	P	A				
Computadores de mesa	[N.2] Daños por agua	MP	A				
	[I.8] Fallo de servicios de comunicaciones	P	A				
	[I.5] Avería de origen físico o lógico	N	A				
	[I.7] Condiciones inadecuadas de temperaturas o humedad	P	A				
	[I.10] Degradación de los soportes de almacenamiento de la información	P	A	M	M		
	[E.14] Escapes de información.	P	A	M	M		
	[E.23] Errores de mantenimiento, actualización de equipos hardware	N	A				
	[E.25] Pérdida de equipos	P	A				

Activos	Amenazas	frecuencia	D	I	C	A	T
	[A.22] Manipulación de programas.	P	A		M		
	[A.6] Abuso de privilegios de acceso	P	A	M	M		
	[A.7] Uso no previsto	P	A	M	M		
	[I.6] suministro eléctrico	P	A				
	[A.23] Manipulación de los equipos.	P	A		M		
Sistema de Información	[E.1] Errores de los usuarios	P	A	M	M		
	[E.8] Difusión de software dañino	P	A	A	A		
	[E.20] Vulnerabilidades del programa (software)	P	M	M	M		
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	N	A				
	[A.7] Uso no previsto	P	A	M	M		
	[A.24] Denegación de servicios	P	M	M	M		
	[A.11] Acceso no autorizado	P	A	M	M		
	[A.6] Abuso de privilegios de acceso	P	A	M	M		
Antivirus	[E.8] Difusión de software dañino	P	M	M	M		

Activos	Amenazas	frecuencia	D	I	C	A	T
	[E.20] Vulnerabilidades de los programas (software)	P	M	M	M		
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	N	A				
Sistema Operativo	[I.5] Avería de origen físico o lógico	P	A	M	M		
	[E.1] Errores de los usuarios	P	A	M	M		
	[E.8] Difusión de software dañino	P	A	A	A		
	[E.20] Vulnerabilidades de los programas (software)	P	M	M	M		
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	N	A				
	[A.7] Uso no previsto	P	A				
Aplicación web	[E.1] Errores de los usuarios	P	A	M	M		
	[E.8] Difusión de software dañino	P	A	A	A		
	[E.20] Vulnerabilidades del programa (software)	P	M	M	M		
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	N	A				

Activos	Amenazas	frecuencia	D	I	C	A	T
	[A.7] Uso no previsto	P	A				
	[A.24] Denegación de servicios	P	A	M	M		
	[A.11] Acceso no autorizado	P	A	M	M		
	[A.6] Abuso de privilegios de acceso	P	A	M	M		
Impresoras	[I.5] Avería de origen físico o lógico	P	A	M	M		
	[I.7] Condiciones inadecuadas de temperaturas o humedad	P	A				
	[E.23] Errores de mantenimiento, actualización de equipos hardware	P	A	M	M		
	[I.6] suministro eléctrico	p	A				
	[A.11] Acceso no autorizado	P	A	M	M		
Router	[N.1] Fuego	P	A				
	[N.2] Daños por agua	P	A				
	[I.5] Avería de origen físico o lógico	P	A	M	M		
	[I.7] Condiciones inadecuadas de temperaturas o humedad	P	A				
	[A.11] Acceso no autorizado	P	A	M	M		
	[E.4] Errores de configuración	P	A	M	M		

Activos	Amenazas	frecuencia	D	I	C	A	T
Telefonía	[A.11] Acceso no autorizado	P	A	M	M		
	[I.6] suministro eléctrico	P	A				
Red WIFI	[I.4] Fallo de servicios de comunicaciones	P	A	A	M		
	[E.8] Errores de re-encaminamiento	P	A	M	M		
INTERNET	[I.8] Fallo de servicios de comunicaciones	P	A	A	M		
	[E.15] Alteración de la información	P	A	M	M		
Documentación digital de procesos.	[A.11] Acceso no autorizado	P	A	A	A		
	[E.15] Alteración de la información	P	A	A	A		
	[A.15] Modificación de la información	P	A	A	A		
	[A.25] Robo de la información	P	A	M	M		
Documentación digital del Sistema de Información.	[A.11] Acceso no autorizado	P	A	A	A		
	[E.15] Alteración de la información	P	A	A	A		
	[A.15] Modificación de la información	P	A	A	A		
	[A.25] Robo de la información	P	A	M	M		

Activos	Amenazas	frecuencia	D	I	C	A	T
Informes en digital y físico	[A.11] Acceso no autorizado	P	A	A	A		
	[E.15] Alteración de la información	P	A	A	A		
	[A.15] Modificación de la información	P	A	A	A		
	[A.25] Robo de la información	P	A	M	M		
Oficina	[N.1] Fuego	P	A				
	[N.2] Daños por agua	P	A				
	[.*] Desastres naturales.	P	A				
	[A.27] Ocupación enemiga	P	A				
Gerente	[E.28] indisponibilidad del personal	P	M				
	[A.29] Extorsión	P	B	A	A		
	[A.30] Ingeniería Social	P	B	A	A		
Coordinación de Terapistas	[E.28] indisponibilidad del personal	P	M				
	[A.29] Extorsión	P	B	A	A		
	[A.30] Ingeniería Social	P	B	A	A		
Coordinación de Enfermerí	[E.28] indisponibilidad del personal	P	M				
	[A.29] Extorsión	P	B	A	A		

Activos	Amenazas	frecuencia	D	I	C	A	T
a	[A.30] Ingeniería Social	P	B	A	A		
Auxiliar Talento Humano	[E.28] indisponibilidad del personal	P	M				
	[A.29] Extorsión	P	B	A	A		
	[A.30] Ingeniería Social	P	B	A	A		
Auxiliar de Referencia	[E.28] indisponibilidad del personal	P	M				
	[A.29] Extorsión	P	B	A	A		
	[A.30] Ingeniería Social	P	B	A	A		
Biomédico	[E.28] indisponibilidad del personal	P	M				
	[A.29] Extorsión	P	B	A	A		
	[A.30] Ingeniería Social	P	B	A	A		
Auxiliar de Historias clínicas	[E.28] indisponibilidad del personal	P	M				
	[A.29] Extorsión	P	B	A	A		
	[A.30] Ingeniería Social	P	B	A	A		
Auxiliar de contabilidad	[E.28] indisponibilidad del personal	P	M				
	[A.29] Extorsión	P	B	A	A		
	[A.30] Ingeniería Social	P	B	A	A		

Activos	Amenazas	frecuencia	D	I	C	A	T
Auxiliar de Facturación	[E.28] indisponibilidad del personal	P	M				
	[A.29] Extorsión	P	B	A	A		
	[A.30] Ingeniería Social	P	B	A	A		

Fuente: Fundación Sabemos Cuidarte

10.12 VALORACION DEL RIESGO

Para poder llevar a cabo la valoración del riesgo se hace indispensable tener una tabla que contenga la descripción del posible riesgo:

Tabla 12. Valores del riesgo

Sigla	Descripción
MA	Crítico
A	Importante
M	Apreciable
B	Bajo
MB	Despreciable

Fuente: Fundación Sabemos Cuidarte

Ahora se establece una matriz de enlace entre el impacto y la probabilidad del riesgo:

Tabla 13. Matriz de riesgos

Riesgo		Probabilidad				
		MP	P	N	F	MF
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M

	MB	MB	MB	MB	B	B

Fuente: Fundación Sabemos Cuidarte

Tabla 14. Identificación de Riesgos

Activos	Amenazas	Probabilidad	Impacto	Riesgo
Computadores portátiles	[N.2] Daños por agua	P	A	A
	[I.8] Fallo de servicios de comunicaciones	MP	B	MB
	[I.5] Avería de origen físico o lógico	P	A	A
	[I.7] Condiciones inadecuadas de temperaturas o humedad	P	A	A
	[I.10] Degradación de los soportes de almacenamiento de la información	P	A	A
	[E.14] Escapes de información.	P	A	A
	[E.23] Errores de mantenimiento, actualización de equipos hardware	P	M	M
	[E.25] Pérdida de equipos	P	M	M
	[A.22] Manipulación de programas.	N	M	M
	[A.6] Abuso de privilegios de acceso	N	M	M
	[A.7] Uso no previsto	P	M	M
	[A.23] Manipulación de los equipos.	P	M	M
	[I.6] Suministro eléctrico	N	M	M

Activos	Amenazas	Probabilidad	Impacto	Riesgo
Computadores de mesa	[N.2] Daños por agua	N	M	M
	[I.8] Fallo de servicios de comunicaciones	P	M	M
	[I.5] Avería de origen físico o lógico	P	M	M
	[I.7] Condiciones inadecuadas de temperaturas o humedad	P	M	M
	[I.10] Degradación de los soportes de almacenamiento de la información	P	M	M
	[E.14] Escapes de información.	P	M	M
	[E.23] Errores de mantenimiento, actualización de equipos hardware	P	M	M
	[E.25] Pérdida de equipos	P	M	M
	[A.22] Manipulación de programas.	P	A	A
	[A.6] Abuso de privilegios de acceso	P	A	A
	[A.7] Uso no previsto	P	A	A
	[I.6] Suministro eléctrico	P	A	A
	[A.23] Manipulación de los equipos.	MP	A	M
Sistema de Informaci	[E.1] Errores de los usuarios	P	A	A
	[E.8] Difusión de software dañino	P	A	A

Activos	Amenazas	Probabilidad	Impacto	Riesgo
ón	[E.20] Vulnerabilidades del programa (software)	P	A	A
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	P	A	A
	[A.7] Uso no previsto	P	A	A
	[A.24] Denegación de servicios	N	A	A
	[A.11] Acceso no autorizado	N	A	A
	[A.6] Abuso de privilegios de acceso	P	A	A
Antivirus	[E.8] Difusión de software dañino	P	A	A
	[E.20] Vulnerabilidades de los programas (software)	N	A	A
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	N	A	A
Sistema Operativo	[I.5] Avería de origen físico o lógico	P	A	A
	[E.1] Errores de los usuarios	P	A	A
	[E.8] Difusión de software dañino	P	A	A
	[E.20] Vulnerabilidades de los programas (software)	P	A	A
	[E.21] Errores de mantenimiento / actualizaciones de programas	P	A	A

Activos	Amenazas	Probabilidad	Impacto	Riesgo
	(software)			
	[A.7] Uso no previsto	P	A	A
Aplicación web	[E.1] Errores de los usuarios	P	A	A
	[E.8] Difusión de software dañino	P	A	A
	[E.20] Vulnerabilidades del programa (software)	P	A	A
	[E.21] Errores de mantenimiento / actualizaciones de programas (software)	P	A	A
	[A.7] Uso no previsto	MP	A	M
	[A.24] Denegación de servicios	P	A	A
	[A.11] Acceso no autorizado	P	A	A
	[A.6] Abuso de privilegios de acceso	P	A	A
Impresoras	[I.5] Avería de origen físico o lógico	P	A	A
	[I.7] Condiciones inadecuadas de temperaturas o humedad	P	A	A
	[E.23] Errores de mantenimiento, actualización de equipos hardware	P	A	A
	[I.6] Suministro eléctrico	P	A	A
	[A.11] Acceso no autorizado	N	A	A
Router	[N.1] Fuego	N	A	A

Activos	Amenazas	Probabilidad	Impacto	Riesgo
	[N.2] Daños por agua	P	A	A
	[I.5] Avería de origen físico o lógico	P	A	A
	[I.7] Condiciones inadecuadas de temperaturas o humedad	N	A	A
	[A.11] Acceso no autorizado	N	A	A
	[E.4] Errores de configuración	P	A	A
Telefonía	[A.11] Acceso no autorizado	P	A	A
	[I.6] Suministro eléctrico	P	A	A
Red WIFI	[I.4] Fallo de servicios de comunicaciones	P	A	A
	[E.8] Errores de re-encaminamiento	P	A	A
INTERNET	[I.8] Fallo de servicios de comunicaciones	P	A	A
	[E.15] Alteración de la información	P	A	A
Documentación digital de procesos.	[A.11] Acceso no autorizado	P	A	A
	[E.15] Alteración de la información	P	A	A
	[A.15] Modificación de la información	P	A	A
	[A.25] Robo de la información	P	A	A
Document	[A.11] Acceso no autorizado	MP	A	M

Activos	Amenazas	Probabilidad	Impacto	Riesgo
ación digital del Sistema de Informaci ón.	[E.15] Alteración de la información	P	A	A
	[A.15] Modificación de la información	P	A	A
	[A.25] Robo de la información	P	A	A
Informes en digital y físico	[A.11] Acceso no autorizado	P	A	A
	[E.15] Alteración de la información	P	A	A
	[A.15] Modificación de la información	N	A	A
	[A.25] Robo de la información	P	A	A
Oficina	[N.1] Fuego	P	A	A
	[N.2] Daños por agua	P	A	A
	[.*] Desastres naturales.	P	A	A
	[A.27] Ocupación enemiga	P	A	A
Gerente	[E.28] indisponibilidad del personal	P	A	A
	[A.29] Extorsión	P	B	B
	[A.30] Ingeniería Social	P	B	B
Coordinac ión de Terapista s	[E.28] indisponibilidad del personal	P	A	A
	[A.29] Extorsión	P	B	B
	[A.30] Ingeniería Social	P	B	B
Coordinac	[E.28] indisponibilidad del personal	P	A	A

Activos	Amenazas	Probabilidad	Impacto	Riesgo
ión de Enfermería	[A.29] Extorsión	P	B	B
	[A.30] Ingeniería Social	P	B	B
Auxiliar Talento Humano	[E.28] indisponibilidad del personal	P	A	A
	[A.29] Extorsión	P	B	B
	[A.30] Ingeniería Social	P	B	B
Auxiliar de Referencia	[E.28] indisponibilidad del personal	P	A	A
	[A.29] Extorsión	P	B	B
	[A.30] Ingeniería Social	P	B	B
Biomédico	[E.28] indisponibilidad del personal	P	A	A
	[A.29] Extorsión	P	B	B
	[A.30] Ingeniería Social	P	B	B
Auxiliar de Historias clínicas	[E.28] indisponibilidad del personal	P	A	A
	[A.29] Extorsión	P	B	B
	[A.30] Ingeniería Social	P	B	B
Auxiliar de contabilidad	[E.28] indisponibilidad del personal	P	A	A
	[A.29] Extorsión	P	B	B
	[A.30] Ingeniería Social	P	B	B
Auxiliar de Facturaci	[E.28] indisponibilidad del personal	P	A	A
	[A.29] Extorsión	P	B	B

Activos	Amenazas	Probabilidad	Impacto	Riesgo
ón	[A.30] Ingeniería Social	P	B	B

Fuente: Fundación Sabemos Cuidarte

11. METODOLOGIA APLICADA

De acuerdo con la información aquí contenida, los riesgos identificados en cada uno de los ítems revisados, además de tener en cuenta que la Entidad eta en proceso de implementación del Sistema de Gestión de Calidad, se propone como metodología para el diseño del SGSI continuar en la misma línea y por consiguiente se opta por la metodología del Planear, Hacer, Verificar y Actuar (PHVA).

12. RECOMENDACIONES

12.1 DENTRO DEL PLANEAR

El planear es establecer una línea de acción y por consiguiente la Fundación debe:

- Elaborar y establecer un cronograma de mantenimiento preventivo donde se incluyan todos los equipos de cómputo y de comunicaciones y el cual debería realizarse como mínimo una vez al año.
- En compañía del contador de la Entidad establecer la vida útil de los equipos de cómputo y de esta manera proyectar un plan de renovación de los mismo.
- Proyectar la vinculación, bien sea por contrato o por prestación de servicios, de un Técnico, Tecnólogo o Ingeniero de Sistemas que les brinde apoyo con este proceso tan importante.
- Revisar, ajustar, aprobar y adoptar políticas que le permitan reducir los riesgos a nivel de seguridad de la información.
- Proyectar la adquisición de un aplicativo que les garantice el manejo adecuado de las historias clínicas, con lo cual la entidad le da cumplimiento a los lineamientos del Gobierno Nacional y reduce costos en términos de papel y archivo físico, aunque es de reconocer que debe hacer una inversión significativa en equipos, en el respaldo y en la seguridad informática.
- Revisar y proyectar el tema de la facturación electrónica de tal manera que cuando esto sea un requisito obligatorio ya la Entidad tenga un avance en el tema.

12.2 DENTRO DEL HACER

El hacer es el llevar acabo lo planeado y por consiguiente la Fundación debe:

- Realizar la adquisición y cambio de algunos teclados y mouse que se encuentran en malas condiciones.
- Realizar la adquisición de un antivirus que permita estandarizar este servicio y mejorar las condiciones de seguridad informática.
- Con el objetivo de evitar inconvenientes por el uso de software no legal se debe realizar las gestiones pertinentes para la legalización del software de los sistemas operativos y office.
- Por las distancias fiiscas que se manejan entre algunos puestos de trabajo y el hecho de que no todos cuentan con un teléfono sería pertinente buscar un software, preferiblemente gratuito, de mensajería instantáneo que les permita mejorar la comunicación y la transferencia de archivos de manera sencilla entre los funcionarios.
- De igual manera seria pertinente instalar un software, preferiblemente gratuito, que les permita realizar copias de seguridad de la información almacenada en cada uno de los equipos.
- Se debe revisar, actualizar, ajustar y dejar funcional la página web de la entidad.
- Se debe revisar el tema de redes sociales (Facebook), se puede concluir que fue habilitada pero no es revisada y tampoco actualizada, si no va a ser utilizada sería pertinente su eliminación.
- La Entidad tiene pendiente el proceso de registro de sus bases de datos ante la Superintendencia de Industria y Comercio.
- La Entidad tiene pendiente gestionar el proceso de actualización del aplicativo DELTA para dar cumplimiento a los requerimientos de las Normas Internacionales de Información Financiera.
- La Entidad debe elaborar un procedimiento para dar de baja los activos y de igual manera se realice el proceso de actualización de información en el sistema contable y financiero.
- Sería pertinente solicitar al proveedor del servicio de internet un informe que nos permita revisar cuales son las páginas que más se visitan y de la capacidad que se tiene cuanto se usa en un día promedio.
- Sería pertinente que se estudie la posibilidad de realizar la adquisición de un sistema de respaldo en caso de fallo del fluido eléctrico, teniendo en

cuenta que de presentarse este hecho se correo un alto riego del daño del equipo y por consiguiente de la pérdida de información.

- Realizar seguimiento permanente al cumplimiento de las políticas adoptadas.
- Se debe realizar el cambio de los tomacorrientes que se encuentran sueltos o en mal estado.
- El rack de comunicaciones, por seguridad, debe estar aislado, con seguridad y con unas condiciones térmicas que garanticen el correcto funcionamiento de los equipos ahí instalados.
- Establecer un proceso de indicadores que permita tener información veraz y oportuna para la toma de decisiones.

12.3 DENTRO DEL VERIFICAR

El verificar consiste en revisar si lo que se ha hecho esta alineado a lo planeado y la identificación de nuevas variables que surgen en el quehacer de la Entidad, y por consiguiente la Fundación debe:

- verificar el cumplimiento a las Políticas y directrices emitidas desde Gerencia o Sistemas.
- Verificar el cumplimiento de los objetivos y de los indicadores propuestos.

12.4 DENTRO DEL ACTUAR

El actuar se da con la identificación de los cambios o ajustes que se presentan por la nueva Normatividad emitida, por los cambios en los procesos o por la dinámica del mercado y por consiguiente la Fundación debe:

- Actuar con los cambios que se generen con nuestros clientes internos o externos.

13. POLITICAS INSTITUCIONALES

Si la Fundación está de acuerdo con las recomendaciones planteadas en el presente documento tendría en su buen haber la implementación y seguimiento de las políticas que a continuación se plantean, las cuales tienen como objetivo primordial la reducción del riesgo de pérdida o fuga de información.

13.1 PROTECCIÓN DE DATOS PERSONALES

Teniendo en cuenta que la Superintendencia de Industria y Comercio exige que todas la empresas que utilizan y manejan datos personales, realicen un proceso de registro de sus Políticas relacionadas con la Protección de los Datos Personales y teniendo en cuenta que para la fecha la Fundación Sabemos Cuidarte no cuenta con esta política se procede a plantear la siguiente propuesta:

13.1.1 NORMATIVIDAD

- Ley Estatutaria 1266 de 2008 por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones**.**
- Ley Estatutaria 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales**.**
- Decreto 2952 de 2010 Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.
- Decreto 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014 Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012 relativo al Registro Nacional de Base de Datos.

13.1.2 DEFINICIONES

Según el Artículo 3 de la Ley Estatutaria 1266 de 2008 se establecen y se adoptan las siguientes definiciones así:

a) **Titular de la información:** persona natural o jurídica a quien se refiere la información que reposa en una base de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la ley.

b) **Fuente de información:** persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos.

c) **Usuario:** persona natural o jurídica que, en los términos y circunstancias previstos en la ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos.

d) **Dato personal:** pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la ley. Cuando en la ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados:

Dato público: dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado: dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la ley Estatutaria 1266 de 2008.

Dato privado: dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

e) **Habeas Data**: derecho fundamental que tiene toda persona para conocer, actualizar y rectificar toda aquella información que se relacione con ella y que se recopile o almacene en bases de datos. (Artículo 15 de la Constitución Política de Colombia, Desarrollado por la Ley 1266 de 2008.)

Según el Artículo 3 de la Ley Estatutaria 1581 de 212 se establecen y se adoptan las siguientes definiciones así:

f) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

g) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.

h) **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

i) **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

j) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

13.1.3 PRINCIPIOS APLICADOS

En el desarrollo, interpretación y aplicación del tratamiento para la Protección de los Datos Personales se tendrán en cuenta, de manera armónica e integral, los principios que están establecidos en el Artículo 4 de la Ley Estatutaria 1266 de 2008 así:

a) **Principio de veracidad**: La información contenida en las bases de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan al error.

b) **Principio de finalidad**: La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto.

c) **Principio de circulación restringida**: La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad de la bases de datos. Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la ley.

d) **Principio de temporalidad:** La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad de la base de datos.

e) **Principio de interpretación integral de derechos constitucionales:** La ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables.

f) **Principio de seguridad:** La información que conforma los registros individuales constitutivos de las bases de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado.

g) **Principio de confidencialidad:** Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

13.1.4 DERECHOS DE LOS TITULARES

Según la Ley Estatutaria 1581 de 2012 en su Título IV “Derechos y Condiciones de Legalidad para el tratamiento de datos” en su artículo 8 se establecen los siguientes Derechos de los Titulares así:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en la ley.

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley y las demás normas que la modifiquen, adicionen o complementen.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la ley y a la Constitución.

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

13.1.5 DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO

Según la Ley Estatutaria 1581 de 2012 en su Título VI “Deberes de los Responsables del Tratamiento y Encargados del tratamiento” en sus artículos 17 y 18 se establece:

Artículo 17. ***Deberes de los Responsables del Tratamiento.*** Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el Titular.

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la ley.

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

m) Informar a solicitud del Titular sobre el uso dado a sus datos.

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Artículo 18. ***Deberes de los Encargados del Tratamiento.*** Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la ley.

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la ley.

f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.

g) Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la ley.

h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

13.1.6 RESPONSABLE DE LA ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS

La Entidad responsable y encargada del Tratamiento de la Información es una persona Jurídica, de Naturaleza Privada, cuyos datos son los siguientes:

Razón Social:	Fundación Sabemos Cuidarte
NIT:	900.260.224-2
Dirección:	Calle 14 Norte #7-56 El recuerdo
Municipio:	Popayán - Cauca
Teléfono:	(2) 8367981
Celular:	316-5714992
Página web:	www.sabemoscuidarte.com
Correo Electrónico:	fscuidarte@hotmail.com

La Entidad tiene establecidos los siguientes medios de contacto para los trámites relacionados con el Tratamiento de los datos personales así:

- Por medio de comunicación escrita y la cual debe ser radicada en la oficina de la entidad.
- Por medio de comunicación enviada al correo electrónico fscuidarte.com

13.1.7 TRATAMIENTO AL CUAL SERAN SOMETIDOS LOS DATOS Y FINALIDAD DE LOS MISMOS

El tratamiento de los datos personales obtenidos de los empleados, los ex empleados, contratistas, proveedores, usuarios de las EPS, Entidades Promotoras de Salud (EPS), Instituciones Prestadoras de Servicios (IPS) y cualquier otra persona natural o jurídica con la cual la Fundación Sabemos Cuidarte establezca cualquier relación bien sea permanente u ocasional, se realizará dentro del marco legal que regula la materia y se hará siempre en el cumplimiento de la misión institucional.

Algunos de los datos personales que se recolectan son: los nombres, los apellidos, la dirección de residencia, correo electrónico, número de teléfono fijo o celular, profesión, genero, edad, fecha y lugar de nacimiento, estado civil, entre otros datos públicos, semiprivado y sensibles

La información recolectada y tratada podrá ser utilizada para:

- Empleados y ex empleados: para dar cumplimiento a la normatividad aplicable en términos laborales y de seguridad social.
- Contratistas, Proveedores, EPS, IPS: para dar cumplimiento a la normatividad aplicable en términos de condiciones comerciales y/o tributarias.
- Con todos nuestros clientes para realizar encuestas que permitan medir el nivel de satisfacción de los mismos.

13.1.8 POLITICAS ESTABLECIDAS

- La **Fundación Sabemos Cuidarte** no presta, no alquila, no vende, no intercambia sus datos personales con ninguna otra Entidad; salvo por una disposición legal.
- La **Fundación Sabemos Cuidarte** almacenará los datos personales durante el tiempo que sea necesario para cumplir los objetivos institucionales para los cuales fueron recolectados, salvo una disposición legal.
- En la **Fundación Sabemos Cuidarte** los datos personales solo serán tratados por aquellos funcionarios que cuentan con autorización para ello.
- La **Fundación Sabemos Cuidarte** autorizará al responsable del área funcional que maneja y procesa los Datos Personales, para que sean ellos los que realicen el tratamiento solicitado por el titular, según sea el caso**.**
- La **Fundación Sabemos Cuidarte** no permitirá el acceso de la información de los datos personales mediante Internet u otros medios masivos de comunicación.
- En la **Fundación Sabemos Cuidarte e**l Titular de los Datos Personales podrá consultar, en cualquier momento, la información consignada en la base de datos previa solicitud realizada por los medios habilitados por la entidad.
- La **Fundación Sabemos Cuidarte suministrará,** actualizará, rectificará y/o suprimirá aquellos Datos Personales previa solicitud realizada por el Titular de los mismos y/o por una orden judicial.
- La **Fundación Sabemos Cuidarte** asegurará el tratamiento de la información garantizando los derechos prevalentes de los niños, niñas y adolescentes**.**
- La **Fundación Sabemos Cuidarte** provee todos los recursos necesarios (humano, técnico, insumos, equipos, etc.) con el objetivo de proteger y salvaguardar la información y de esta manera poder prevenir la copia, la adulteración, la eliminación y/o la consulta de la información por personal no autorizado.
- La **Fundación Sabemos Cuidarte** no realiza transferencia internacional de datos personales.
- La **Fundación Sabemos Cuidarte** no realiza transmisión internacional de datos personales.

- La **Fundación Sabemos Cuidarte** cuenta con la autonomía para realizar la revisión, ajuste y/o actualización de sus Políticas, siempre en concordancia con la Normatividad Legal vigente aplicable al caso**.**
- La **Fundación Sabemos Cuidarte** registrará sus bases de datos en el Registro Nacional de Base de Datos – RNBD dando cumplimiento a lo establecido en la Ley 1581 de 2012.

13.1.9 PROCEDIMIENTO PARA QUE LOS TITULARES PUEDAN EJERCER SUS DERECHOS

El procedimiento que se debe realizar para que los Titulares de los datos Personales puedan ejercer sus derechos sobre la información contenida en la base de datos se tiene establecido de la siguiente manera:

- **Para Consulta**: en el caso en que la solicitud sea únicamente para consulta de la información el Titular debe presentar comunicación por escrito en la oficina de la Entidad o mediante un correo electrónico enviado a. La solicitud debe incluir sus nombres y apellidos, su identificación, su dirección y el motivo de la consulta. Para estos casos el funcionario responsable de la revisión y respuesta a la Consulta cuenta con un máximo de diez (10) días hábiles para la respuesta.
- **Para Actualizar, Rectificar y/o Suprimir Información**: en el caso en que el usuario requiera Actualizar, Rectificar y/o Suprimir Información contenida en la base de datos, el Titular debe presentar comunicación por escrito en la oficina de la Entidad o mediante un correo electrónico enviado a. La solicitud debe incluir sus nombres y apellidos, su identificación, su dirección, el motivo del requerimiento y si existen documentos o pruebas que permitan soportar la solicitud. Para estos casos el funcionario responsable de la revisión y respuesta del caso cuenta con un máximo de quince (15) días hábiles para la respuesta.

13.1.10 VIGENCIA

Las políticas y lineamientos establecidos en el presente documento entrar a regir a partir de la fecha de su expedición.

Dado en la Ciudad de Popayán, a los dos (02) días del mes de Febrero de 2017.

HECTOR SAID SARMIENTO MARTINEZ

Gerente

13.2 POLITICA DE SEGURIDAD INFORMATICA

13.2.1 INTRODUCCION

Para la Fundación Sabemos Cuidarte es muy importante la generación, almacenamiento y condiciones de protección de la información, a través del uso de las Tecnologías de la Información y las Comunicaciones - Tics, como uno de sus activos más valiosos, por lo tanto es importante determinar lineamientos de seguridad que eviten la perdida, el deterioro y/o posibles ataques a la información, identificando las vulnerabilidades, los riesgos y las actividades consecuentes con el fin de garantizar el normal funcionamiento de la Entidad.

Las políticas planteadas deben servir de instrumento y de guía a todos los Funcionarios de la Fundación para prevenir y ayudar en el proceso de protección de la información, por consiguiente estas directrices son de obligatorio cumplimiento.

13.2.2 DEFINICIONES

- **TIC**: abreviatura de tecnología de la Información y las comunicaciones.
- **Hardware**: conjunto de elementos físicos o materiales que constituyen un computador.
- **Software**: conjunto de programas y rutinas que permite al computador realizar determinadas tareas.
- **Clave de acceso**: palabra privada utilizada para confirmar una identidad en un sistema remoto y evitar que una persona sea suplantada en su identidad.
- **Internet**: red de redes que permite la interconexión descentralizada de los computadores.
- **Virus Informático**: es un tipo de programa que busca alterar el normal funcionamiento del computador o sistema informático.
- **Seguridad de la Información**: conjunto de medidas preventivas y correctivas que buscan proteger la información manteniendo su confidencialidad, integridad y disponibilidad de la misma.

- **“Hueco” de seguridad**: es una vulnerabilidad de un sistema de información que permite mediante su explotación violar la seguridad del sistema.

13.2.3 ALCANCE

Las Políticas o Lineamientos consignados en el presente documento son de carácter obligatorio y deben cumplirse por parte de todos los funcionarios de la Fundación Sabemos Cuidarte; si se comprueba el incumplimiento de los mismos esta falta se puede catalogar como Grave y podría ser considerada como causal para la terminación del contrato de trabajo.

13.2.4 COMPROMISO DE LA GERENCIA

El Gerente de la Fundación Sabemos Cuidarte se compromete con los procesos de implementación de la Políticas, el seguimiento periódico de las mismas y de suministrar los recursos humanos, económicos y técnicos que le permitan a la Entidad el logro de los objetivos propuestos. Además reconoce que para tener éxito en el proceso es indispensable invertir en los procesos de capacitación y concientización de todos sus Funcionarios, haciendo un énfasis especial en aquellos Funcionarios que ingresen nuevos a la Entidad.

13.2.5 REVISION Y ACTUALIZACION

Las Políticas y Lineamientos aquí establecidos se deben revisar de manera periódica (cada dos meses) y/o en el caso que se presente algún evento considerado grave y la actualización del presente documento se debe realizar como mínimo una vez al año.

13.2.6 CONFIDENCIALIDAD

Toda aquella información que se maneje o se procese dentro y/o con motivo de las labores que desarrolla la Fundación Sabemos Cuidarte es de uso exclusivo y confidencial de la Fundación, por tal motivo ninguno de sus Funcionarios podrá utilizar dicha información para uso o beneficio de tipo personal.

13.2.7 DEBERES Y RESPONSABILIDADES DE LOS USUARIOS

13.2.7.1 CON RESPECTO A LOS EQUIPOS.

Los usuarios de los equipos de cómputo tienen establecidos los siguientes deberes y responsabilidades con el objetivo de brindar el mejor uso posible de estos elementos de trabajo y prolongar la vida útil de estos equipos, asi:

- Será su responsabilidad el correcto manejo y la debida custodia.
- Está prohibido utilizarlos para propósitos personales o en beneficio de terceros.
- Se prohíbe el uso indebido que se pudiese dar a los equipos tales como producción, reproducción y operación de programas en beneficio de terceros.
- Está prohibido asumir personalmente la solución de problemas mecánicos eléctricos o electrónicos.
- Está prohibido retirar, añadir o suprimir partes o elementos internos o externos de los equipos de cómputo. Lo anterior, para evitar al usuario alguna descarga eléctrica, corto circuito, etc., así como, en su caso, el invalidar la garantía del equipo.
- Por ningún motivo está autorizado a trasladar equipos dentro y fuera de las instalaciones, salvo en aquellos casos en el que se tenga autorización escrita por parte del Gerente.
- Está prohibido consumir alimentos en los puestos de trabajo que tengan instalados equipos de cómputo.
- Deben mantener los equipos de cómputo libre de todo tipo de objetos que puedan impedir la adecuada ventilación o afecten de alguna manera a los mismos.
- Es su responsabilidad apagar los equipos al terminar su labor o en los

momentos en que se retire por largo tiempo del puesto de trabajo.

- Es su responsabilidad informar cualquier anomalía que pueda presentar su equipo al Gerente o al área de sistemas.
- El Usuario no debe cambiar la configuración del equipo de cómputo que le sea asignado, que altere la operación de los servicios prestados a través de este medio por seguridad de la empresa.
- Es responsabilidad de cada usuario el adecuado manejo y las consecuencias derivadas del uso de medios de almacenamiento externos (CD, DVD, memorias, USB, discos externos, etc.) a los equipos de cómputo autorizados.
- Ningún tipo de equipo informático podrá ser instalado con la configuración por defecto del fabricante o proveedor, ya que esto abre “huecos” de seguridad, haciendo más vulnerables los sistemas, la configuración es manejada únicamente por el área de sistemas.
- Permitir al personal de sistemas el acceso a los equipos de cómputo y comunicaciones, para llevar a cabo la asistencia técnica, revisiones e instalaciones necesarias y/o los servicios de mantenimiento requeridos.
- Verificar que los equipos de cómputo asignados, estén conectados a los dispositivos de corriente regulada, con el objeto de prevenir fallas ocasionadas por descargas eléctricas y/o variaciones de voltaje.
- Abstenerse de conectar cafeteras, hornos de microondas, aspiradoras y en general aparatos con motor a los contactos de corriente regulada, con el objeto de prevenir o evitar daños a los equipos de cómputo.
- El área de sistemas podrá bloquear el acceso a cualquier servicio que suponga una amenaza temporal o permanente para la seguridad o integridad de la red institucional.

13.2.7.2 CON RESPECTO A LAS CLAVES DE ACCESO

Las claves de acceso brinden un cierto grado de seguridad y su objetivo es no permitir que personas no autorizadas accedan a datos o información que solo le interesa a la Entidad, por lo tanto los usuarios de los equipos de cómputo tienen establecidos los siguientes deberes y responsabilidades con relación al correcto uso de las claves de acceso, asi:

- Las claves de acceso son personales e intransferibles: debe ser mantenida con carácter confidencial, por lo tanto no debe ser revelada a otros

funcionarios o a terceros. Está prohibido divulgar cualquier tipo de clave de acceso.

- El usuario es responsable de establecer contraseñas de fácil recordación pero no obvias.
- Es responsabilidad del usuario cambiar la clave asignada cada vez que se requiera o cuando considere ha perdido la confidencialidad de la misma.
- Al retirarse de su puesto de trabajo es su responsabilidad, verificar que el equipo quede bloqueado y que se requiera la contraseña para su activación.

13.2.7.3 CON RESPECTO A LOS PROGRAMAS Y LA INFORMACION

La reproducción, duplicación o uso sin licencia de programas de computación (software), es ilegal y puede exponer al usuario implicado y a la Fundación Sabemos Cuidarte a demandas y denuncias civiles, penales y administrativas, de conformidad con la Ley 603 del 2000 sobre la obligatoriedad de presentar informes de Gestión, incluyendo el estado del cumplimiento de las normas sobre propiedad intelectual y derechos de autor, la Directiva Presidencial No 001 de 1999 y la Directiva No 002 de 2002 sobre la adquisición de software, por lo tanto:

- No se permitirá que funcionario alguno realice copias no autorizadas de software, bien sea para el uso propio o para terceros.
- Está prohibido entregar información propia del Fundación Sabemos Cuidarte. a personas distintas a las autorizadas, ya sea por medio magnético (DVD, CD, USB, etc.) o por medio electrónico (Internet, Correo electrónico, mensajería instantánea, etc.).
- Usted no debe copiar, ni instalar ningún programa en el computador que le ha sido asignado por el Fundación Sabemos Cuidarte. así el programa (software) sea de libre distribución, sin estar previamente autorizado por el área de sistemas, de esta forma se evita infringir de manera intencional o por equivocación los derechos de autor de las compañías productoras de software.
- En caso de requerir instalar software compartido con otras entidades e indispensable para el cumplimiento de nuestras actividades, se deberá reportar al área de sistemas, para verificar los requisitos que se deben tener en cuenta para estos casos.
- Es su responsabilidad de cada funcionario revisar los medios magnéticos

de almacenamiento de información (USB, DVD, cd, etc.), mediante las herramientas que ha dispuesto el Fundación Sabemos Cuidarte., con el fin de evitar que los equipos se infecten de virus.

- Es obligación de todos los usuarios, reportar al área de Sistemas y/o a su Jefe Inmediato, todas las irregularidades que observe o conozca y que puedan afectar la seguridad e integridad de la información.
- Es responsabilidad de cada usuario realizar copias de seguridad de la información perteneciente a su área y que maneja periódicamente de acuerdo a la relevancia e importancia de la misma. Las copias de seguridad de las bases de datos del sistema de información integral de la Entidad es realizada por el área de sistemas.
- Toda información que maneje cualquier funcionario que trabaje para la Fundación deberá velar por su buen uso, custodia y confidencialidad.
- El usuario es responsable de cualquier programa que se encuentre instalado en los equipos de cómputo asignados. El programa de cómputo que no cuente con la licencia de uso respectiva o que no sea de uso libre, se considera fuera de esta política de seguridad.

13.2.7.4 CON RESPECTIVO AL USO DE INTERNET

Internet es una herramienta muy valiosa de comunicación para todos, pero se hace necesario establecer unos lineamientos para dar un buen uso a la misma, por lo tanto los usuarios de los equipos de cómputo que tienen acceso a este servcio tienen los siguientes deberes y responsabilidades con relación al correcto uso del servcio de Internet, asi:

- El uso de internet puede ser utilizado solamente con fines autorizados y legales.
- El uso de internet y la utilización de activos para su conectividad y explotación, están restringidos. Su uso se da únicamente para el cumplimiento de la misión institucional y para el desarrollo de las labores de los funcionarios.
- La utilización de este recurso se hará dentro del marco que genera la aplicación de principios y valores morales y éticos por parte de todos sus usuarios.
- Con el objeto de aprovechar al máximo la conexión en Internet y optimizar el ancho de banda y la productividad de los usuarios, queda restringido el

acceso a los servicios de mensajería instantánea y redes sociales. Todas las actividades que los usuarios realicen en Internet, serán susceptibles de ser registradas y analizadas.

- Los usuarios deben abstenerse de modificar los parámetros de configuración del navegador de Internet de los equipos de cómputo propiedad de la Fundación.

13.2.7.5 CON RESPECTO AL USO DE CORREO ELECTRONICO INSTITUCIONAL

Las cuentas de correo electrónico corporativo o institucional se habilitan con el fin de que sean utilizadas única y exclusivamente para temas Institucionales y laborales, por consiguiente se establecen los siguientes deberes y responsabilidades con relación al correcto uso del servicio de correo electrónico institucioanal, asi:

- El sistema de correo electrónico institucional proporcionado por el Fundación Sabemos Cuidarte., no debe ser utilizado con fines particulares. El uso incorrecto pone a la Fundación Sabemos Cuidarte. en riesgo debido a la posibilidad de importar virus informáticos a los sistemas internos.
- Cuando el Fundación Sabemos Cuidarte. lo estime necesario tendrá el derecho a acceder el contenido del correo electrónico institucional asignado.
- Los usuarios son responsables de depurar, respaldar y archivar los correos electrónicos contenidos en su buzón.
- El servidor de correo electrónico institucional tendrá una capacidad de almacenamiento de 200 MB por cuenta, en caso de que se requiera más capacidad, deberá solicitarlo por escrito, indicando la justificación correspondiente para ser analizada y aprobada.
- Por razones de seguridad, los usuarios deben abstenerse de compartir el nombre de la cuenta y contraseña para acceder a los servicios de correo electrónico institucional, ya que estos son de carácter personal e intransferible, por lo que el uso inadecuado será responsabilidad de la persona a la que se asignó la cuenta de correo.
- Es responsabilidad del usuario el correcto uso de la información a la que tenga acceso, por lo que queda bajo su responsabilidad él envió de la misma a través del correo electrónico.

13.2.7.6 ANTIVIRUS

Los antivirus buscan prevenir la afectación o el daño de los equipos cómputo, de la información y protección a ciertas transacciones, por consiguiente se establecen los siguientes deberes y responsabilidades con relación al correcto uso del antivirus, asi:

- Todos los equipos propiedad de la Fundación deben tener instalado, configurado y actualizado el antivirus que se tiene establecido para la Entidad.
- Es responsabilidad de los usuarios realizar el análisis de los dispositivos de almacenamiento externo que manejan (CD, DVD, USB, memorias flash y/o cualquier otro dispositivo de almacenamiento) como medio de prevención y detección de posibles virus informáticos.
- Los usuarios deben reportar al área de Sistemas cualquier problema con la operación de la herramienta de antivirus y/o mensajes de virus que se presenten en sus equipos.

13.2.7.7 RESPALDOS DE INFORMACION

Las copias de seguridad permiten realizar el respaldo de la información considera vital para el funcionamiento permanente y continúo de la Entidad, por consiguiente:

- Es responsabilidad de los usuarios custodiar y respaldar periódicamente la información contenida en los dispositivos de almacenamiento (disco duro, cd, diskettes, memorias flash, USB, etc.) de los equipos de cómputo que les sean asignados, en especial ante una solicitud de soporte técnico. Lo anterior contribuirá a incrementar la cultura informática y llevar un adecuado control de la información propiedad de la Fundación.

13.2.7.8 CONTROL DE ACTIVOS E INFORMACIÓN

La Fundación Sabemos Cuidarte debe tener:

- El inventario actualizado de sus activos hardware, software e información.
- Todos los equipos deberán estar etiquetados de acuerdo al nivel de criticidad e Información que manejan.
- Todo producto generado a través de cualquier activo informático de la Fundación es propiedad de la organización.
- Cada usuario debe utilizar únicamente los activos informáticos asignados para su Labor.
- Definición y restricción de páginas y aplicativos no autorizadas para su acceso por su contenido o interferencia en el desempeño de las labores asignadas al personal.

13.2.7.9 USO DE LA INFRAESTRUCTURA INFORMÁTICA

La infraestructura en términos de la informática esta relacionada con el equipo de cómputo, de comunicaciones, las conexiones de red y de energía, por consiguiente:

- La infraestructura de cómputo, es única y exclusivamente para la realización de las actividades encomendadas a los funcionarios.
- La conexión a la red de datos institucional, es exclusiva para equipos de cómputo propiedad de la Fundación. La conexión de equipos ajenos a la Fundación, requiere de la autorización del Gerente.
- Los perfiles de configuración de software, serán proporcionados por el área de sistemas, con base a las actividades y funciones que desempeñen los funcionarios.

13.2.8 VIGENCIA

Las políticas y lineamientos establecidos en el presente documento entrar a regir a partir de la fecha de su expedición.

Dado en la Ciudad de Popayán, a los dos (02) días del mes de Diciembre de 2017.

HECTOR SAID SARMIENTO MARTINEZ
Gerente

14. PERSONAS QUE PARTICIPARON EN EL PROYECTO

Las personas que intervinieron en el proyecto fueron:

- El Docente o Tutor asignado al Curso de Proyectos de Seguridad Informática II.
- El Docente o Tutor asignado al presente proyecto.
- Los Funcionarios de la “Fundación Sabemos Cuidarte”.
- El Ingeniero en Sistemas que realizo el proyecto.

15. CONCLUSIONES

Se plantean las siguientes conclusiones así:

- Se realiza el diseño y el diligenciamiento de un hoja de vida para los equipos de cómputo, con la cual se recoge toda la información tanto del hardware, como del software y otra información considerada relevante de los equipos utilizados actualmente en la prestación de servicios en la Fundación Sabemos Cuidarte.
- Se realiza el diseño y se plantean una serie de actividades y de políticas orientadas a mejorar la seguridad de la información de la fundación Sabemos Cuidarte.
- Este proceso con la Fundación Sabemos Cuidarte fue muy productivo para mí, teniendo en cuenta que se pudo identificar una gran cantidad de falencias al interior de la organización y se poner en práctica los conocimientos adquiridos en el proceso de capacitación con la Universidad.

16. RECOMENDACIONES

Teniendo en cuenta la recopilación, la revisión y el análisis realizado se plantean una serie de sugerencias o recomendaciones con el objetivo de prevenir o mitigar el riesgo de la perdida de la información de la Entidad:

- La Fundación Sabemos Cuidarte debe realizar la implementación de un acta mediante la cual se le hace entrega, de manera oficial, al funcionario de su respectivo equipo de cómputo y garantizar que conozca las directrices institucionales con relación al uso correcto de estos equipos.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para poder legalizar su software, adquirir un sistema de protección de antivirus y realizar copias de seguridad de la información.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para poder gestionar la actualización y rediseño de su página web, tomar decisiones con su presencia en las redes sociales e implementar el uso del sistema de correo electrónico corporativo.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para poder adquirir e instalar un sistema eléctrico de respaldo que les permita salvaguardar la información en caso de cortes de energía.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para poder programar y llevar a cabo mantenimientos preventivos de todos los equipos de cómputo.
- La Fundación Sabemos Cuidarte debe organizar con su área de Contabilidad un proceso para dar de baja los equipos de cómputo que hayan cumplido su respectivo ciclo de vida.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para poder realizar la transición de la historia clínica manual a la historia clínica electrónica.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para empezar a trabajar en el proceso de transición a la Facturación electrónica.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para programar y realizar capacitaciones a todos su personal en el tema de sistemas informativos y de seguridad de la información.
- La Fundación Sabemos Cuidarte debe estudiar la posibilidad de contratar (de planta o por prestación de servicios) a un Profesional que los apoye o que sea el responsable del área de Sistemas.

17. DIVULGACION

Para el proceso de divulgación de las políticas se plantean las siguientes estrategias:

- Folleto informativo: diseñar y entregar a cada uno de los funcionarios de la Fundación un folleto que contenga una combinación de ilustraciones y Políticas, los objetivos tener un documento que sea “llamativo” de leer y que permita realizar la socialización y recordación de dichas políticas.
- Socialización: organizar una reunión con todos los funcionarios de la Fundación con el objetivo de poner en conocimiento cada una de las políticas establecidas, explicar el porqué de las mismas, los beneficios para la Entidad y las consecuencias en los cuales se pueden ver abocados por el incumplimiento de dichas directrices.
- Protector de Pantalla: diseñar y establecer en cada uno de los equipos de cómputo una presentación que contenga las políticas y se realice un proceso de cambio cada 15 días, el objetivo primordial realizar procesos de recordación de las directrices establecidas.
- Página web: la Política que tiene que ver con el manejo de los datos personales debe ser publicada en la página web de la Fundación.
- Inducción de Personal: garantizar que en los procesos de inducción del personal nuevo que ingresa a la Fundación se realice el proceso de socialización y entrega del folleto, el objetivo garantizar que todos los Funcionarios conozcan las directrices institucionales con relación al tema de seguridad informática.

BIBLIOGRAFÍA

BACA URBINA, Gabriel. Introduccíon a la Seguridad Informatica. Primera Edición Ebook. Mexico, 2016.

CARPENTER, Jean-Francois. La Seguridad Informatica en la Pyme, Situación actual y mejores practicas. España, 2016.

CORDOBA, Leyda. DELGADO, Wilson. Diseño de las Politicas de Control de Riesgos de la Seguridad de la Información para la Sede Central de la Gobernación del Putumayo (Mocoa). 2016 [Revisado en Agosto de 2017]. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Basicas, Tecnologia e Ingenieria. Obtenido de biblioteca virtual de la UNAD: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/8511/3/1124848759.pdf

GOMEZ VIEITES, Alvaro. Enciclopedoa de la Seguridad Informatica. Segunda Edición actualizada. España, 2010.

HUERTA, Antonio. Introducción al análisis de riesgos – Metodologías (II). 2012. Security A®twork. Disponible en: https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

MATALOBOS, Juan. Análisis de Riesgos de Seguridad de la Información. 2009. Universidad Politécnica de Madrid. Facultad de Informática. Disponible en: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

MOLINA, María. Propuesta de un Plan de Gestión de Riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral. 2015. Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación. Disponible en: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

PULIDO, Ana. MANTILLA, Jenith. Modelo para la implementación del Sistema General de Seguridad Informatica y Protocolos de Seguridad Informatica en la oficina TIC de la Alcaldia Municipal de Fusagasuga, Basados en la Gestión del Riesgo Informatico. Fusagasuga. 2016 [Revisado en Agosto de 2017]. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Basicas, Tecnologia e Ingenieria. Obtenido de biblioteca virtual de la UNAD: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/6327/1/35250225.pdf

REINA, Elkin. MORALES, Jose. Modelamiento de Procesos basados en el grupo de Normas Internacionales ISO/IEC 27000 para Gestionar el Riesgo y Seleccionar Controles en la Implementación del Sistema de Gestion de Seguridad de la Información. Pereira. 2014 [Revisado en Agosto de 2017]. Universidad Tecnologica de Pereira. Facultad de Ingenieria Electrica, electronica, Fisica y Ciencias de la Computación. Programa de Ingenieria de Sistemas y Computación. Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4894/0058R364.pdf?sequence=1&isAllowed=y

RODRIGUEZ, Claudia. ALEMAN, Helena. Metodologías para el Análisis de Riesgos en los SGSI. 2015. Publicaciones e investigación. Revista Especializada en Ingeniería. Universidad Nacional Abierta a Distancia UNAD. Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

VANEGAS, Gonzalo. PARDO, Cesar. Hacia un Modelo para la gestión de riesgos de TI en MiPymes: MOGRIT. 2014. Artículo publicado en la Revista S&T. Universidad ICESI. Facultad de Ingeniería. Disponible en: https://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/download/1860/2398/

EBIOS. 2004. Secrétariat Général de la Défense Nationale. Republica de Francia. Disponible en: https://www.ssi.gouv.fr/archive/es/confianza/documents/methods/ebiosv2-section1-introduction-2004-02-05_es.pdf

¿Qué es la seguridad informática y como puede ayudarme? Universidad Internacional de Valencia. Disponible en: https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/#/plus

Magerit V 3: Metodología de Análisis y Gestión de riesgos de los sistemas de información. 2012. Portal Administración Electrónica. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WtDN7S7wbIU

ANEXOS

Anexo 1. Hoja de Vida equipo Talento humano

	HOJA DE VIDA DE EQUIPOS DE CÓMPUTO	FECHA	23/09/2016
		VERSIÓN	1

Nombre PC	User1

1. DATOS DEL EQUIPO

Marca	PHOENIX	Proveedor		Modelo	

2. CONFIGURACION DE HARDWARE

Placa Inventario	S/P			Marca y/o modelo Monitor	SAMSUNG
Modelo CPU				Serial Monitor	ZUGTHTLD402227T
Serial CPU	S/S			Marca y/o modelo Teclado	JANUS
Procesador	AMD E3500 APU HD GRAPHICS	Velocidad	1,6	Serial Teclado	1305108959
Memoria RAM	2 GB			Marca y/o modelo Mouse	JANUS
Disco Duro	Marca	Capacidad	Tecnología	Serial Mouse	8959
		550	IDE / SATA	Otro	

3. CONFIGURACION DE RED

Nombre del Equipo	En red		Dirección IP	Dirección MAC	Marca	Velocidad
User1	SI		192.168.0.14			

4. SISTEMA OPERATIVO INSTALADO

Nombre del SO	Bits	Licencia
windows 8 pro	32	00178-70000-00011-AA129

5. SOFTWARE INSTALADO

Nombre del Aplicativo	Requiere Licencia	Licencia
office profesional plus 2010	si	
avast		
Kmspico - activador		
spotify		

6. MANTENIMIENTOS PREVENTIVOS

Mantenimiento				
Fecha Realización	**No es posible determinar**	Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa

Observaciones				
				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:

7. Ubicación Actual

Usuario Responsable	Ubicación dentro de la Empresa	Fecha	Firma Responsable
MARIA MERCEDES TORRES	RECURSOS HUMANOS		
		DD / MM / AAAA	

8. RECOMENDACIONES Y/O OBSERVACIONES

cpu del equipo no tiene esticker de licencia de SO
se debe verificar la autencidad de la licencia del office
se debe revisar el antivirus y su licenciamiento
temp 849 elementos el mas antiguo 06 de mayo 2016
se debe cambiar el nombre del equipo
utiliza la cuenta de correo talentohumanofsc@hotmail.com

Anexo 2. Hoja de Vida equipo Referencia

	HOJA DE VIDA DE EQUIPOS DE CÓMPUTO	FECHA	23/09/2016
		VERSIÓN	1

Nombre PC	REFERENCIA-PC

1. DATOS DEL EQUIPO

Marca	JANUS	Proveedor		Modelo	

2. CONFIGURACION DE HARDWARE

Placa Inventario	S/P				Marca y/o modelo Monitor	SAMSUNG
Modelo CPU					Serial Monitor	YC5RH9LZ309413T
Serial CPU	S/S				Marca y/o modelo Teclado	GENIUS
Procesador	Intel Celeron cpu G1610	Velocidad	2,6 ghz		Serial Teclado	WE1C92083371
Memoria RAM	2 GB				Marca y/o modelo Mouse	PHOENIX
Disco Duro	Marca	Capacidad	Tecnología		Serial Mouse	S/S
		500	IDE	SATA	Otro	

3. CONFIGURACION DE RED

Nombre del Equipo	En red		Dirección IP	Dirección MAC	Marca	Velocidad
REFERENCIA-pc	SI		192.168.0.7			

4. SISTEMA OPERATIVO INSTALADO

Nombre del SO	Bits	Licencia
windows 7 ultimate	32	00426-0em-8992662-00006

5. SOFTWARE INSTALADO

Nombre del Aplicativo	Requiere Licencia	Licencia
office profesional plus 2010	si	
avg		

6. MANTENIMIENTOS PREVENTIVOS

Mantenimiento				
Fecha Realización	**No es posible determinar**	Realizó		Aceptación Empresa
Observaciones				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				Firma
				Nombre:

7. Ubicación Actual

Usuario Responsable	Ubicación dentro de la Empresa	Fecha	Firma Responsable
ADRIANA SOTO	REFERENCIA Y CONTRAREFERENCIA		
		DD / MM / AAAA	

8. RECOMENDACIONES Y/O OBSERVACIONES

cpu del equipo no tiene esticker de licencia de SO y el numero de licencia es igual al de facturacion
se debe verificar la autencidad de la licencia del office
se debe revisar el antivirus y su licenciamiento avf free
temp 1246 elemtos el mas antiguo 04/01/2013
descargas 23 eleementos
sin copias de seguridad

fscuidarte@hotmail.com es la cuenta de correo de difusión y conocimiento para usuarios y eps

Anexo 3. Hoja de Vida equipo Coordinación de Terapistas

	HOJA DE VIDA DE EQUIPOS DE CÓMPUTO	FECHA	23/09/2016
		VERSIÓN	1

Nombre PC	FSCFISIOFONO

1. DATOS DEL EQUIPO

Marca	PHOENIX	Proveedor		Modelo	

2. CONFIGURACION DE HARDWARE

Placa Inventario	S/P			Marca y/o modelo Monitor	SAMSUNG
Modelo CPU				Serial Monitor	YC5RH9LZ309416Z
Serial CPU	S/S			Marca y/o modelo Teclado	GENIUS
Procesador	AMD	Velocidad	2,72 GHz	Serial Teclado	WE1C92083362
Memoria RAM	2 GB			Marca y/o modelo Mouse	COMPAQ
Disco Duro	Marca	Capacidad	Tecnología	Serial Mouse	S/S
		930	IDE / SATA	Otro	

3. CONFIGURACION DE RED

Nombre del Equipo	En red		Dirección IP	Dirección MAC	Marca	Velocidad
FSCFISIOFONO	SI		192.168.0.21			

4. SISTEMA OPERATIVO INSTALADO

Nombre del SO	Bits	Licencia
windows xp profesional	32	55274-640-0263172-23784

5. SOFTWARE INSTALADO

Nombre del Aplicativo	Requiere Licencia	Licencia
office profesional plus 2007	si	89409-726-2958074-65650
avast free		

6. MANTENIMIENTOS PREVENTIVOS

Mantenimiento				
Fecha Realización	**No es posible determinar**	Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma

				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:

7. Ubicación Actual

Usuario Responsable	Ubicación dentro de la Empresa	Fecha	Firma Responsable
CLAUDIA ALBAN	COORDINACION		
		DD / MM / AAAA	

8. RECOMENDACIONES Y/O OBSERVACIONES

cpu del equipo no tiene esticker de licencia de SO
se debe verificar la autencidad de la licencia del office
se debe revisar el antivirus y su licenciamiento
temp 1208 mas antiguo 15 feb 2008
chrome mensaje "no compatible con xp y vista"
copia de seguridad sin identificar
cyal77@hotmail.com

utiliza su cuenta de correo personal

Anexo 4. Hoja de Vida equipo Biomédico

Fundación SABEMOS CUIDARTE	**HOJA DE VIDA DE EQUIPOS DE CÓMPUTO**	FECHA	23/09/2016
		VERSIÓN	1

Nombre PC	FCCBiomedico-PC

1. DATOS DEL EQUIPO

Marca	HG	Proveedor		Modelo	

2. CONFIGURACION DE HARDWARE

Placa Inventario	S/P					Marca y/o modelo Monitor	AOC
Modelo CPU						Serial Monitor	FWYD31A000831
Serial CPU	F1074R0510131700514					Marca y/o modelo Teclado	HG
Procesador	Intel Celeron CPU G1610	Velocidad	2,6 GHz			Serial Teclado	2,01304E+12
Memoria RAM	2 GB					Marca y/o modelo Mouse	HP
Disco Duro	Marca	Capacidad	Tecnología			Serial Mouse	S/S
		180	IDE	SATA		Otro	

3. CONFIGURACION DE RED

Nombre del Equipo	En red	Dirección IP	Dirección MAC	Marca	Velocidad

FCCBiomedico-PC	SI		192.168.0.25			

4. SISTEMA OPERATIVO INSTALADO

Nombre del SO	Bits	Licencia
windows 7 ultimate	32	00426-065-1809377-86575

5. SOFTWARE INSTALADO

Nombre del Aplicativo	Requiere Licencia	Licencia
office profesional plus 2010	si	
avast		

6. MANTENIMIENTOS PREVENTIVOS

Mantenimiento				
Fecha Realización	**No es posible determinar**	Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:

7. Ubicación Actual

Usuario Responsable	Ubicación dentro de la Empresa	Fecha	Firma Responsable
		DD / MM / AAAA	

8. RECOMENDACIONES Y/O OBSERVACIONES

cpu del equipo no tiene esticker de licencia de SO mensaje "esta copia de windows no es original"
se debe verificar la autencidad de la licencia del office
se debe revisar el antivirus y su licenciamiento
teclado sin letras
sivigila
temp 206 elementos el mas antiguo 08/08/2016
descargas 62 eleemntos

Anexo 5. Hoja de Vida equipo Historias Clínicas

	HOJA DE VIDA DE EQUIPOS DE CÓMPUTO	FECHA	23/09/2016
		VERSIÓN	1

Nombre PC	FSCsecretaria

1. DATOS DEL EQUIPO

Marca	COMPAQ	Proveedor		Modelo	PRESARIO

2. CONFIGURACION DE HARDWARE

Placa Inventario	S/P			Marca y/o modelo Monitor	COMPAQ
Modelo CPU				Serial Monitor	CNC043QMOJ
Serial CPU	MXX0420YDT			Marca y/o modelo Teclado	COMPAQ
Procesador	AMD ATHLON II X 3440	Velocidad	3 GHz	Serial Teclado	LE10119331
Memoria RAM	2 GB			Marca y/o modelo Mouse	HG
Disco Duro	Marca	Capacidad	Tecnología	Serial Mouse	S/S
		700	IDE / SATA	Otro	

3. CONFIGURACION DE RED

Nombre del Equipo	En red		Dirección IP	Dirección MAC	Marca	Velocidad
FSCsecretaria	SI		192.168.0.50			

4. SISTEMA OPERATIVO INSTALADO

Nombre del SO	Bits	Licencia
windows 7 home basic	64	00346-OEM-8992752-50008

5. SOFTWARE INSTALADO

Nombre del Aplicativo	Requiere Licencia	Licencia
office 2010 hogar y pequena empresa	si	
	si	x verificar

6. MANTENIMIENTOS PREVENTIVOS

Mantenimiento				
Fecha Realización	**No es posible determinar**	Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				

Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:

7. Ubicación Actual

Usuario Responsable	Ubicación dentro de la Empresa	Fecha	Firma Responsable
VIVIANA JURADO	ARCHIVO HC		
		DD / MM / AAAA	

8. RECOMENDACIONES Y/O OBSERVACIONES

cpu del equipo con sticker so original
se debe verificar la autencidad de la licencia del office
dos antivirus advanced system protector y avast
actualizar nombre pc según area
temp 2492 elementos

Anexo 6. Hoja de Vida equipo Coordinación Enfermería

	HOJA DE VIDA DE EQUIPOS DE CÓMPUTO	FECHA	23/09/2016
		VERSIÓN	1

Nombre PC	Enfermeria-PC

1. DATOS DEL EQUIPO

Marca	DELL	Proveedor		Modelo	INSPIRON

2. CONFIGURACION DE HARDWARE

Placa Inventario	S/P				Marca y/o modelo Monitor	PORTATIL
Modelo CPU					Serial Monitor	
Serial CPU	36399498373				Marca y/o modelo Teclado	
Procesador	INTEL CORE i3-2310M	Velocidad	2,1		Serial Teclado	
Memoria RAM	3				Marca y/o modelo Mouse	GENIUS
Disco Duro	Marca	Capacidad	Tecnología		Serial Mouse	X64487808329
		600	IDE	SATA	Otro	

3. CONFIGURACION DE RED

Nombre del Equipo	En red		Dirección IP	Dirección MAC	Marca	Velocidad
Enfermeria-PC	SI		192.168.0.13			

4. SISTEMA OPERATIVO INSTALADO

Nombre del SO	Bits	Licencia
windows 10 PRO	32	00330-80000-00000-AA213

5. SOFTWARE INSTALADO

Nombre del Aplicativo	Requiere Licencia	Licencia
office 2007	si	89388-726-2958074-65518

6. MANTENIMIENTOS PREVENTIVOS

Mantenimiento				
Fecha Realización	**No es posible determinar**	Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:

7. Ubicación Actual

Usuario Responsable	Ubicación dentro de la Empresa	Fecha	Firma Responsable
PATRICIA BALLESTEROS	COORDINADORA ENFERMERIA		
		DD / MM / AAAA	

8. RECOMENDACIONES Y/O OBSERVACIONES

sticker so original
se debe verificar la autencidad de la licencia del office
sin antivirus
temp 148 elementos 14/07/2016
historial navegador 1948 eleemntos
descargas 255 elementos
utiliza su cuenta de correo personal

Anexo 7. Hoja de Vida equipo Contabilidad

	HOJA DE VIDA DE EQUIPOS DE CÓMPUTO	FECHA	23/09/2016
		VERSIÓN	1

Nombre PC	fsccontabilidad

1. DATOS DEL EQUIPO

Marca	ARGOM	Proveedor		Modelo	

2. CONFIGURACION DE HARDWARE

Placa Inventario	S/P			Marca y/o modelo Monitor	LG LED 19EN33
Modelo CPU				Serial Monitor	304NDRFGM454
Serial CPU	SQ6506446335ZF			Marca y/o modelo Teclado	ARGOM
Procesador	Intel Celeron CPU G1610	Velocidad	2,6 GHz	Serial Teclado	KB20130406070
Memoria RAM	2 GB			Marca y/o modelo Mouse	ARGOM
Disco Duro	Marca	Capacidad	Tecnología	Serial Mouse	KB20130406076
		200	IDE / SATA	Otro	

3. CONFIGURACION DE RED

Nombre del Equipo	En red		Dirección IP	Dirección MAC	Marca	Velocidad
fsccontabilidad	SI		192.168.0.12			

4. SISTEMA OPERATIVO INSTALADO

Nombre del SO	Bits	Licencia
windows 7 ultimate	64	00426-OEM-8992662-00006

5. SOFTWARE INSTALADO

Nombre del Aplicativo	Requiere Licencia	Licencia
office profesional plus 2010	si	error de activacion
avast FREE		
delta	si	01-19001-C-27684

6. MANTENIMIENTOS PREVENTIVOS

Mantenimiento				
Fecha Realización	**No es posible determinar**	Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				

Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:

7. Ubicación Actual

Usuario Responsable	Ubicación dentro de la Empresa	Fecha	Firma Responsable
ANGELA ARROYAVE	CONTABILIDAD		
		DD / MM / AAAA	

8. RECOMENDACIONES Y/O OBSERVACIONES

cpu del equipo no tiene esticker de licencia de SO
se debe verificar la autencidad de la licencia del office aparece error de activación
se debe revisar el antivirus y su licenciamiento
teclado sin letras
verificar licencia de delta
pasa con niif
historial de navegacion 389 elementos
temporal 2393 elementos el mas antiguo es de 18 de julio de 2012
copia de seguridad solo DELTA, diario en el equipo pero no tenemos mas copias de seguridad
descargas 23 elementos

utiliza su cuenta de correo personal o en su defecto la cuenta angela.sabemoscuidarte@hotmail.com

Anexo 8. Hoja de Vida equipo Facturación

	HOJA DE VIDA DE EQUIPOS DE CÓMPUTO	FECHA	23/09/2016
		VERSIÓN	1

Nombre PC	facturacion-PC

1. DATOS DEL EQUIPO

Marca	ARGOM	Proveedor		Modelo	

2. CONFIGURACION DE HARDWARE

Placa Inventario	S/P			Marca y/o modelo Monitor	LG 19EN33
Modelo CPU				Serial Monitor	304NDJXGM428
Serial CPU	SQ6506446360ZF			Marca y/o modelo Teclado	ARGOM TECH
Procesador	Intel Celeron cpu G1610	Velocidad	2,6 ghz	Serial Teclado	KB20130405524
Memoria RAM	2 GB			Marca y/o modelo Mouse	COMPAQ
Disco Duro	Marca	Capacidad	Tecnología	Serial Mouse	505131-001
		150	IDE / SATA	Otro	

3. CONFIGURACION DE RED

Nombre del Equipo	En red	Dirección IP	Dirección MAC	Marca	Velocida

						d
facturacion-pc	SI		192.168.0.13		ARGOM	

4. SISTEMA OPERATIVO INSTALADO

Nombre del SO	Bits	Licencia
windows 7 ultimate	32	00426-0em-8992662-00006

5. SOFTWARE INSTALADO

Nombre del Aplicativo	Requiere Licencia	Licencia
office 2007	si	89388-726-2958074-65203
EmRips	si	sin información
Postgresql		
microsoft security		

6. MANTENIMIENTOS PREVENTIVOS

Mantenimiento				
Fecha Realización	**No es posible determinar**	Realizó		Aceptación Empresa
Observaciones				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				Firma
				Nombre:

7. Ubicación Actual

Usuario Responsable	Ubicación dentro de la Empresa	Fecha	Firma Responsable
FERNANDA MELENGE	FACTURACION		
		DD / MM / AAAA	

8. RECOMENDACIONES Y/O OBSERVACIONES

Revisar la posibilidad del cambio de teclado no se ven las letras
cpu del equipo no tiene esticker de licencia de SO
se debe verificar la autencidad de la licencia del office
se debe solicitar licenciamiento del programa emrips
se debe revisar el antivirus y su licenciamiento
carpeta 517 elementos mas antiguo de abril 2015
historial navegador 17018 elementos
copia de seguridad emrips en el equipo no hay mas copias
descargas 4 elementos

utiliza su cuenta de correo personal

Anexo 9. Hoja de Vida equipo Gerencia

	HOJA DE VIDA DE EQUIPOS DE CÓMPUTO	FECHA	23/09/2016
		VERSIÓN	1

Nombre PC	fscgerencia

1. DATOS DEL EQUIPO

Marca	HP	Proveedor		Modelo	

2. CONFIGURACION DE HARDWARE

Placa Inventario	S/P			Marca y/o modelo Monitor	PORTATIL
Modelo CPU				Serial Monitor	
Serial CPU	S/S			Marca y/o modelo Teclado	
Procesador	INTEL CORE i7 3630qm	Velocidad	2,4	Serial Teclado	
Memoria RAM	6			Marca y/o modelo Mouse	
Disco Duro	Marca	Capacidad	Tecnología	Serial Mouse	
		700	IDE / SATA	Otro	

3. CONFIGURACION DE RED

Nombre del Equipo	En red		Dirección IP	Dirección MAC	Marca	Velocidad
fscgerencia	SI		192.168.0.31			

4. SISTEMA OPERATIVO INSTALADO

Nombre del SO	Bits	Licencia
windows 8.1	64	00179-40170-28688-AAOEM

5. SOFTWARE INSTALADO

Nombre del Aplicativo	Requiere Licencia	Licencia
Office hogar y pequeña empresa 2010	si	89388-726-2958074-65518
avast		

6. MANTENIMIENTOS PREVENTIVOS

Mantenimiento				
Fecha Realización	**No es posible determinar**	Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				
Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:
Mantenimiento				

Fecha Realización		Realizó		Aceptación Empresa
Observaciones				
				Firma
				Nombre:

7. Ubicación Actual

Usuario Responsable	Ubicación dentro de la Empresa	Fecha	Firma Responsable
HECTOR SARMIENTO	GERENTE		
		DD / MM / AAAA	

8. RECOMENDACIONES Y/O OBSERVACIONES

sticker so original
se debe verificar la autencidad de la licencia del office
temp 1193 elementos mas antiguo 15 julio 2014
historial del navegador 1059 elementos
usa su cuenta de correo personal

RESUMEN ANÁLITICO RAE.

Título de Documento	DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA - SGSI PARA LA FUNDACIÓN SABEMOS CUIDARTE EN LA CIUDAD DE POPAYÁN
Autor	Saúl Aquilino Bautista Sarria
Palabras Claves	Seguridad Informática, Seguridad de la Información, Titular de la información, Fuente de información, Usuario, Dato personal, Habeas Data, Autorización, Base de Datos, Encargado del Tratamiento, Responsable del Tratamiento, Tratamiento, Fundación Sabemos cuidarte.
Descripción: El presente trabajo contiene una investigación básica sobre los activos, la valoración de los posibles riesgos y la proyección de algunas medidas para mejorar la Seguridad a nivel informático de la Fundación Sabemos Cuidarte, que es una Entidad del sector salud, que presta sus servicios a varias Entidades Promotoras de Salud (EPS) y que atiende a los usuarios directamente en la casa (atención domiciliaria) en la Ciudad de Popayán y en algunos Municipios aledaños.	
Fuentes Bibliográficas	BACA URBINA, Gabriel. Introduccíon a la Seguridad Informatica. Primera Edición Ebook. Mexico, 2016. CARPENTER, Jean-Francois. La Seguridad Informatica en la Pyme, Situación actual y mejores practicas. España, 2016. CORDOBA, Leyda. DELGADO, Wilson. Diseño de las Politicas de Control de Riesgos de la Seguridad de la Información para la Sede Central de la Gobernación del Putumayo (Mocoa). 2016 [Revisado en Agosto de 2017]. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Basicas, Tecnologia e Ingenieria. Obtenido de biblioteca virtual de la UNAD: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/8511/3/1124848759.pdf

GOMEZ VIEITES, Alvaro. Enciclopedoa de la Seguridad Informatica. Segunda Edición actualizada. España, 2010.

HUERTA, Antonio. Introducción al análisis de riesgos – Metodologías (II). 2012. Security A®twork. Disponible en: https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

MATALOBOS, Juan. Análisis de Riesgos de Seguridad de la Información. 2009. Universidad Politécnica de Madrid. Facultad de Informática. Disponible en: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

MOLINA, María. Propuesta de un Plan de Gestión de Riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral. 2015. Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación. Disponible en: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

PULIDO, Ana. MANTILLA, Jenith. Modelo para la implementación del Sistema General de Seguridad Informatica y Protocolos de Seguridad Informatica en la oficina TIC de la Alcaldia Municipal de Fusagasuga, Basados en la Gestión del Riesgo Informatico. Fusagasuga. 2016 [Revisado en Agosto de 2017]. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Basicas, Tecnologia e Ingenieria. Obtenido de biblioteca virtual de la UNAD: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/6327/1/35250225.pdf

REINA, Elkin. MORALES, Jose. Modelamiento de Procesos basados en el grupo de Normas Internacionales ISO/IEC 27000 para Gestionar el Riesgo y Seleccionar Controles en la Implementación del Sistema de Gestion de Seguridad de la Información. Pereira. 2014 [Revisado en Agosto de 2017]. Universidad Tecnologica de Pereira. Facultad de Ingenieria

Electrica, electronica, Fisica y Ciencias de la Computación. Programa de Ingenieria de Sistemas y Computación. Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4894/0058R364.pdf?sequence=1&isAllowed=y

RODRIGUEZ, Claudia. ALEMAN, Helena. Metodologías para el Análisis de Riesgos en los SGSI. 2015. Publicaciones e investigación. Revista Especializada en Ingeniería. Universidad Nacional Abierta a Distancia UNAD. Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

VANEGAS, Gonzalo. PARDO, Cesar. Hacia un Modelo para la gestión de riesgos de TI en MiPymes: MOGRIT. 2014. Artículo publicado en la Revista S&T. Universidad ICESI. Facultad de Ingeniería. Disponible en: https://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/download/1860/2398/

EBIOS. 2004. Secrétariat Général de la Défense Nationale. Republica de Francia. Disponible en: https://www.ssi.gouv.fr/archive/es/confianza/documents/methods/ebiosv2-section1-introduction-2004-02-05_es.pdf

¿Qué es la seguridad informática y como puede ayudarme? Universidad Internacional de Valencia. Disponible en: https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/#/plus

Magerit V 3: Metodología de Análisis y Gestión de riesgos de los sistemas de información. 2012. Portal Administración Electrónica. Disponible en:

	https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WtDN7S7wbIU

CONTENIDO:

Diseño de un sistema de gestión de seguridad informática - SGSI para la Fundación Sabemos Cuidarte en la ciudad de Popayán.

DESCRIPCIÓN DEL PROBLEMA:

La Fundación Sabemos Cuidarte tiene serios problemas con la seguridad de la información ya que no cuenta con un inventario de los equipos de cómputo y su licenciamiento, no se cuenta con planes de mantenimiento preventivo, las claves de acceso a la red inalámbrica se han convertido en públicas, no se cuenta con un procedimiento establecido para la realización de las copias de seguridad y de recuperación de información, no se realiza un proceso periódico de revisión de las actualizaciones del sistema operativo, se cuenta con antivirus libres configurados en su opción más básica; en parte todos estos inconvenientes se presentan porque no existe una persona responsable de esta actividades y no se cuentan con políticas de seguridad de información entre otras.

OBJETIVO GENERAL.

Diseñar un Sistema de Gestión de Seguridad Informática en la Fundación Sabemos Cuidarte.

OBJETIVOS ESPECÍFICOS.

- Realizar el inventario del hardware y software utilizados actualmente en la prestación de servicios en la Fundación Sabemos Cuidarte.
- Identificación de riesgos en el manejo de la seguridad de la información

existentes en la Fundación Sabemos Cuidarte.

- Definir las políticas de seguridad de la información para la Fundación Sabemos Cuidarte.

RESUMEN DE LO DESARROLLADO EN EL PROYECTO.

Para el desarrollo del presente proyecto se ejecutaran las siguientes etapas:

Etapa 1. Establecer diagnostico frente a los requisitos de la ISO 27001. Se realizará con los responsables el levantamiento de la información evaluando el grado de cumplimiento de cada requisito en la Fundación Sabemos Cuidarte, incluyendo la identificación de las necesidades de protección del sistema informático objeto de análisis (caracterización del sistema informático. Identificación de las amenazas y estimación de los riesgos. Evaluación del estado actual de la seguridad).

Etapa 2: Definir el plan de acción para el diseño del sistema de seguridad informática: En esta etapa se establecerá cronograma de trabajo incluyendo actividades, productos, fechas de ejecución, así como los responsables de la actividad.

Etapa 3: Diseño del Sistema de Seguridad que garantice minimizar los riesgos identificados en la primera etapa. Definir las políticas de seguridad. Definir las medidas y procedimientos a implementar, según las actividades aprobadas en el plan de acción establecido.

Se plantean las siguientes políticas así:

Protección de Datos Personales: Teniendo en cuenta que la Superintendencia de Industria y Comercio exige que todas la empresas que utilizan y manejan datos personales, realicen un proceso de registro de sus Políticas relacionadas con la Protección de los Datos Personales y teniendo en cuenta que para la fecha la Fundación Sabemos Cuidarte no cuenta con esta política se procede a plantear la respectiva Política Institucional.

La Política de Protección de Datos Personales se encuentra estructurada en las siguientes partes:

- Derechos de los titulares.
- Deberes de los responsables del tratamiento y encargados del

tratamiento.

- Responsable de la atención de peticiones, consultas y reclamos.
- Tratamiento al cual serán sometidos los datos y finalidad de los mismos.
- Políticas establecidas.
- Procedimiento para que los titulares puedan ejercer sus derechos

POLITICA DE SEGURIDAD INFORMATICA

Las políticas planteadas deben servir de instrumento y de guía a todos los Funcionarios de la Fundación para prevenir y ayudar en el proceso de protección de la información, por consiguiente estas directrices son de obligatorio cumplimiento

Se plantean los siguientes lineamientos:

- Con respecto a los equipos.
- Con respecto a las claves de acceso.
- Con respecto a los programas y la información.
- Con respectivo al uso de internet.
- Con respectivo al uso de correo electrónico institucional.
- Con el antivirus.
- Con el respaldos de información.
- Con el control de activos e información.
- Con el uso de la infraestructura informática.

METODOLOGÍA DE DESARROLLO:

Para el desarrollo del presente proyecto se utilizara el ciclo de Mejoramiento Continua PHVA (Planear, Hacer, Verificar y Actuar), teniendo en cuenta que es una de las estrategias más seguidas en la implementación de Sistemas de Gestión de Calidad y considerando que la Fundación Sabemos Cuidarte dentro de su estructura organizacional tiene establecida una Área de Calidad que trabaja bajo es lineamiento, de esta manera se mantiene y se trabaja bajo una misma línea u orientación dentro de la Entidad.

Conclusiones:

- Se realiza el diseño y el diligenciamiento de un hoja de vida para los equipos de cómputo, con la cual se recoge toda la información tanto del hardware, como del software y otra información considerada relevante de los equipos utilizados actualmente en la prestación de servicios en la Fundación Sabemos Cuidarte.
- Se realiza el diseño y se plantean una serie de actividades y de políticas orientadas a mejorar la seguridad de la información de la fundación Sabemos cuidarte y quedaría pendiente que la Entidad realice los respectivos procesos de revisión, aprobación implementación y seguimiento.
- Este proceso con la Fundación Sabemos Cuidarte fue muy productivo para mí, teniendo en cuenta que se pudo identificar una gran cantidad de falencias al interior de la organización y se poner en práctica los conocimientos adquiridos en el proceso de capacitación con la Universidad.

Recomendaciones:

- La Fundación Sabemos Cuidarte debe realizar la implementación de un acta mediante la cual se le hace entrega, de manera oficial, al funcionario de su respectivo equipo de cómputo y garantizar que conozca las directrices institucionales con relación al uso correcto de estos equipos.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para poder legalizar su software, adquirir un sistema de protección de antivirus y realizar copias de seguridad de la información.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para poder gestionar la actualización y rediseño de su página web, tomar decisiones con su presencia en las redes sociales e implementar el uso del sistema de correo electrónico corporativo.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para

poder adquirir e instalar un sistema eléctrico de respaldo que les permita salvaguardar la información en caso de cortes de energía.

- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para poder programar y llevar a cabo mantenimientos preventivos de todos los equipos de cómputo.
- La Fundación Sabemos Cuidarte debe organizar con su área de Contabilidad un proceso para dar de baja los equipos de cómputo que hayan cumplido su respectivo ciclo de vida.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para poder realizar la transición de la historia clínica manual a la historia clínica electrónica.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para empezar a trabajar en el proceso de transición a la Facturación electrónica.
- La Fundación Sabemos Cuidarte debe realizar las gestiones pertinentes para programar y realizar capacitaciones a todos su personal en el tema de sistemas informativos y de seguridad de la información.
- La Fundación Sabemos Cuidarte debe estudiar la posibilidad de contratar (de planta o por prestación de servicios) a un Profesional que los apoye o que sea el responsable del área de Sistemas.