DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA ADMINISTRATIVA DE LA E.S.E HOSPITAL REGIONAL NOROCCIDENTAL IPS ABREGO BAJO LA NORMA ISO 27001:2013

JUAN PABLO ÁLVAREZ PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

ABREGO, NORTE DE SANTANDER

2019

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA ADMINISTRATIVA DE LA E.S.E HOSPITAL REGIONAL NOROCCIDENTAL IPS ABREGO BAJO LA NORMA ISO 27001:2013

JUAN PABLO ÁLVAREZ PEREZ

Trabajo de grado presentado como requisito para optar por al título de:

Especialista en Seguridad Informática

Asesor de Proyecto:

Esp. Daniel Felipe Palomo Luna

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

ABREGO, NORTE DE SANTANDER

2019

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Abrego, Mayo 2019

DEDICATORIA

Dedico esta monografía en primera instancia a Dios por haberme dado la fortaleza y sabiduría para lograr mis objetivos, además de su infinita bondad y amor.

A mi Madre Quien ha sido el apoyo inquebrantable durante todo mi existir, por los ejemplos de perseverancia y constancia que la caracterizan, las cuales me ha infundado siempre y son fuente de toda mi vitalidad.

A mi padre (QEPD) quien fue el pilar fundamental de mi familia, el cual con su arduo trabajo y emprendimiento sentó las bases para el futuro de lo que hoy soy.

A mi esposa e hijas que son el motor de mi vida, que con su apoyo incondicional y desinteresado son la razón de seguir cosechando nuevos triunfos.

AGRADECIMIENTOS

Quiero agradecer a las directivas de la Empresa Social del Estado hospital regional noroccidental IPS Abrego por la confianza depositada en mí para la realización de este proyecto.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

Activo: se refiere a cualquier elemento que posee la compañía.

Amenaza: es un suceso no esperado que puede ocasionar daño a un sistema de información o a la compañía.

Confidencialidad: característica de la información que está disponible solo para personas o sistemas autorizados.

Disponibilidad: característica de la información a la cual pueden acceder solo las personas autorizadas cuando sea necesario.

E.S.E: hace referencia al acrónimo de “Empresa Social del Estado”, en su mayoría son clínicas u hospitales.

Integridad: característica de la información que es modificada solo por personas o sistemas autorizados y de una forma permitida.

IPS: hace referencia al acrónimo “Instituto prestador de salud”, estas son todas las instituciones en Colombia que prestan los servicios médicos de consulta, hospitalarios y clínicos y de cuidados intensivos.

Riesgo: es un evento al cual se está expuesto por ausencia de controles.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: hace referencia al acrónimo “sistema de gestión de la seguridad de la información”, hace referencia a un conjunto de políticas de administración de la información.

Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

RESUMEN

El desarrollo de este proyecto permite conocer la situación actual de la Empresa Social del Estado hospital regional noroccidental IPS Abrego, en cuanto a su objetivo de diseñar un sistema de seguridad de la información que sirva como respaldo de las actividades realizadas en el área administrativa, agilizando el análisis de riesgos, confiabilidad y disponibilidad a los que se ve expuesta la información en el caso particular del área de contabilidad, la cual busca poder minimizar y controlar las amenazas que pueden estar presentes en el flujo, almacenamiento y ejecución de la información. Este sistema se realizó bajo un proceso sistemático, documentado y conocido por toda la organización para ser revisado y actualizado constantemente, con el uso de una metodología que permitiera indagar como era su funcionamiento y la incidencia directa e indirecta sobre el medio operativo de la empresa, ya que la información contable es de vital importancia para la toma de decisiones en el funcionamiento de esta.

El desarrollo del proyecto está basado en la norma de gestión de seguridad ISO/IEC 27001:2013 la cual proporciona las directrices, practicas, selección, implementación y gestión de los controles, teniendo en cuenta el medio ambiente, riesgo y seguridad de la información para su diseño. La metodología empleada se basó en el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) la cual ofrece una opción que permite mantener la competitividad de los servicios, mejorar la calidad, reduce los costos, mejora la productividad, la confiabilidad de la información, la toma de decisiones, supervivencia de la empresa y aumenta la rentabilidad de esta.

El Diseño del Sistema de Gestión de Seguridad Informática fue concebido para suministrar un conjunto de actividades que deben realizarse mediante procesos sistemáticos enfocados en el proceso contable de la Empresa Social del Estado hospital regional noroccidental IPS Abrego, la cual genera un impacto en la continuidad del negocio y del funcionamiento de los demás procesos dentro de la empresa. Su objetivo está orientado a generar políticas y controles de seguridad para que los riesgos sean conocidos, asumidos, gestionados y minimizados, de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la misma.

SUMMARY

The development of this project allows us to know the current situation of the State Social Enterprise of the regional hospital, the north-western IPS Abrego, in terms of its objective of designing an information security system that serves as a backup for the activities carried out in the administrative area, speeding up the analysis of risks, reliability and availability to which the information is exposed in the particular case of the accounting area, which seeks to minimize and control the threats that may be present in the flow, storage and execution of the information. This system was carried out under a systematic process, documented and known throughout the organization to be constantly reviewed and updated, with the use of a methodology that would allow to investigate how was its operation and the direct and indirect impact on the operating environment of the company, since the accounting information is of vital importance for the decision making in the operation of this.

The development of the project is based on the security management standard ISO / IEC 27001: 2013 which provides the guidelines, practices, selection, implementation and management of the controls, taking into account the environment, risk and security of information for his design. The methodology used was based on the PHVA cycle (Plan, Do, Verify and Act) which offers an option that maintains the competitiveness of services, improves quality, reduces costs, improves productivity, reliability of information, making decisions, survival of the company and increases the profitability of this.

The Design of the Information Security Management System was conceived to provide a set of activities that must be carried out through systematic processes focused on the accounting process of the State Social Enterprise of the Northwest Regional Hospital IPS Abrego, which generates an impact on business continuity and the operation of the other processes within the company. Its objective is aimed at generating security policies and controls so that the risks are known, assumed, managed and minimized, in a documented, systematic, structured, continuous, repeatable, efficient and adapted to the changes that occur in it.

INTRODUCCION

La información es uno de los activos esenciales y valiosos de una organización y los costos que generan la pérdida y recuperación de este activo son muy altos. Dada esta situación se debe invertir en herramientas y procesos que permitan tener un control de la información.

Constantemente la información está expuesta a diferentes amenazas que ponen en peligro la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad, conservación de los datos, la estabilidad de los procesos, los niveles de competitividad, la imagen corporativa, la rentabilidad y la legalidad, aspectos necesarios para alcanzar los objetivos estratégicos de la organización.

El Sistema de Gestión de Seguridad de la Información o SGSI, provee una serie de controles, políticas, procedimientos y acciones que servirán para identificar, medir, vigilar, limitar, informar y revelar los riesgos a que se encuentre expuesta los sistemas informáticos. Un SGSI establece un completo plan de acciones que buscan solucionar los problemas técnicos de seguridad, organizativos y legislativos mediante el análisis de riesgos, mejorando y manteniendo la seguridad de la información corporativa y garantizando una continuidad de negocio.

Gracias al desarrollo de este proyecto se diseñó un Sistema de Gestión de Seguridad de la Información, el cual permitirá comenzar a salvaguardar los recursos informáticos de la Empresa Social del Estado hospital regional noroccidental IPS Abrego, ayudando a la organización a cumplir sus objetivos.

Durante el desarrollo de este proyecto se utilizaron los métodos de investigación inductiva y deductiva, las cuales permitieron la identificación o determinación de que controles o aspectos de la política son aplicables al Área de Contabilidad de la E.S.E Hospital Regional noroccidental I.PS Abrego, así como descartar aquellos que no sean necesarios. Además, se aplicaron las siguientes técnicas de recolección de información: Observación Directa, Entrevistas, Encuestas, Listas de chequeo, Datos estadísticos, Evaluación en base a experiencia, para así desarrollar la declaración de aplicabilidad según la metodología *Magerit* y cumplir con los objetivos de este proyecto.

1. DESCRIPCION DEL PROBLEMA

Al analizar la infraestructura tecnológica del Área Administrativa de la Empresa Social del Estado (E.S.E) Hospital Regional Noroccidental Instituto Prestador de Salud (I.P.S) Abrego, es notable el crecimiento experimentado con el paso de los años, este hecho ha provocado que los controles a nivel de seguridad de la información que se encuentran vigentes, no sean los adecuados para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información, razón por la cual es necesario que sean revisados y mejorados.

En caso de no remediarse la situación anteriormente expuesta, se eleva exponencialmente el riesgo de ocurrencia de incidentes de seguridad, pérdida de información o disponibilidad de los servicios y sistemas que sustentan la operación del Área Administrativa del Hospital, esto redundaría en pérdidas económicas y podría generar desconfianza sobre la imagen que mantiene la E.S.E Hospital Regional Noroccidental I.P.S Abrego en el medio de la salud.

En la actualidad las compañías están expuestas a múltiples riesgos y amenazas que atentan contra la integridad, confidencialidad y disponibilidad de la información, Esto obliga a plantearse la siguiente pregunta

¿Cuál sería la mejor solución para que una compañía pueda gestionar adecuadamente la información, siendo este el activo más importante de la misma?

2. JUSTIFICACIÓN

Para el diseño de un sistema de gestión de seguridad de la información basándose en normas reconocidas internacionalmente como lo es la ISO 27001:2013, se debe tener en cuenta en primer lugar, proporcionar condiciones de gobernabilidad y vialidad necesarias para que la seguridad de la información garantice el cumplimiento de los objetivos estratégicos de una empresa, compañía u organización. Esto, mediante la correcta protección, que asegure que la función de la información de la entidad en materia financiera, administrativa y operativa, entre otras, pueda ser cumplida a cabalidad.

Un adecuado sistema de gestión de seguridad de la información, evidencia a modo tangible un alto grado de compromiso de la organización con el resguardo de la información sensible que se maneja a nivel gerencial, de este modo, se proveen herramientas requeridas para gestionar de manera correcta y eficaz elementos de riesgos que atentan contra la seguridad de la información. Esto, por supuesto, genera confianza en todos los sectores inherentes a la organización. Debido a esto, establecer un adecuado sistema de gestión de seguridad informática, implica que la organización goza de un modelo de seguridad activo, dinámico, coherente y estratégico, acorde con los requerimientos que este sector demanda.

Para el área administrativa de la E.S.E Hospital Regional Noroccidental IPS Abrego, contar con un adecuado sistema de gestión de seguridad, le permitirá a la entidad tramitar de modo efectivo los riesgos que conlleva la seguridad de la información, pudiendo identificar amenazas que puedan comprometer la integridad, disponibilidad y confidencialidad de los activos de información, pudiendo con la anticipada identificación, ejecutar las herramientas adecuadas para reducir el impacto en caso de presentarse riesgos referentes a esta área.

Además, un sistema de gestión de seguridad de la información permite a la E.S.E Hospital Regional Noroccidental IPS Abrego alinear las necesidades de seguridad con los objetivos estratégicos de la organización. Esto, mediante mecanismos compuestos por una estructura organizacional con roles y responsabilidades dentro de un marco de políticas coherentes con procesos y procedimientos orientados a crear, originar y desarrollar una cultura de seguridad en todos los niveles de la organización, para de este modo tramitar de manera optima la seguridad de la información.

De esta manera, se fortalece cada uno de las áreas de la entidad, integrando a cada sector de la organización; cimentando los pilares fundamentales de la seguridad que involucran la integridad, confidencialidad y disponibilidad de la información, lo cual ayuda a fomentar y garantizar el fiel manejo de esta.

En este sentido, un correcto diseño de seguridad de información proporciona herramientas adecuadas que proporcionan elementos necesarios para lograr de manera óptima objetivos de seguridad, tales como:

- Promover una cultura de seguridad en la información en todos los sectores de la organización.
- Infundar sentido de pertenencia en los temas relacionados con la seguridad en los funcionarios de la organización, logrando en este sentido, la participación activa de toda la empresa en la planeacion, descripción, tipificación y ejecución de inspecciones y disposiciones enfocadas en proteger la información vital de la E.S.E Hospital Regional Noroccidental IPS Abrego.
- Evitar fugas de información por ataques informáticos externos e internos.
- Permitir la correcta identificación de riesgos de seguridad de la información existentes, haciéndolos reconocibles por todos los funcionarios y en todas las áreas de la organización, logrando con esto gestionar de manera adecuada y pertinente la información.
- Promover una correcta cultura interna de la organización en materia de protección de la información, evitando inversiones innecesarias de tecnologías costosas destinadas a la seguridad de la información, que resultan invalidadas si los mecanismos de control no son responsablemente acatados por todos los integrantes de los distintos niveles de la estructura organizativa de la empresa.

Finalmente, el diseño de gestión de seguridad de la información ayuda a cuantificar los niveles de cumplimiento de los indicadores de seguridad de la información dentro de la estructura de organización de la E.S.E Hospital Regional Noroccidental IPS Abrego. De modo tal, que la información vital de la empresa se verá protegida íntegramente mediante mecanismos de controles eficientes que proporcionen y garanticen una fiabilidad alta de la información que circula dentro de la organización.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información para el área administrativa E.S.E Hospital Regional Noroccidental IPS Abrego bajo la norma ISO 27001:2013

3.2 OBJETIVOS ESPECÍFICOS

- Definir el alcance y límites del SGSI para el área administrativa de la E.S.E Hospital Regional Noroccidental IPS Abrego.
- Realizar inventario de los activos tecnológicos.
- Elaborar la política del SGSI.
- Elaborar la definición del SOA (Aplicabilidad).
- Identificar, evaluar y ejecutar el análisis de riesgos de los activos informáticos.

4. MARCO REFERENCIAL

4.1 MARCO TEORICO

Las políticas y los procedimientos de seguridad informática surgen como una herramienta para concientizar a cada uno de los miembros de una organización sobre la importancia y la confidencialidad de la información, lo cual favorece al desarrollo y el buen funcionamiento de la organización. Deben considerarse como reglas a cumplir que surgen para evitar problemas y que se establecen para dar soporte a los mecanismos de seguridad implementados en los sistemas y en las redes de comunicación.

4.1.1 Norma ISO 270002. Esta norma ofrece distintas directrices necesarias para proporcionar mayor seguridad en la información que circula por una organización empresarial. Además, vincula elementos tales como; selección, riesgo, implementación y gestión de los controles, teniendo en cuenta el medio ambiente y la seguridad de los datos generados por el grupo y/o proyecto organizacional, encaminados a mejorar las prácticas de gestión de seguridad de cualquier empresa, institución u organización donde el cuido de la información siempre es importante. Esta norma cuenta con 114 controles los cuales se agrupan en 14 capítulos que se describirán a continuación:[1].

4.1.1.1 Políticas de Seguridad de la Información. Este capítulo se basa en una adecuada política de seguridad, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior.

4.1.1.2 Organización de la Seguridad de la Información. Este capítulo buscan estructurar un marco de seguridad eficiente mediante los roles, tareas, seguridad, etc. como en los dispositivos móviles. Se tendrá presente que cada vez es mayor el peso que está ocupando el teletrabajo dentro de las empresas, y por ello, se deben tener en cuenta todas sus características especiales para que ningún momento la seguridad de la información se vea afectada.

4.1.1.3 Seguridad relativa a los recursos humanos. Este apartado trata de concientizar y formar al personal en términos de empleo de la información en el desarrollo de sus actividades, además de la importancia que tiene promover,

[1] MARTINEZ, Sergio. Normas de uso común para proyectos de TI (ISO). (En línea) (Citado el 27 de junio del 2014). Disponible en: https://checomart.wordpress.com/2014/01/

mantener y mejorar el nivel de seguridad adecuándolo a las características de los datos y la información que maneja es vital y uno de los objetivos que se debe perseguir.

4.1.1.4 Gestión de activos. Trata la información como un activo y en cómo se deben establecer las medidas adecuadas para guardarlos de las incidencias, fugas o alteración no deseada.

4.1.1.5 Control de acceso. Controlar quien accede a la información es un aspecto relevante. Todas las personas de una organización necesitan acceder para realizar sus actividades diarias a todos los datos, entendiéndose que hay roles que necesitan un mayor acceso y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de los usuarios, gestión de los privilegios de acceso, etc. siendo algunos de los protocolos que se incluyen en este apartado.

4.1.1.6 Criptografía. Tratando la información sensible o crítica, puede ser interesante o menester utilizar diferentes técnicas criptográficas para proteger y garantizar su autenticidad, confidencialidad e integridad.

4.1.1.7 Seguridad física y del entorno. La seguridad también es física, es decir, una simple labor de no dejar las pantallas e impresoras en zonas que sean fácilmente accesibles, por parte del personal externo a los documentos con los que se están trabajando, no sólo permitirá gestionar de forma adecuada la seguridad, sino que se acabarán convirtiendo en hábitos que aportan eficiencia en la gestión.

4.1.1.8 Seguridad de las operaciones. La protección del *software* malicioso, copias de seguridad, control de *software* en explotación, gestión de vulnerabilidad.

4.1.1.9 Seguridad de las comunicaciones. Proteger de forma adecuada los medios de transmisión de estos datos es un aspecto muy clave que la norma plantea.

4.1.1.10 Adquisiciones Desarrollo y mantenimiento de los sistemas de información. La seguridad no es un aspecto de un área en concreto, ni de un determinado proceso, ya que es general, abarca toda la organización y tiene que estar presente como elemento transversal clave dentro del ciclo de vida del sistema de gestión.

4.1.1.11 Relación de proveedores. Cuando se establecen las relaciones con terceras partes, como puede ser proveedores, se deben establecer medidas de seguridad pudiendo ser muy recomendable e incluso menester en determinados casos.

4.1.1.12 Gestión de incidentes de seguridad de la información. Se debe estar preparados para cuando estos incidentes ocurran, dando una respuesta rápida y eficiente para prevenirlos en el futuro.

4.1.1.13 Aspectos de seguridad de la información para la gestión de la continuidad de negocio. Sufrir una pérdida de información relevante y no poder recuperarla de alguna forma puede poner en peligro la continuidad de negocio de la organización.

4.1.1.14 Cumplimiento. Este módulo trata de la legislación, normas y políticas aplicables que se encuentre relacionadas con este campo y con las que conviven en las organizaciones. Estas ocupan un enorme lugar en cualquier sistema de gestión y deben garantizar que se cumple y que están actualizados con los últimos cambios siendo esencial para no encontrar sorpresas no gratas.

4.1.2 Beneficios. La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios en pro de los objetivos de la organización y asegurar beneficios económicos. A continuación, una breve mención a los principales aspectos a considerar:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorias externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 1800).

- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

4.1.3 Sistema de Gestión de la Seguridad de la Información (SGSI). Son los procedimientos que permiten que una empresa preste un servicio o elabore un producto de manera confiable cumpliendo con las normas internacionales; garantizando que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, adaptada a los cambios que se produzcan en el entorno y las tecnologías garantizando la preservación de su confidencialidad, integridad y disponibilidad, así como los servicios implicados en su tratamiento dentro de la empresa. De esta manera, los tres términos son el pilar en la que se fundamenta la seguridad de la información, los cuales se explican a continuación:

- Confidencialidad: La información presente en la organización no se encuentra a disposición ni se revela a individuos, entidades o procesos; está protegida de personal no autorizadas.
- Integridad: La información se muestra como se pretende, sin modificaciones inapropiadas.
- Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- Para garantizar la seguridad en la información, esta es tratada de forma idónea, se debe hacer uso de un procedimiento sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI. Tal como lo explica la Norma Técnica Colombiana2

[2]NORMA TÉCNICA COLOMBIANA. Sistema de Gestión de la Seguridad de la Información, ¿Qué es un SGSI? (En línea) (Citado el 27 de junio del 2018). Disponible en: Disponible en: http://www.iso27000.es/sgsi.html.

4.1.4 Aplicación de un SGSI. El Sistema de Gestión de la Seguridad de la Información (SGSI) establece políticas y procedimientos basados en los objetivos de negocio de la organización, como prioridad de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. A continuación, en la siguiente figura se observa una secuencia de riesgos que explica los riesgos del SGSI.

Figura 1. Riesgos SGSI

Fuente: http://www.iso27000.es/sgsi.html.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de estos.

4.1.5 Documentación de un SGSI. En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001. Según como se observa a continuación en la figura 2.

Figura 2. Documentación del sistema de seguridad

Fuente: http://www.iso27000.es/sgsi.html.

- **Manual de seguridad**: Documentación en la que se basa todo el sistema, alcance, objetivos, responsabilidades, políticas y principales directrices del SGSI.
- **Procedimientos**: Documentación que asegura la realización de forma idónea la planificación, operación y control de los procesos de seguridad de la información presente en la organización.
- **Instrucciones *Cheklists* formularios**: Documentación que determina la ejecución de las tareas y las actividades específicas correspondientes a la seguridad de la información.
- **Registros:** Documentación que certifica de una forma imparcial y objetiva el cumplimiento de los requisitos del SGSI; estos registros se basan con anteriores niveles.

De manera específica, ISO 27001 indica que un SGSI debe estar integrado por los siguientes documentos:

- **Alcance del SGSI:** Identificación clara y precisa de las áreas, divisiones, procesos, dependencias y sus respectivas relaciones y limitantes que abarca el SGSI.
- **Política y objetivos de seguridad:** Documento que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- **Procedimientos y mecanismos de control que soportan al SGSI:** Todos los procedimientos que regulan el propio funcionamiento del SGSI.
- **Enfoque de evaluación de riesgos:** Descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación con los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables. Tal como lo explica la Norma Técnica Colombiana[3].
- **Informe de evaluación de riesgos:** Estudio como resultante de cotejar y aplicar la metodología de evaluación mencionada con anterioridad a los activos de información de la organización.
- **Plan de tratamiento de riesgos:** Documento el cual, a partir de la evaluación del riesgo y los objetivos de control establecidos identifica las acciones, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información.
- **Procedimientos documentados:** Todos aquellos necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para el buen funcionamiento de los controles implantados.
- **Registros:** Documentos que evidencian el constante y correcto funcionamiento del SGSI.
- **Declaración de aplicabilidad**: Documento en el que describen los objetivos de control y controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

4.1.6 Aspectos de seguridad que cubre un SGSI. Niveles de seguridad:

- **Lógica:** Confidencialidad, integridad y disponibilidad del *software* y datos de un SGI.
- **Organizativa:** Relativa a la prevención, detección y corrección de riesgos.
- **Física:** Protección de elementos físicos de las instalaciones: Protección a servidores, PCs, etc.
- **Legal:** Cumplimiento de la legislación vigente

[3]Ibíd., p. 5.

4.1.7 Revisión del SGSI. La dirección de la organización, al menos una vez por año asigna la tarea de revisar el SGSI, en pro de asegurar que continúe siendo adecuado y eficaz. Por ende, ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.
- En la información obtenida anteriormente, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:
- Modificar los procesos y controles que afectan la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, marco legal, procesos de negocio, obligaciones contractuales, criterios de aceptación de riesgos y niveles de riesgo.
- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles.

4.2 MARCO CONCEPTUAL

A continuación, se presentan algunas definiciones importantes relacionadas al SGSI que se busca diseñar

4.2.1 Control. El control es un proceso por el cual la administración verifica si la acción ocurrente concuerda con la situación que debería presentarse. Permite que se realicen los ajustes o correcciones necesarias en caso de que se detecten eventos que escapan a la naturaleza del proceso.

Es una etapa primordial en la administración, pues, por más que una empresa cuente con magníficos planes, una estructura organizacional adecuada y una

dirección eficiente, no se podrá verificar la situación real de la organización si no existe un mecanismo que verifique e informe si los hechos van de acuerdo con los objetivos Según la *International Standard Iso/Iec* [4].

4.2.2 Declaración de aplicabilidad. La declaración de aplicabilidad o SOA, del inglés *Statement of Applicability*, es un documento que describe los objetivos de control y controles relevantes y aplicables al alcance del SGSI de la empresa, en función de la política y conclusiones del proceso de evaluación y tratamiento del riesgo. En el documento básicamente van 2 campos: Uno donde va el control específico y una columna donde va la aplicabilidad, donde se justifica la decisión tomada sobre si el control es aplicable o no. Tal como lo explica la Norma Técnica Colombiana [5]

4.2.3 Direccionamiento estratégico. Es una disciplina que integra varias estrategias, que incorporan diversas tácticas. El conocimiento, fundamentado en información de la realidad y en la reflexión sobre las circunstancias presentes y previsibles, coadyuva a la definición de la "Dirección Estratégica" en un proceso conocido como "Planeamiento Estratégico", que compila tres ítems, estrategia corporativa, estrategia de mercadeo y estrategia operativa o de competitividad. Según Trujillo[6]

4.2.4 Estructura organizacional. La estructura organizacional puede ser definida como las distintas maneras en que puede ser dividido el trabajo dentro de una organización para alcanzar luego la coordinación del mismo orientándolo al logro de los objetivos.

4.2.5 Gestión de riesgos. Es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular, tal como lo explica la Norma Técnica Colombiana [7]

---

[4]INTERNATIONAL STANDARD ISO/IEC 17799. (En línea) (Citado el 16 de Mayo del 2005). Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf.

[5] Sistema de Gestión de la Seguridad de la Información, ¿Qué incluye un SGSI? Op. cit., p 6.

[6]TRUJILLLO, Freddy. C.E Soft Colombia. (En línea) (Citado el 15 de septiembre del 2010). Disponible en: http://cesoftco.net/2cmc/PAPER.htm.

[7]NORMA TÉCNICA COLOMBIANA. Gestión de riesgo. (En línea) (Citado el 23 de Enero del 2016). Disponible en: https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_riesgos.

4.2.6 Información. Es un conjunto estructurado de datos, los cuales se procesan para construir un mensaje. Este mensaje es entregado por un emisor a un receptor, o proporcionado por un sistema de información. La información, ya sea impresa, almacenada digitalmente o hablada, actualmente es considerada como un activo dentro de las compañías y que se debe proteger, ya que es de gran importancia.

4.2.7 Política de seguridad. Declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran. Esto según Reynolds[8].

4.2.8 Riesgo. Se define como cualquier impedimento, obstáculo, amenaza o problema que pueda impedirle a la empresa que alcance un objetivo. Se puede ver también como la posibilidad de sufrir un daño o pérdida. Se mide en términos de impacto y probabilidad de ocurrencia, Tal como lo explica la Norma Técnica Colombiana [9].

4.2.9 Seguridad de la información. Es la preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

4.2.10 Sistema de gestión de Seguridad de la Información (SGSI). Un SGSI o ISMS, de sus siglas en inglés (*Information Security Management Systems*), es la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información. Según lo explica la Norma Técnica Colombiana[10].

4.3 MARCO LEGAL

El gran impacto generado por las nuevas tecnologías a nivel mundial y al cual no es ajeno Colombia, ha generado la necesidad de tener una legislación que proteja

[8] REYNOLDS Jean y HOLBROOK, Paul. RFC 1244: Site Security Handbook. 1 ed. New York: McGraw-Hill, 1991. 102 p.
[9]NORMA TÉCNICA COLOMBIANA. Administración De Riesgos. AS/NZS 4360. (En línea) (Citado el 13 de Octubre del 2014). Disponible en: http://auditoriauc20102mivi.wikispaces.com/file/view/Resumen_NTCAS436020101700422184.pdf.
[10]NORMA TÉCNICA COLOMBIANA. Sistema de Gestión de la Seguridad de la Información, ¿Qué es un SGSI? Op. cit. p 2.

a todos los implicados en el uso y el tratamiento que se hace de la información a través de estos nuevos sistemas tecnológicos, según Blázquez [11], El Marco Legal para el SGSI es continuamente cambiante ya que día a día surgen nuevas necesidades con el fin de proteger a quienes hacen uso de la información, ya que surgen variados y efectivos métodos de fraude conocidos como delitos informáticos que principalmente buscan afectar la seguridad de la información en las empresas. Por esta razón uno de los factores importantes en la implementación de SGSI es el cumplimiento de la legislación vigente.

4.3.1 Derechos de autor. Las siguientes son aquellas normas o leyes que se relacionan con el tema en cuestión:

- **Decisión 351 de la C.A.N:** Tienen por finalidad reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino. Según disposición del Congreso de la Republica de Colombia[12].
- **Ley 23 de 1982:** Contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia. A partir de esta se empiezan a regular los aspectos legales relacionados con el *software* y a partir de esta regulación se crean nuevas normas y algunas circulares de la DNDA (Dirección Nacional del Derecho de Autor) reglamentando y ajustando la protección jurídica del *software*. Según disposición del Congreso de la Republica de Colombia [13].
- **Decreto 1360 de 1989:** Este decreto contiene los lineamientos que se deben tener en cuenta en el momento de realizar la inscripción del soporte lógico (*software*) en el Registro Nacional del Derecho de Autor, se debe tener en cuenta tanto el programa de computador, descripción del programa y material auxiliar, como la información completa del solicitante, Según disposición del Congreso de la Republica de Colombia [14].
- **Ley 44 de 1993:** Ley que trata de las actividades, escritos o demás que podrán ser inscritos en el Registro Nacional del Derecho de Autor, también habla sobre los beneficios u objetivos que se tienen al realizar la inscripción, y

[11]BLÁZQUEZ Entonado. Sistema de la información y la educación, Florentino [(En línea) (Citado el 26 de Mayo del 2015). Disponible en: http://www.ub.edu/prometheus21/articulos/obsciberprome/blanquez.pdf

[12] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado. Diario Oficial. Bogotá, D.C: El Congreso, 2009. 18 p.

[13]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 23. (28, enero, 1982). Sobre derechos de autor. Diario Oficial. Bogotá, D.C: El Congreso, 1982. 23 p.

[14]COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1360. (23, junio, 1989). Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor. Diario Oficial. Bogotá, D.C: El Congreso, 1989. 63 p.

así mismo habla de las multas que se deberán cumplir en el momento de violar o incumplir este acuerdo, Según disposición del Congreso de la Republica de Colombia[15].

- **Decreto 460 de 1995:** En este decreto se reglamenta el Registro Nacional de Derecho de Autor, principalmente la forma en cómo está formado y su finalidad frente a los suscriptores. También trata sobre la veracidad del contenido consignado en el Registro Nacional de Derecho de Autor, es de resaltar que en este decreto dejan claro que toda inscripción realizada en el Registro Nacional de Derecho de Autor es de carácter público, Según disposición del Congreso de la Republica de Colombia[16].
- **Decreto 162 de 1996:** Decreto que habla sobre la conformación de sociedades de gestión colectiva sin ánimo de lucro de los titulares de derechos de autor o de derechos conexos. Por tanto, en este decreto se reglamenta la Decisión Andina 351 de 1993 y la Ley 44 de 1993, en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos, Según disposición del Congreso de la Republica de Colombia[17].
- **Ley 545 de 1999:** Esta ley trata de los derechos que están a favor de los artistas, intérpretes o ejecutantes, productos de fonogramas y organismos de radiodifusión. Por medio de esta ley se aprueba el "Tratado de la OMPI – Organización Mundial de la Propiedad Intelectual- sobre Interpretación o Ejecución y Fonogramas (WPPT)", adoptado en Ginebra el veinte (20) de diciembre de mil novecientos noventa y seis (1996), Según disposición del Congreso de la Republica de Colombia[18].
- **Ley 565 de 2000:** Esta ley trata sobre las protecciones y derechos que favorecen a las TIC'S, manteniendo el equilibrio entre los derechos de autor y los intereses del público en general, en particular en la educación, la investigación y el acceso a la información, como se refleja en el convenio de Berna. Por medio de esta ley se aprueba el "Tratado de la OMPI – Organización Mundial de la Propiedad Intelectual- sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos

[15]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 44. (5, febrero, 1993). por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. Diario Oficial. Bogotá, D.C: El Congreso, 1993. 14 p.

[16] COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 460. (5, marzo, 1995). Por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal. Bogotá, D.C: El Congreso, 1995. 2 p.

[17] COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 162. (22, enero, 1996). Por el cual se reglamenta la Decisión Andina 351de 1993 y la Ley 44 de 1993, en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos. Bogotá, D.C: El Congreso, 1995. 26 p.

[18] COLOMBIA. MINISTERIO DEL INTERIOR. Ley 545 de 1999. por medio de la cual se apreueba el tratado de la OMPI sobre interpretación o ejecución y fonogramas. Bogotá, D.C: El Ministerio, 1999. 15 p.

noventa y seis (1996), y dispuesto por el Congreso de la Republica de Colombia [19].

- **Ley 603 de 2000:** Es utilizada por la DIAN para realizar verificaciones y enfatiza en la obligación de declarar en los informes de gestión el cumplimiento de las normas que protegen el *software*. Según disposición del Congreso de la Republica de Colombia[20].
- **Ley 719 de 2001**: Esta ley trata de las tarifas que se deberán pagar como derechos de autor por el uso de la obra suscrita. En esta ley se modifican las Leyes 23 de 1982 y 44 de 1993 y se dictan otras disposiciones, Según disposición del Congreso de la Republica de Colombia[21].

4.3.2 Comercio electrónico y firmas digitales. Se explica a continuación:

- **Ley 527 de 1999:** Por medio de esta ley se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación, Según disposición del Congreso de la Republica de Colombia[22].
- **Decreto 1747 de 2000:** Este decreto reglamenta parcialmente la ley 527 de 1999, especialmente en lo relacionado con las entidades de certificación cerradas y abiertas, Según disposición del Congreso de la Republica de Colombia[23].

[19]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 565. (2, febrero, 2000). por medio de la cual se aprueba el "Tratado de la OMPI –Organización Mundial de la Propiedad Intelectual– sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996). Diario Oficial. Bogotá, D.C: El Congreso, 2000. 18 p.

[20]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 603. (27, julio, 2000 Por la cual se modifica el artículo 47 de la Ley 222 de 1995. Diario Oficial. Bogotá, D.C: El Congreso, 2000. 21 p.

[21]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 719. (24, febrero, 2001 Por la cual se modifican las Leyes 23 de 1982 y **44** de 1993 y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C: El Congreso, 1999. 187 p.

[22]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527. (18, agosto, 1999). por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Oficial. Bogotá, D.C: El Congreso, 1999. 15 p.

[23]COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1747. (11, septiembre, 2000). Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. El Presidente de la República de Colombia, en ejercicio de las facultades constitucionales y legales, en especial de las conferidas en el numeral 11 del artículo 189 de la Constitución Política y en desarrollo de lo previsto en la Ley 527 de 1999. Diario Oficial. Bogotá, D.C: El Congreso, 2000. 63 p.

- **Resolución 26930 de 2000:** En esta resolución se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores, Según disposición del Congreso de la Republica de Colombia[24].

4.3.3 Protección de datos personales. Se explica a continuación:

- **Ley 1581 de 2012:** La ley de protección de datos personales – Ley 1581 de 2012 – es una ley que complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales, Según disposición del Congreso de la Republica de Colombia[25].
- **Ley 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, Según disposición del Congreso de la Republica de Colombia[26].
- **Ley 1273 de 2009:** (La cual añade dos nuevos capítulos al Código Penal), Según disposición del Congreso de la Republica de Colombia[27]

Capítulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Capitulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver en el primer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información,

[24]COLOMBIA. CONGRESO DE LA REPÚBLICA. Resolución 26930. (26, octubre, 2000). Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores. Diario Oficial. Bogotá, D.C: El Congreso, 2000. 69 p.

[25]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581. (17, octubre, 2002). *Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial. Bogotá, D.C: El Congreso, 2002. 91 p.

[26]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266. (31, diciembre, 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*. Diario Oficial. Bogotá, D.C: El Congreso, 2008. 75 p.

[27] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogotá, D.C: El Congreso, 2009. 58p.

abriendo así la posibilidad de nuevas entradas con este tema. Protección de Datos personales en un sentido amplio, el delito informático es todo aquello que implica la utilización de cualquier medio de tecnología informática para captar información de manera irregular. Delitos contra la intimidad, en el que se produce un tratamiento ilegal de los datos de carácter personal. Relativos al contenido, es decir a la difusión de contenidos ilegales en la Red; delitos económicos, relacionados con el acceso autorizado a sistemas informáticos para llevar a cabo fraude, sabotaje o falsificación, suplantación de entidades bancarias, delitos contra la propiedad intelectual vinculados con la protección de programas de ordenador, bases de datos y derechos de autor.

5. METODOLOGIA

5.1 TIPOS DE ESTUDIO

Durante el desarrollo de este proyecto se utilizó los métodos de investigación inductiva, deductiva y la metodología *Magerit*.

5.2 POBLACIÓN Y MUESTRA

La población objeto de estudio, estuvo conformada en su medio interno por el personal del área de contabilidad adscrito a la organización. Además, se llevó acabo una visita a las instalaciones para la identificación y determinación de cuales controles o aspectos de la política son aplicables al Área de Contabilidad de la E.S.E Hospital Regional noroccidental I.PS Abrego, ubicada en el segundo piso del edificio, donde se hizo de un levantamiento de *hardware, software* y recursos humanos disponibles asociados al área de seguridad y sistemas. Finalmente, se evaluó al personal de ingeniería usando como criterio de inclusión, a aquellos con más de 8 años de experiencia dedicados al área de seguridad de la información.

5.3 TÉCNICAS E INSTRUMENTOS PARA LA RECOLECCIÓN DE INFORMACIÓN

Las técnicas de recolección de información son la columna vertebral del proyecto ya que estás permiten conocer el estado actual de la empresa, para la realización de este proyecto se aplicaron las siguientes técnicas de recolección de información:

- Observación Directa
- Entrevistas
- Evaluación en base a experiencia

5.4 ANÁLISIS DE INFORMACIÓN

Durante el desarrollo de este proyecto se recopiló información relacionada con el uso de tecnologías de información dentro del Área de Contabilidad de la E.S.E Hospital Regional Noroccidental I.P.S Abrego, se realizó un estudio de la

información recibida, topología de red, herramientas y aplicativos utilizados, para luego establecer los aspectos que conformarán el Sistema de Gestión de Seguridad de la Información aplicables a la misma.

5.4.1 Observación directa. Esta se llevó acabo por medio de una visita a las instalaciones de la E.S.E, en la cual se inspeccionaron las oficinas del área de contabilidad ubicadas en el segundo piso del edificio, mediante esta inspección se procedió a realizar un levantamiento de activos físicos (*hardware*, *software*) y humano.

- Inventario de *software*
- Inventario de *hardware*
- Inventario de personal
- Inventario de inmueble
- Inventario de redes

Este levantamiento se describe en el análisis de riesgos.

5.4.2 Entrevista. Se procedió a realizar una entrevista al personal del área de contabilidad, esta entrevista consta de preguntas relacionadas con la Seguridad de la información, *Hardware*, Compra, Garantía, Redes, comunicaciones, Instalaciones, energía. Los ítems de la entrevista se pueden encontrar en el anexo C.

La información recaudada, se analizó cualitativamente, donde se determinaron los aspectos relacionados con el proyecto, estableciendo así un diagnóstico, para lo cual se espera la veracidad por parte de las personas entrevistadas. La herramienta que se utilizará para realizar el análisis de la información son hojas de recolección de datos y tablas de Excel para su tabulación, esta se puede encontrar en el anexo D.

6. ANÁLISIS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El compromiso de la dirección es la base fundamental para iniciar el proyecto, el apoyo y la decisión de implementar el Sistema de Gestión de Seguridad de la Información es vital dado que es la Dirección quien garantiza la implementación del Sistema de Gestión al interior de la organización. La norma ISO 27001, establece los compromisos que deben tener la Dirección para lograr el funcionamiento del SGSI:

6.1 PLANEAR

6.1.1 Alcance del sistema de gestión de seguridad de la información. Ejecutar la etapa de planeación de un SGSI para el área administrativa – Departamento de contabilidad de la Empresa Social del Estado hospital regional noroccidental IPS Abrego.

En la siguiente tabla se ilustra un ejemplo del SGSI.

Tabla 1. Ejemplo de SGSI

Código	**xxxxxxxxxx**
Versión	1.0
Fecha de la versión:	Abril 22 de 2018
Creado por	Juan Pablo Álvarez Pérez
Aprobado por	
Nivel de confidencialidad:	Confidencial

Fuente: Elaboración propia

6.1.1.1 Objetivo, alcance y usuarios. El objetivo de este documento es definir claramente los límites del Sistema de gestión de seguridad de la información (SGSI) en el área administrativa – Departamento de contabilidad de la E.S.E hospital regional noroccidental IPS Abrego.

Este documento se aplica a toda la documentación y actividades dentro del SGSI.

Los usuarios de este documento son los miembros de la dirección de la E.S.E hospital regional noroccidental IPS Abrego, los miembros del equipo del proyecto que implementa el SGSI y el jefe del área financiera.

6.1.1.2 Documentos de referencia. Se explican a continuación:

- Norma ISO/IEC 27001, punto 4,3:
- Lista de la documentación legal, regulatoria y contractual (Ley 1273 de 2009 [Ley de Delitos Informáticos en Colombia] y Decreto 2573 de 2014 [Estrategia de Gobierno en Línea]).

6.1.1.3 Definición del alcance del SGSI. El área contable de la E.S.E hospital regional noroccidental I.P.S Abrego necesita definir los límites del SGSI para decidir qué información quiere proteger. Esa información deberá ser protegida independientemente de si además es almacenada, procesada o transferida dentro o fuera del alcance del SGSI. El hecho de que determinada información esté disponible fuera del alcance no significa que no se le brindarán las medidas de seguridad pertinente; esto solamente implica que la responsabilidad de las medidas de seguridad será transferida a un tercero que administre esa información.

La planeación del SGSI se desarrolló bajo el estándar ISO/IEC 27001:2013 teniendo en cuenta las leyes y regulaciones que se rige la E.S.E hospital regional noroccidental I.P.S Abrego, como lo es la Ley 1273 de 2009 (Ley de Delitos Informáticos en Colombia) y el Decreto 2573 de 2014 (Estrategia de Gobierno en Línea).

Esta fase de planeación del SGSI comprende las siguientes áreas del Departamento de contabilidad.

Departamento de contabilidad: Comprende el personal administrativo (área financiera, Contabilidad, Presupuesto, Tesorería, Cartera, Activos fijos y almacén) sus activos informáticos y toda la infraestructura. Tomando esto en cuenta, los requisitos legales, normativos, contractuales y de otra índole, el alcance del SGSI se define de acuerdo a los siguientes aspectos:

- **Procesos y servicios:** Captura de los datos de la realidad económica y jurídica. Todos los hechos económicos, financieros, sociales y ambientales

realizados en cualquier dependencia de la I.P.S. Elaboración de los estados, informes y reportes contables

- **Unidades organizativas:** Financiera, contabilidad, presupuesto, tesorería, cartera, activos fijos y almacén.
- **Se explica a continuación:** Ubicación; Segundo piso de la I.P.S Abrego sede administrativa
- **Redes e infraestructura de TI:** La infraestructura de red se maneja mediante una red LAN de cableado estructurado la cual se encuentra conectada a toda la I.P.S, sistema de respaldo eléctrico (UPS y planta eléctrica).
- **Exclusiones del alcance:** Los siguientes elementos no están incluidos en el alcance: Servidor de historia clínica y demás terminales que no se encuentra en el departamento de contabilidad.

6.1.2 Análisis de riesgos. Para la actividad de análisis de riesgos se utilizó la metodología *Magerit* ya que esta se esfuerza por enfatizar y dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contramedidas efectivas para evitar así cualquier inconveniente.

6.1.3 Análisis de activos. Se llaman activos a todos los recursos que posee la E.S.E Hospital Regional Noroccidental en el departamento de contabilidad tanto de *hardware* como en *software*, recurso humano y demás. Basado en esto se clasificaron los activos de acuerdo con la Tabla 2.

Tabla 2. Inventario de activos

Tipos de activos	Descripción
Activo de información	Base de datos TNS
Software o aplicación	Sistema de información TNS
	Sistema operativo
	Antivirus
	Ofimática (Microsoft office)
Hardware	Servidor de la base de datos
	Equipos de escritorio
	Impresoras
	Switch 16 puertos TRENET
	Router
	Cámaras de seguridad
Red	Internet
	Red telefónica

Fuente: Elaboración propia

Tabla 2. (Continuación)

Tipos de activos	Descripción
Soporte de información	Disco duro externo
	Disco compacto Cd
Equipamiento auxiliar	UPS
	Generador eléctrico
	Aire acondicionado
	Sistemas de vigilancia
	Cableado
	Mobiliario
Instalación	Edificio
Servicios	Conectividad a internet
	Servicio de mantenimiento
Tipos de activos	Descripción
Personal	Jefe del área financiera
	Coordinador de Contabilidad
	Coordinador de Presupuesto
	Coordinador de Tesorería
	Auxiliar de Cartera
	Auxiliar de Activos fijos
	Jefe de Almacén

Fuente: Elaboración propia

6.1.4 Valoración de los activos. La valoración de activos se encuentra en la Tabla 3 y su respectivo análisis en la Tabla 4.

Tabla 3. Valoración de activos

VALORACION DE ACTIVOS	
CUALITATIVA	**CUANTITATIVA**
[MA] Muy Alto	>10.000.000
[A] Alto	10.000.000 <valor>5.000.000
[M] Medio	5.000.000 <valor>2.000.000
[B] Bajo	2.000.000 <valor>1.000.000
[MB] MUY BAJO	1.000.000 <valor>100.000

Fuente: Elaboración propia

Tabla 4. Análisis de valoración de los activos

Tipos de activos	Descripción	Valor Del Activo	Valor
Activo de información	Base de datos TNS	A	5.000.000
Software o aplicación	Sistema de información TNS	M	3.000.000
	Sistema operativo	M	4.000.000
	Antivirus	MB	240.000
	Ofimática (Microsoft office)	M	4.600.000
Hardware	Servidor de la base de datos	M	2.300.000
	Equipos de escritorio	A	7.000.000
	Impresoras	B	1.400.000
	Switch 16 puertos TRENET	MB	350.000
	Router	MB	250.000
	Cámaras de seguridad	A	6.000.000
Red	Internet	B	1.800.000
	Red telefónica	B	1.700.000
Soporte de información	Disco duro externo	MB	250.000
	Disco compacto CD	MB	100.000
Equipamiento auxiliar	UPS	B	1.800.000
	Generador eléctrico	MA	25.000.000
	Aires acondicionados	B	1.600.000
	Sistemas de vigilancia	A	7.200.00
	Cableado	B	1.800.000

Fuente: Elaboración propia

Tabla 4. (Continuación)

Tipos de activos	Descripción	Valor Del Activo	Valor
	Mobiliario	A	7.900.00
Instalación	Edificio	MA	60.000.00
Servicios	Conectividad a internet	B	1.800.00
	Servicio de mantenimiento	A	6.000.000
Personal	Jefe del área financiera	M	2.100.000
	Coordinador de Contabilidad	B	1.500.000
	Coordinador de Presupuesto	B	1.500.000
	Coordinador de Tesorería	M	2.100.000
	Auxiliar de Cartera	B	1.500.000
	Auxiliar de Activos fijos	B	1.500.00
	Jefe Almacén	B	1.500.000

Fuente: Elaboración propia

6.1.5 Dimensiones de seguridad. La valoración se realizará en una escala cualitativa y estos valores se refieren a la importancia del activo en caso de daño o falla

Tabla 5. Escala de valoración de los activos

Valor	Criterio
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Fuente: Elaboración propia

6.1.6 Dimensiones. Se explica a continuación:

[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos
En la Tabla 6 se denota la valoración de dimensiones de seguridad de los activos.

Tabla 6. Valoración de dimensiones de seguridad de los activos

Activos	**Dimensiones**				
Activos	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Activo de información					
Base de datos TNS	[9]	[10]	[10]	[10]	[9]
***Software* o Aplicación**					
Sistema de información TNS	[9]	[10]	[10]	[9]	[9]
Sistemas operativos					[7]
Antivirus					[7]
Ofimática (Microsoft office)					[7]
Hardware					
Servidor de la base de datos	[9]	[9]	[9]	[9]	[9]
Equipos de escritorio					[8]
Impresoras					[6]
Switch 16 puertos TRENET				[7]	[8]
Router TPLINK				[7]	[8]
Cámaras de seguridad		[8]	[8]		[8]
Red					
Internet			[7]	[8]	[7]
Red Telefónica				[8]	[7]
Soporte de Información					
Disco duro externo		[7]	[9]	[4]	[5]
Disco compacto		[6]	[3]		
Equipamiento Auxiliar					
UPS				[7]	
Generador eléctrico				[7]	
Aire acondicionado				[5]	
Sistemas de Vigilancia				[7]	
Cableado				[7]	

Fuente: Elaboración propia

Tabla 6. (Continuación)

Activos	Dimensiones				
Activos	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Mobiliario				[7]	
Instalaciones					
Edificio	[8]	[8]	[8]	[10]	[8]
Servicios					
Internet		[8]			
Servicio de mantenimiento		[8]	[8]	[8]	
Personal					
Jefe Financiero		[8]			
Coordinador de Contabilidad		[8]			
Coordinador de Presupuesto		[8]			
Coordinador de Tesorería		[8]			
Auxiliar de Cartera		[8]			
Auxiliar de Activos fijos		[8]			
Jefe de Almacén		[8]			

Fuente: Elaboración propia

6.1.7 Identificación de amenazas. Se explica a continuación:

[N] Desastre Natural
[I] De origen industrial
[E] Errores y fallos no intencionados
[A] Ataque intencionado

En la Tabla 7 se muestra la identificación de las amenazas.

Tabla 7. Identificación de amenazas

Activos	Amenazas
Base de datos TNS	[E.1] Errores de los usuarios [E.2] Vulnerabilidades de los programas (*software*) [E.3] Errores de mantenimiento / actualizaciones de programas (*software*) [A.2] Difusión de *software* dañino

Fuente: Elaboración propia

Tabla 7. (Continuación)

Activos	Amenazas
Ofimática (Microsoft office)	[E.1] Errores de los usuarios [E.2] Vulnerabilidades de los programas (*software*) [E.3] Errores de mantenimiento / actualizaciones de programas (*software*) [A.2] Difusión de *software* dañino
Antivirus	[A.2] Difusión de *software* dañino [E.2] Vulnerabilidades de los programas (*software*) [E.3] Errores de mantenimiento / actualizaciones de programas (*software*)
Sistema Operativo	[I.1] Avería de origen físico o lógico [E.1] Errores de los usuarios [E.4] Difusión de *software* dañino [E.2] Vulnerabilidades de los programas (*software*) [E.3] Errores de mantenimiento / actualizaciones de programas (*software*) [A.1] Uso no previsto
Sistema de Información TNS	[E.1] Errores de los usuarios [E.4] Difusión de *software* dañino [E.2] Vulnerabilidades del programa (*software*) [E.3] Errores de mantenimiento / actualizaciones de programas (*software*) [A.1] Uso no previsto [A.2] Denegación de servicios [A.3] Acceso no autorizado [A.4] Abuso de privilegios de acceso
Servidor de base de datos	[N.1] Fuego [N.2] Daños por agua [I.2] Contaminación medioambiental [I.1] Avería de origen físico o lógico [I.3] Condiciones inadecuadas de temperaturas o humedad [E.5] Errores del administrador del sistema, de la seguridad [E.6] Errores de mantenimiento, actualización de equipos *hardware* [A.3] Acceso no autorizado [A.4] Manipulación del *hardware*

Fuente: Elaboración propia

Tabla 7. (Continuación)

Activos	Amenazas
Impresoras	[I.1] Avería de origen físico o lógico
	[I.3] Condiciones inadecuadas de temperaturas o humedad
	[E.6] Errores de mantenimiento, actualización de equipos *hardware*
	[A.3] Acceso no autorizado
Equipos de escritorio	[N.2] Daños por agua
	[I.1] Avería de origen físico o lógico
	[I.3] Condiciones inadecuadas de temperaturas o humedad
	[E.6] Errores de mantenimiento, actualización de equipos *hardware*
	[E.7] Caída del sistema por agotamiento de recursos
	[A.4] Abuso de privilegios de acceso
	[A.1] Uso no previsto
Router	N.2] Daños por agua
	[I.1] Avería de origen físico o lógico
	[I.3] Condiciones inadecuadas de temperaturas o humedad
	[E.7] Caída del sistema por agotamiento de recursos
Switch 16 puertos TRENET	[N.2] Daños por agua
	[I.1] Avería de origen físico o lógico
	[I.3] Condiciones inadecuadas de temperaturas o humedad
	[E.7] Caída del sistema por agotamiento de recursos
Cámaras de seguridad	[A.3] Acceso no autorizado
	[N.2] Daños por agua
	[I.2] Contaminación medioambiental
	[I.1] Avería de origen físico o lógico
	[A.1] Uso no previsto
Internet	[A.3] Acceso no autorizado
Telefonía	[A.3] Acceso no autorizado
Disco duro Externo	[A.3] Acceso no autorizado
	[E.10] Alteración de la información
	[A.10] Modificación de la información
	[A.11] Robo de la información

Fuente: Elaboración propia

Tabla 7. (Continuación)

Activos	Amenazas
Disco compacto	[A.3] Acceso no autorizado
	[E.10] Alteración de la información
	[A.10] Modificación de la información
	[A.11] Robo de la información
Generador eléctrico	[I.2] Contaminación medioambiental
	[I.3] Condiciones inadecuadas de temperaturas o humedad
UPS	[I.3] Condiciones inadecuadas de temperaturas o humedad
Cableado	[I.2] Contaminación medioambiental
	[I.3] Condiciones inadecuadas de temperaturas o humedad
Sistema de Vigilancia	[I.2] Contaminación medioambiental
	[I.3] Condiciones inadecuadas de temperaturas o humedad
Aire acondicionado	[I.2] Contaminación medioambiental
	[I.3] Condiciones inadecuadas de temperaturas o humedad
Mobiliario	[N.1] Fuego
	[N.2] Daños por agua
Edificio	[N.1] Fuego
	[N.2] Daños por agua
	[N.3] Tormentas
	[N.4] Terremotos
	[A.7] Ocupación enemiga
Servicio de mantenimiento	[E.11] Enfermedad
	[E.12] Huelga
	[A.8] Extorsión
	[A.9] Ingeniería Social
Jefe del área financiera	[E.11] Enfermedad
	[E.12] Huelga
	[A.8] Extorsión
	[A.9] Ingeniería Social
Coordinador de Contabilidad	[E.11] Enfermedad
	[E.12] Huelga
	[A.8] Extorsión
	[A.9] Ingeniería Social

Fuente: Elaboración propia

Tabla 7. (Continuación)

Activos	Amenazas
Coordinador de Presupuesto	[E.11] Enfermedad [E.12] Huelga [A.8] Extorsión [A.9] Ingeniería Social
Coordinador de Tesorería	[E.11] Enfermedad [E.12] Huelga [A.8] Extorsión [A.9] Ingeniería Social
Auxiliar de Cartera	[E.11] Enfermedad [E.12] Huelga [A.8] Extorsión [A.9] Ingeniería Social
Auxiliar de Activos fijos	E.11] Enfermedad [E.12] Huelga [A.8] Extorsión [A.9] Ingeniería Social
Jefe de Almacén	E.11] Enfermedad [E.12] Huelga [A.8] Extorsión [A.9] Ingeniería Social

Fuente: Elaboración propia

La probabilidad de ocurrencia se valorará de acuerdo a la siguiente escala puesta en la Tabla 8 y en la Tabla 9 y 10, se escala y resume la amenaza.

Tabla 8. Escala de valoración cuantitativo

Impacto	Valor cuantitativo
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: Elaboración propia

Tabla 9. Escala de rango de frecuencia de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semanas	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: Elaboración propia

Tabla 10. Resumen valoración de la amenaza

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
Base de datos TNS	[E.1] Errores de los usuarios	5	75%				
	[E.2] Vulnerabilidades de los programas (*software*)	5	75%		75 %		
	[E.3] Errores de mantenimiento / actualizaciones de programas (*software*)	10	75%		75 %		
	[A.2] Difusión de *software* dañino	5	75%	75 %	75 %		
Ofimática (Microsoft office)	[E.1] Errores de los usuarios	5		50 %	50 %	50 %	
	[E.2] Vulnerabilidades de los programas (*software*)	5		50 %	50 %	50 %	

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
	[E.3] Errores de mantenimiento / actualizaciones de programas (*software*)	5			20 %	50 %	
	[A.2] Difusión de *software* dañino	10		20 %	20 %	20 %	
Antivirus	[A.2] Difusión de *software* dañino	10		20 %	20 %	20 %	
	[E.2] Vulnerabilidades de los programas (*software*)	10		50 %	50 %	50 %	
	[E.3] Errores de mantenimiento / actualizaciones de programas (*software*)	10			50 %	50 %	
Sistema Operativo	[I.1] Avería de origen físico o lógico	10				50 %	
	[E.1] Errores de los usuarios	5		50 %	50 %	50 %	
	[E.4] Difusión de *software* dañino	5		20 %	20 %	20 %	

Fuente: Elaboración propia

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
Sistema de Información TNS	[E.2] Vulnerabilidades de los programas (*software*)	10		50 %	50 %	20 %	
	[E.3] Errores de mantenimiento / actualizaciones de programas (*software*)	5			20 %	50 %	
	[A.1] Uso no previsto	50		20 %	20 %	20 %	
	[E.1] Errores de los usuarios	10		20 %	20 %	20 %	
	[E.4] Difusión de *software* dañino	10		20 %	20 %	20 %	
	[E.2] Vulnerabilidades del programa (*software*)	10		20 %	20 %	20 %	
	[E.3] Errores de mantenimiento / actualizaciones de programas (*software*)	10			50 %	50 %	
	[A.1] Uso no previsto	5		20 %	20 %	20 %	
	[A.2] Denegación de servicios	5	75%	75 %	75 %	75 %	

Fuente: Elaboración propia

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
Servidor de base de datos	[A.3] Acceso no autorizado	5	75%	75 %	75 %	75 %	
	[A.4] Abuso de privilegios de acceso	5	50%	50 %	50 %	50 %	
	[N.1] Fuego	5				75 %	
	[N.2] Daños por agua	5				75 %	
	[I.2] Contaminación medioambiental	5				75 %	
	[I.1] Avería de origen físico o lógico	10				75 %	
	[I.3] Condiciones inadecuadas de temperaturas o humedad	5				50 %75%	
	[E.5] Errores del administrador del sistema, de la seguridad	5		50 %	50 %	50 %	
	[E.6] Errores de mantenimiento, actualización de equipos *hardware*	10				50 %	
	[A.3] Acceso no autorizado	10		50 %	50 %		

Fuente: Elaboración propia

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
	[A.4] Manipulación del hardware	5				50 %	
Impresoras	[I.1] Avería de origen físico o lógico	5				50 %	
	[I.3] Condiciones inadecuadas de temperaturas o humedad	5				50 %	
	[E.6] Errores de mantenimiento, actualización de equipos *hardware*	5				50 %	
	[A.3] Acceso no autorizado	5		50 %	50 %		
Equipos de escritorio	[N.2] Daños por agua	5				50 %	
	[I.1] Avería de origen físico o lógico	10				50 %	
	[I.3] Condiciones inadecuadas de temperaturas o humedad	5				50 %	
	[E.6] Errores de mantenimiento, actualización de equipos *hardware*	5				50 %	

Fuente: Elaboración propia

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
	[E.7] Caída del sistema por agotamiento de recursos	10				50 %	
	[A.4] Abuso de privilegios de acceso	10		50 %	50 %	50 %	
	[A.1] Uso no previsto	70		50 %	50 %	50 %	
Switch 16 puertos TRENET	[N.1] Fuego	10				50 %	
	[N.2] Daños por agua	10				50 %	
	[I.2] Contaminación medioambiental	5				50 %	
	[I.1] Avería de origen físico o lógico	5				50 %	
	[I.3] Condiciones inadecuadas de temperaturas o humedad	5				50 %	
	[A.3] Acceso no autorizado	5		50 %	50 %	50 %	
Router	[N.1] Fuego	5				50 %	
	[N.2] Daños por agua	10				50 %	
	[I.2] Contaminación medioambiental	5				50 %	
	[I.1] Avería de origen físico o lógico	5				50 %	

Fuente: Elaboración propia

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
	[I.3] Condiciones inadecuadas de temperaturas o humedad	5				50 %	
	[A.3] Acceso no autorizado	5		50 %	50 %	50 %	
Cámaras de seguridad	[A.3] Acceso no autorizado	5		50 %	50 %	50 %	
	[N.2] Daños por agua	50		50 %	50 %	50 %	
	[I.2] Contaminación medioambiental	5		50 %	50 %	50 %	
	[I.1] Avería de origen físico o lógico	50				50 %	
	[A.1] Uso no previsto	5				50 %	
Telefonía	[A.3] Acceso no autorizado	70		50 %	50 %	50 %	
Internet	[I.4] Fallo de servicios de comunicaciones	50				75 %	
	[E.10] Alteración de la información	5			20 %		
Disco Duro Externo	[E.10] Alteración de la información	5			20 %		
	[E.13] Fuga de información	5		20 %			
	[A.10] Modificación de la información	10			20 %		

Fuente: Elaboración propia

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
	[A.12] Revelación de la información	10				75 %	
Disco compacto	[E.10] Alteración de la información	5			20 %		
	[E.13] Fuga de información	5		20 %			
	[A.10] Modificación de la información	5			20 %		
	[A.12] Revelación de la información	10				75 %	
	[A.11] Robo de la información	10		20 %	20 %		
Generador eléctrico	[I.2] Contaminación medioambiental	10				50 %	
	[I.3] Condiciones inadecuadas de temperaturas o humedad	10				75 %	
UPS	[I.2] Contaminación medioambiental	5				50 %	
	[I.3] Condiciones inadecuadas de temperaturas o humedad	5				75 %	

Fuente: Elaboración propia

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
Cableado	[I.2] Contaminación medioambiental	5				75 %	
	[I.3] Condiciones inadecuadas de temperaturas o humedad	5				20 %	
Mobiliario	[I.2] Contaminación medioambiental	5				50 %	
Sistema de Vigilancia	[I.2] Contaminación medioambiental	5				50 %	
	[I.3] Condiciones inadecuadas de temperaturas o humedad	5				75 %	
Aire acondicionado	[I.2] Contaminación medioambiental	5				75 %	
	[I.3] Condiciones inadecuadas de temperaturas o humedad	5				50 %	

Fuente: Elaboración propia

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
Edificio	[N.1] Fuego	5				75 %	
	[N.2] Daños por agua	10				75 %	
	[N.3] Tormentas	10				50 %	
	[N.4] Terremotos	5				50 %	
	[A.7] Ocupación enemiga	5		75 %		50 %75%	
Servicio de mantenimiento	[E.11] Enfermedad	10		50 %	50 %	50 %	
	[E.12] Huelga	5				20 %	
	[A.8] Extorsión	5		50 %	50 %	50 %	
	[A.9] Ingeniería Social	5		20 %	75 %	75 %	
Jefe del área financiera	[E.11] Enfermedad	10		50 %	50 %	50 %	
	[E.12] Huelga	5				20 %	
	[A.8] Extorsión	5		50 %	50 %	50 %	
	[A.9] Ingeniería Social	5		20 %	75 %	75 %	
Coordinador de Contabilidad	[E.11] Enfermedad	5		50 %	50 %	50 %	
	[E.12] Huelga	5				20 %	
	[A.8] Extorsión	5		50 %	50 %	50 %	
	[A.9] Ingeniería Social	5		20 %	75 %	75 %	

Fuente: Elaboración propia

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
Coordinador de Presupuesto	[E.11] Enfermedad	5		50 %	50 %	50 %	
	[E.12] Huelga	5				20 %	
	[A.8] Extorsión	5		50 %	50 %	50 %	
	[A.9] Ingeniería Social	5		50 %	75 %	75 %	
Coordinador de Tesorería	[E.11] Enfermedad	5		50 %	50 %	50 %	
	[E.12] Huelga	5		75 %	50 %	75 %	
	[A.8] Extorsión	5		50 %	50 %	50 %	
	[A.9] Ingeniería Social	5		75 %	75 %	75 %	
	[A.4] Abuso de privilegios de acceso	5		50 %	50 %	50 %	
Auxiliar de Cartera	[E.11] Enfermedad	5		50 %	50 %	50 %	
	[E.12] Huelga	5		75 %	50 %	75 %	
	[A.8] Extorsión	5		50 %	50 %	50 %	
	[A.9] Ingeniería Social	5		50 %	50 %	50 %	

Fuente: Elaboración propia

Tabla 10. (Continuación)

Activos	Amenazas	Frecuencia de la amenaza	[A]	[C]	[I]	[D]	[T]
Auxiliar de Activos fijos	[E.11] Enfermedad	5		50 %	50 %	50 %	
	[E.12] Huelga	5		75 %	50 %	75 %	
	[A.8] Extorsión	5		50 %	50 %	50 %	
	[A.9] Ingeniería Social	5		50 %	50 %	50 %	
Jefe de Almacén	[E.11] Enfermedad	10		50 %	50 %	50 %	
	[E.12] Huelga	5		75 %	50 %	75 %	
	[A.8] Extorsión	5		50 %	50 %	50 %	
	[A.9] Ingeniería Social	5		50 %	50 %	50 %	

Fuente: Elaboración propia

6.1.8 Políticas de seguridad. Se explica a continuación:

6.1.8.1 Objetivo, alcance y usuarios. Establecer las políticas de seguridad de la información del área administrativa – Departamento de contabilidad de la E.S.E hospital regional noroccidental IPS Abrego, con el fin de proteger, preservar y administrar la información de acuerdo con las buenas prácticas y ejecutar controles de actualización para las políticas de información definidas.

Las políticas de seguridad definidas serán de aplicación obligatoria para todo el personal del E.S.E hospital regional noroccidental IPS Abrego, cualquier sea su contratación, dependencia y nivel de responsabilidades.

La Gerencia aprueba la política y es responsable de la autorización de sus modificaciones.

6.1.8.2 Documentos de referencia. Norma ISO/IEC 27001, capítulos 5.2 y 5.3

- Documento sobre el alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales

6.1.8.3 Políticas generales de la seguridad de la información. Se explica a continuación:

Acceso a los sistemas de información:

- Se debe diligenciar el formato de creación de usuario, estar autorizado por el jefe de área y gestionado por el personal de TI.
- Se deben asignar los roles y perfiles que requiera el usuario para el desempeño de sus funciones.
- El acceso a los sistemas de información del departamento de contabilidad debe tener una autenticación con usuario y contraseña incluyendo conexiones externas como VPN.
- La contraseña debe cumplir con las siguientes condiciones: Longitud de contraseña mínimo de 8 caracteres, Utilizar caracteres especiales Utilizar mayúsculas, minúsculas, Alfanumérica y Periodicidad de cambio cada 90 días.
- El usuario es responsable de realizar el cambio periódico de la contraseña.
- Se realizará monitoreo de las acciones de los usuarios sobre los sistemas de información por medio de los logs. Por lo tanto, el usuario es responsable por el tratamiento que se de en los sistemas de información.
- El uso de la contraseña es personal e intransferible y no puede ser compartida con ningún usuario interno incluyendo el personal de TI, ni con personal externo.
- El usuario es responsable de la seguridad del equipo asignado y de los sistemas de información a los cuales se le ha otorgado el acceso, el bloqueo del equipo debe ser inmediato una vez se retire de su puesto de trabajo.

Acceso no autorizado a la información:

- Ningún usuario puede realizar instalación de aplicaciones que no estén autorizadas por la compañía.
- Se prohíbe el uso de cualquier dispositivo de almacenamiento externo (USB, Disco duro, CD, entre otros).

- Ningún usuario puede intentar acceder de manera forzosa a las unidades de red o carpetas compartidas a las cuales no se ha autorizado el acceso.
- Se prohíbe utilizar herramientas que permita el acceso remoto de terceros como Chrome remote desktop, ShoMyPc, teamviewer, entre otros.
- Cualquier evento sospechoso que sea identificado por el usuario, deberá ser informado al área de TI.

Activos de la información:

En este punto, en consonancia con el SGSI la empresa debe tener claro cuales son los activos informáticos, e identificar la ubicación de estos con sus respectivos responsables. Todo ello, encaminado a realizar un inventario de los recursos informáticos con los cuales cuenta la organización.

Para la correcta elaboración del inventario Informático, se debe en primer lugar documentar y mantener actualizada la *data* acerca de los activos asociados a los medios de procesamiento. Para ello, la periodicidad de los inventarios debe ser con una frecuencia menor a un año.

La labor de mantener actualizado el inventario de activos informáticos, recae primordialmente en el responsable del departamento de contabilidad en la compañía. Para ello, la confidencialidad, Integridad y Disponibilidad son los criterios de clasificación bajo los cuales se fundamenta la seguridad de la información en la empresa.

Definición de los criterios de calificación de la información:

- **Uso Público:** Dentro de este criterio, se localiza toda la información que por sus características intrínsecas pueden estar a disposición de toda persona natural o jurídica en el ámbito legal colombiano. Pueden ser, noticias, informes de prensa, información de rendición de cuentas, información sobre trámites, normatividad, entre otras muchas.
- **Interno:** En este criterio se localiza aquella información que solo puede estar a disposición de personal interno de la compañía o terceros vinculados con la organización directamente.
- **Uso Confidencial:** Dentro de este criterio de información se encuentra aquella que de alguna forma afecta el sano desenvolvimiento de la misión de la empresa y cuya divulgación requiere tener la autorización de los responsables de esta. Dentro del rango de manejo de información en este nivel, se incluye los terceros; para los cuales debe existir un acuerdo de confidencialidad.

Dado lo anterior, se debe tener la información debidamente resguardada con claves o encriptada, de modo pues; que permita poder transportar la misma en los medios físicos de almacenamiento de una forma segura. Además, es indispensable incentivar el manejo responsable de los datos informativos, respetando criterios como: Privacidad, habeas data y copyright de la empresa en su manejo informativo.

Seguridad en el recurso humano:

En este nivel, es importante manejar criterios de selección del personal acudiendo a juicios adecuados por medio de la verificación de antecedentes; tanto a nivel de empleados, como de contratistas y terceros relacionados con la empresa. Estos controles de selección deben ser apegados a las disposiciones legales vigentes en la normativa del estado.

Además de lo dicho anteriormente, la empresa debe ofrecer al personal capacitaciones que divulguen la seguridad en la información. Además, se deben ofrecer los procedimientos del sistema de gestión de seguridad informática a fin de que los empleados conozcan las normativas en materia de seguridad. Esto, tomando en cuenta lo siguiente: El desconocimiento de la norma no exime de culpa a quienes cometan violaciones a las políticas de seguridad de la información en la compañía, quedando abierta la posibilidad de procesos disciplinarios motivados a incumplimientos normativos por parte de la empresa, a personal que se encuentre en franca violación de la seguridad informática.

Finalmente, la compañía tiene la obligación de abrir un proceso de desvinculación al personal con acceso privilegiado a la información. Esto, ocasiona la eliminación de acceso ilimitado al sistema informativo de personal que no garantice el proceso de seguridad.

Control del acceso:

Continuando con este marco de ideas concerniente a los privilegios en los sistemas de información, se debe contar con un responsable que autorice el uso de la infraestructura de red, equipos de cómputos e información sensible de la organización, privilegiando así su uso solo a personal autorizado.

Dentro del proceso de tecnologías de la información, de acuerdo al perfil de cargo, se debe definir el acceso a red, sistemas operativos, servicios y sistemas de información.

También, dentro de este departamento de control de acceso se debe mantener un registro cronológico que permita tener un control acerca del personal propio, externo o de terceros al que se le haya permitido acceso a cualquiera de los diferentes sistemas de información de la empresa. Así mismo, la plataforma de acceso a los distintos sistemas de información deberá incluir, nombre de usuario y contraseña personal para poder acceder.

Añadido a esto, cuando en la eventualidad de retiro o cambio de un empleado, dentro del marco de seguridad informativa se debe proceder a la eliminación y cambios de privilegio a los que el empleado tenía acceso, bajo la supervisión del proceso de talento humano.

Sumado a esto, el proceso de tecnologías de la información deberá revisar los privilegios de acceso con una periodicidad no mayor de un año, llevando además un registro de las revisiones con las eventualidades y observaciones que se hayan notado. Sumado a esto, los sistemas de información deben bloquear a cualquier usuario que haya intentado acceder 5 veces consecutivas de forma fallida.

Dentro de los criterios de seguridad que deben tener los usuarios para sus cuentas, deben existir los siguientes: Absoluto secreto de acceso, las contraseñas deben ser fáciles de recordar; que no este relacionada con información del usuario (fecha de nacimiento, teléfono, nombre). Además, es conveniente que se reporte cualquier eventualidad relacionado con sus cuentas de usuario, robo o sospecha de perdida de seguridad.

Adicionalmente, se debe activar protectores de pantallas en los equipos una vez que el funcionario abandone la estación de trabajo o no haya actividad por un tiempo determinado. Esto con el fin de evitar que terceros accedan a información en esta situación.[28]

[28] SUAREZ, Sandra. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & Cía. Ltda, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Trabajo de grado Especialista en Seguridad Informática. Bogota. D.C.: Universidad Nacional Abierta y a Distancia, Escuela de Tecnología e Ingeniería. Especialización en seguridad informática, 2015. 135 p.

Acceso físico:

- Todo equipo de cómputo (portátil, Tablet, video beam, entre otros), deben ser registrados al ingreso.
- Todo el personal debe portar el carné de identificación al igual que el personal externo (contratistas, visitantes).
- Todo el personal visitante debe estar en compañía de la persona de contacto de la IPS.
- Todo el personal externo (contratistas, visitantes) no debe ingresar a zonas restringidas sin estar en compañía de personal autorizado.

Acceso a Internet:

Se prohíbe el acceso a páginas web ilegales relacionadas con: Drogas, abuso infantil, pornografía, violencia, entre otros. Se prohíbe el acceso a páginas de entretenimiento relacionadas con: Redes sociales, mensajería instantánea, correo electrónico personal, juegos en línea, películas, videos, música en línea. Mediante un protocolo de excepción que permita acceder a correos previamente notificados, se puede acceder a correos laborales o institucionales.

Se prohíbe la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, *software* de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual

Instalación de *Software* y *Hardware*:

Para la instalación del *software* y *hardware*, estos componentes serán únicamente instalados por el personal técnico capacitado de la institución. A cada equipo se le realizará un inventario de *hardware* y la información será mantenida en la hoja de vida del equipo. Se realizará un chequeo de este componente cada vez que se inicie el equipo y se conecte a la red; si se detectan cambios no autorizados, quedará deshabilitado automáticamente.

Almacenamiento y custodia de la información:

- El usuario es responsable del almacenamiento de la información en las carpetas que serán destinadas para la realización de los backups.
- En caso de extraer información del equipo, el dispositivo debe estar cifrado de acuerdo con las políticas de la E.S.E.
- En ninguna circunstancia se debe enviar información de la compañía por correos externos al institucional.
- El usuario no podrá compartir ni suministrar información a terceros, sin la debida autorización de la E.S.E.

Gestión de operaciones y comunicaciones:

Control de procedimientos operativos: Solo previa autorización del responsable del área informática, el sistema operativo podrá ser actualizado o modificado, para ello el responsable dejará constancia de cada acción realizada.

Control de cambios operativos: Asimismo, los cambios operacionales de protocolo deben ser evaluados y posteriormente aprobados, bajo los siguientes criterios: Planificación, impacto, prueba y tipificación de responsabilidades en caso de cambios nocivos o fallidos.

Control de manejo de incidentes: El responsable de seguridad juntamente con el del área informática, son los encargados de establecer los protocolos a seguir en casos de incidentes y eventualidades relacionadas con esas áreas. Por tal razón, todo error operativo de índole humano, sistemático, natural e informático debe ser comunicado a la dirección siguiendo la ruta de control o plan de acción diseñado para hacer frente a las irregularidades e implementar control de la situación y recuperación del sistema.

Planificación y Aprobación de sistemas:

Planificación de la capacidad: En el área de seguridad informática, el responsable deberá evaluar a modo de prevención, futuras fallas, para evitarlas antes de que acontezcan.

Aprobación del sistema: La tarea de actualización, de los equipos y *software* destinados al área de seguridad informática recae sobre el responsable de dichas dependencias de la empresa.

Protección contra *software* malicioso:

Los encargados del área de seguridad y de informática, son los encargados de definir las normas y criterios bajo los cuales se regirá ambas áreas en materia de seguridad. Dentro de esos criterios, estaría la prohibición de instalación y descargas de material dudoso en la plataforma tecnológica de la empresa. Otra tarea en este sentido es la de verificar, monitorear, escanear el *software* de los servidores antes de realizar instalaciones de programas. Adicionalmente, se debe auditar toda la información entrante para constatar que se encuentre libre de cualquier amenaza potencial. Para ello, se debe concienciar en ese sentido a todo el personal.

Seguridad de la información:

Los esquemas y protocolos a seguir para la protección de la información, será función de los responsables de información y seguridad, entre los protocolos a seguir se sugiere los siguientes: Esquema de rotulado único, copia de seguridad con prueba de restauración, protocolo de rotulado de copias de documentos originales. Adicionalmente, el almacenamiento de las copias de seguridad deberá estar resguardado con todas las consideraciones pertinentes para garantizar su resguardo apropiadamente.

Registro de actividades del personal operativo: En este sentido, la persona responsable de la seguridad informática debe llevar un registro detallado con todas las eventualidades que se puedan presentar tales como: Intentos de acceso, errores, inicio y cierre, entre otros.

- **Registro de fallas:** Para la correcta documentación, el mecanismo de los desarrollos de seguridad deberá llevar un registro detallado de las fallas presentadas, medidas tomadas para la corrección y como fueron resueltas.
- **Administración de la Red:** En este apartado, el jefe del área de seguridad es el encargado de tomar todas las medidas que considere necesarias para garantizar la protección de la red de datos de la empresa.

Además, le corresponde crear los mecanismos de protocolo a implementar para abrir procedimientos administrativos para todas las actividades realizadas en la red. Para ello, puede delegar un responsable que establezca los mecanismos necesarios para garantizar la seguridad, confidencialidad, disponibilidad e integridad de la información.

Finalmente, es tarea del responsable de la red, establecer los métodos mediante el cual se supervisa que los controles de seguridad se están efectuando cabalmente. Para ello, se debe vigilar el fiel cumplimiento de los mecanismos diseñados para ese fin.

Administración de medios de almacenamiento: La tarea, de verificar y asegurar que se cumplan con los correctos procedimientos para el almacenamiento, respaldo, y eliminación de los discos de almacenamiento, buscando evitar el desvió de información sensible, corresponde a los responsables del área de informática y el área de seguridad.

Además, el responsable de la seguridad y el responsable del área de informática, son responsables directos de la eliminación de información. Por tal motivo, deben diseñar planes en conjunto que facilite el control de las áreas bajo su supervisión, integrando mecanismos que conlleven a ese fin.

Procedimientos de manejo de información: El protocolo de protección de la información, que deberán seguir los empleados involucra: Proteger documentos, redes y dispositivos, restringir acceso al personal que no cuente con la facultad para acceder, el almacenamiento de dispositivos en sitios seguros. Así mismo, la documentación del sistema de conservarse almacenada en un lugar seguro dispuesto por el jefe del departamento, lugar; que deberá tener el acceso restringido.

Intercambios de Información y de *Software*: En este sentido, se recomienda el empleo de medios como: mensajería institucional. Debido a esto, el uso de este medio debe ser adecuado, con precauciones tales como: evitar abrir mensajería de remitente desconocido, la información que arribe al sistema debe ser escaneada, y tener un conocimiento de los peligros y riesgos de seguridad a los que se enfrenta para poder tener conciencia clara de los mecanismos de precaución que se debe tomar[29].

[29] Ibíd., p. 23.

Adquisición, desarrollo y mantenimiento de los sistemas de información:

Las políticas planteadas aplican a todos los sistemas de información ya sean desarrollos propios o de terceros, estas políticas se basan en los controles publicados en el Portal ISO “Adquisición, desarrollo y mantenimiento de los sistemas de información”

En cuanto a seguridad de las comunicaciones en servicios accesibles por redes públicas, la política de seguridad es proteger la información que pasa atreves de las aplicaciones que utilizan redes públicas para transferirla. Pará el cumplimiento de esta política, es necesario que al momento de transferir la información esta sea encriptada para evitar el ingreso o cambio no autorizado, el encargado del área de seguridad de la información debe analizar a profundidad, los servicios que acceden a redes públicas y evaluar los riesgos y vulnerabilidades, establecer los procedimientos necesarios para proteger la información que interviene en el correcto funcionamiento de los servicios.

Protección de las transacciones por redes telemáticas, la política de seguridad es proteger la información de la transmisión o enrutamiento incorrecto y evitar la alteración duplicación o divulgación no autorizada, Para el cumplimiento de esta política es necesario que se realice revisiones periódicas del funcionamiento y almacenamiento de la información que procesan los sistemas, para verificar si se está almacenado en el lugar correcto y evitar la alteración, divulgación y/o duplicación no autorizada.

Partiendo de allí, se debe asegurar que tanto los sistemas de información como los aplicativos del mismo cumplan con todos los requerimientos de ley a los que hubiere lugar.

En ese orden de ideas, cuando se adquiere nuevos equipos y sistemas, tanto físicos como virtuales, que conecten con la plataforma tecnológica de la empresa, deberá ser diligenciado completamente por el área de tecnología e informática, cuidando que la configuración sea la correcta para garantizar el funcionamiento óptimo del mismo.

Cuando se trate de programas de desarrollo autóctono, lo primordial es que dicho sistema este debidamente registrado ante las instancias correspondientes, que la documentación sea la adecuada y cumpla con todos los requisitos de ley ante todos los organismos que guarden relación con este principio. Además, debe tener sus respectivas copias de seguridad como respaldo.

Cuando la empresa adquiera una licencia de algún programa determinado, se debe realizar una copia de seguridad (siempre y cuando posea legalmente ese derecho) para de ese modo tener un respaldo en caso de avería del sistema.

En ese sentido, cualquier otra copia que se tenga del programa en cuestión puede ser considerada ilegal y su uso conlleva las consideraciones que la ley estipule en caso de uso no autorizado de una licencia. [30]

- El Área de Tecnología y Sistemas de Información será la única dependencia autorizada para realizar copia de seguridad del *software* original.
- La instalación del *software* en las máquinas de la Empresa Social del Estado hospital regional noroccidental IPS Abrego, se realizará únicamente a través del Área TI
- El *software* proporcionado por la Empresa Social del Estado hospital regional noroccidental IPS Abrego no puede ser copiado o suministrado a terceros.
- En los equipos de la Empresa Social del Estado hospital regional noroccidental IPS Abrego se podrá utilizar el *software* licenciado por el Área de TI y el adquirido o licenciado por los proyectos o programas que se encuentran en la Empresa.
- Para la adquisición y actualización de *software*, es necesario efectuar la solicitud al Área de TI con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.
- Se encuentra prohibido el uso e instalación de juegos en los computadores de la Empresa Social del Estado hospital regional noroccidental IPS Abrego.
- Se presentarán para dar de baja el *software* de acuerdo con los lineamientos dados por la Entidad.

Gestión de Incidentes de Seguridad:

Responsabilidades y procedimientos: Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Notificación de los eventos de seguridad de la información: Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.

[30] COLOMBIA, PRESIDENCIA DE LA REPUBLICA. Lineamiento de adquisición, desarrollo y mantenimiento de sistemas de información. Bogota: La Presidencia, 2017. 12 p.

Notificación de puntos débiles de la seguridad: Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.

Valoración de eventos de seguridad de la información y toma de decisiones: Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.

Respuesta a los incidentes de seguridad: Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.

Aprendizaje de los incidentes de seguridad de la información: Se deberá utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.

Recopilación de evidencias: La Empresa Social del Estado hospital regional noroccidental IPS Abrego debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

Sanciones por incumplimiento de la política:

El usuario es responsable del cumplimiento de la política de seguridad de la información, en cualquier caso, que se presente incumplimiento este será sancionado por la compañía después de evaluar el caso en el comité de seguridad, teniendo en cuenta que actualmente se cuenta con la Ley colombiana 1273 de 2009 que respalda cualquier atentado contra la información.

6.1.9 Declaración de aplicabilidad (SOA). Es un documento escrito y redactado por exigencia de la norma ISO 27001 en el cual, entre otros aspectos se detalla los objetivos de control aplicables al Sistema de Gestión de Seguridad de la Información (SGSI). Es importante señalar, que estos objetivos se basan en el rendimiento de los medios de valoración y tratamiento adecuado de los riesgos, responsabilidades contractuales y requisitos legales o del negocio de la empresa para la seguridad de la información:

6.1.9.1 Objetivo, alcance y usuarios. El objetivo del presente documento es definir qué controles son adecuados para implementar en el área contable de la E.S.E Hospital regional noroccidental, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.

Este documento, incluye todos los controles detallados en el Anexo A de la norma ISO 27001. Los controles se aplican a todo el alcance del Sistema de gestión de seguridad de la información (SGSI) previstos en la referida normativa. Cabe destacar, que los usuarios de este instrumento son todos los empleados de el área administrativa de la E.S.E Hospital Regional Noroccidental IPS Abrego que cumplen una función dentro del SGSI.

6.1.9.2 Documentos de referencia. La siguiente es una pequeña lista de aquellos documentos que sirven de fundamento para la realización de este trabajo:

- Norma ISO/IEC 27001, capítulo 6.1.3
- Norma ISO/IEC 27002
- Política de Seguridad de la Información
- Metodología de evaluación y tratamiento de riesgos
- Informe de evaluación y tratamiento de riesgos

6.1.9.3 Aplicabilidad de los controles. Son aplicables los siguientes controles del Anexo A de la norma ISO 27001, como lo ilustra el Cuadro 1**.**

Cuadro 1. Anexo A de la norma ISO 27001

Id	Objetivos de control	Control	Aplicable
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**		
A5.1	Orientación de la dirección para la gestión de la seguridad de la información		
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Si
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	SI
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**		
A6.1	Organización interna		
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	SI
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
a6.1.3	contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	si
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	SI
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	SI
A6.2	Dispositivos móviles y teletrabajo		
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	NO
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	NO

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A7.1	Antes de asumir el empleo		
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	SI
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	SI
A7.2	Durante la ejecución del empleo		
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	SI
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI
A7.3	Terminación y cambio de empleo		
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A8	**GESTION DE ACTIVOS**		
A8.1	Responsabilidad por los activos		
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	SI
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A8.2	Clasificación de la información		
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	SI
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI
A8.3	Manejo de medios		
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	SIS
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	SI
A9	**CONTROL DE ACCESO**		
A9.1	Requisitos del negocio para el control de acceso		
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	SI
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A9.2	Gestión de acceso de usuarios		
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	SI
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	SIS
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	SI
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	SI
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	SI
A9.3	Responsabilidades de los usuarios		
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	SI
A9.4	Control de acceso a sistemas y aplicaciones		
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	SIS
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	SI
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	SI
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	SI
A10	**CRIPTOGRAFIA**		
A10.1	Controles criptográficos		
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	NO
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	NO

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A11	**SEGURIDAD FISICA Y DEL ENTORNO**		
A11.1	Áreas seguras		
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	SI
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	SI
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..	SI
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	SI
A11.2	Equipos		
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	SI
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	SI
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A11.2.5	Retiro de activos	Control: Los equipos, información o *software* no se deben retirar de su sitio sin autorización previa	SI
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	NO
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o *software* licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.	SI
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	NO

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	SI
A12	**SEGURIDAD DE LAS OPERACIONES**		
A12.1	Procedimientos operacionales y responsabilidades		
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	NO
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	NO
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	NO
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	NO

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A12.2	Protección contra códigos maliciosos		
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI
A12.3	Copias de respaldo		
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, *software* e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	SI
A12.4	Registro y seguimiento		
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	NO

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	NO
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	NO
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	NO
A12.5	Control de *software* operacional		
A12.5.1	Instalación de *software* en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de *software* en sistemas operativos.	SI
A12.6	Gestión de la vulnerabilidad técnica		

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	SI
A12.6.2	Restricciones sobre la instalación de *software*	Control: Se deben establecer e implementar las reglas para la instalación de *software* por parte de los usuarios.	SI
A12.7	Consideraciones sobre auditorias de sistemas de información		
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI
A13	**SEGURIDAD DE LAS COMUNICACIONES**		
A13.1	Gestión de la seguridad de las redes		
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI
A13.2	Transferencia de información		
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	SI
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	SI
A14	**Adquisición, desarrollo y mantenimiento de sistemas**		
A14.1	Requisitos de seguridad de los sistemas de información		

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	NO
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A14.2	Seguridad en los procesos de Desarrollo y de Soporte		
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de *software* y de sistemas, a los desarrollos dentro de la organización.	NO
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	NO
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	NO
A.14.2.4	Restricciones en los cambios a los paquetes de *software*	Control: Se deben desalentar las modificaciones a los paquetes de *software*, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	NO

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	NO
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	NO
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	SI
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A14.3	Datos de prueba		
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	NO
A15	**RELACIONES CON LOS PROVEEDORES**		
A15.1	Seguridad de la información en las relaciones con los proveedores.		
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	NO
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	NO

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	NO
A15.2	Gestión de la prestación de servicios de proveedores		
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	NO
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	NO

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**		
A16.1	Gestión de incidentes y mejoras en la seguridad de la información		
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	SI
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	SI
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	SI
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SI
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**		
A17.1	Continuidad de Seguridad de la información		

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	SI
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	SI
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A17.2	Redundancias		
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI
A18	**CUMPLIMIENTO**		
A18.1	Cumplimiento de requisitos legales y contractuales		
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	SI
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de *software* patentados.	SI

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	SI
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	SI
A18.2	Revisiones de seguridad de la información		

Cuadro 1. (Continuación)

Id	Objetivos de control	Control	Aplicable
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	SI
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	SI
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI

Fuente: NORMA TÉCNICA COLOMBIANA. Administración de Riesgos. AS/NZS 4360. (En línea) (Citado el 13 de Octubre del 2014). Disponible en: http://auditoriauc20102mivi.wikispaces.com/file/view/Resumen_NTCAS436020101700422184.pdf.

7. CONCLUSIONES

La realización de este proyecto permitió el diseño de un sistema de gestión de seguridad de la información para el área administrativa E.S.E Hospital regional Noroccidental IPS Abrego bajo la norma ISO 27001: 2013, lo cual sirvió como base estructural que dio el sustento necesario para la creación del sistema y el medio tecnológico indispensable para la creación de los diferentes componentes del sistema de información del referido hospital.

Además, Se implemento un conjunto de medidas encaminadas a realizar un inventario fidedigno de los activos tecnológicos, equipos, aplicativos, *hardware software*, archivos, implementos de seguridad informática e incluso infraestructura requerida. Tomando en consideración, la enorme cantidad de activos que se involucraron en esta faena es resaltante que el hospital requiere con urgencia desarrollar las medidas apropiadas para mantener la seguridad informática, sobre todo a nivel de procedimientos adecuados para tal fin.

Seguidamente, se elaboró la política de SGSI necearía para la implementación de los dispositivos y mecanismos destinados para corregir las fallas que se evidenciaron en el sistema.

También, se definió y estructuro la aplicabilidad de los mecanismos del SOA. Para ello, fue necesario un marco conceptual que sirviera como base para este punto.

Finalmente, al identificarse el nivel de riesgo de los activos informáticos. Se evaluaron, ejecutaron y analizaron estos riesgos para la toma de medidas preventivas encaminadas a la protección de estos.

8. RECOMENDACIONES

Se recomienda ampliamente la aplicación de los mecanismos de seguridad necesarios para fomentar la protección de los datos de información que involucran todos los activos informáticos dispuestos para ese fin, en la empresa.

Es vital que se concientice al personal acerca de los enormes riesgos que existen a nivel de seguridad, para que teniendo esa información procedan con mayor precaución, sin tomar a la ligera este punto importante para la empresa.

Además, se debe capacitar al personal acerca de los mecanismos, protocolos y demás acciones motivadas a preservar la información, la *data*, los equipos y en general la integridad de empresa.

Es imprescindible, que la cadena de mando y de responsabilidad en la fuga de información sea bien delimitada y hacer a todo el personal (incluyendo el administrativo) responsable de cualquier alteración del sistema informático, para poder establecer responsabilidades.

Finalmente, es importante también la adecuación tecnológica en materia informática del E.S.E Hospital Regional Noroccidental IPS Abrego.

BIBLIOGRAFIA

BLÁZQUEZ, Entonado. Sistema de la información y la educación, Florentino [(En línea) (Citado el 26 de Mayo del 2015). Disponible en: http://www.ub.edu/prometheus21/articulos/obsciberprome/blanquez.pdf

COLOMBIA, PRESIDENCIA DE LA REPUBLICA. Lineamiento de adquisición, desarrollo y mantenimiento de sistemas de información. Bogota: La Presidencia, 2017. 12 p.

-------. Decreto 1360. (23, junio, 1989). Bogotá, D.C: El Congreso, 1989. 63 p.

-------. Decreto 162. (22, enero, 1996). Bogotá, D.C: El Congreso, 1995. 26 p.

-------. Decreto 1747. (11, septiembre, 2000). Bogotá, D.C: El Congreso, 2000. 63 p.

-------. Decreto 460. (5, marzo, 1995).. Bogotá, D.C: El Congreso, 1995. 2 p.

-------. Ley 1266. (31, diciembre, 2008). Bogotá, D.C: El Congreso, 2008. 75 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogotá, D.C: El Congreso, 2009. 58p.

-------. Ley 1273. (5, enero, 2009). Bogotá, D.C: El Congreso, 2009. 18 p.

-------. Ley 1581. (17, octubre, 2002). Bogotá, D.C: El Congreso, 2002. 91 p.

-------. Ley 23. (28, enero, 1982). Bogotá, D.C: El Congreso, 1982. 23 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 44. (5, febrero, 1993). Bogotá, D.C: El Congreso, 1993. 14 p.

-------. Ley 527. (18, agosto, 1999). Bogotá, D.C: El Congreso, 1999. 15 p.

-------. Ley 565. (2, febrero, 2000). Bogotá, D.C: El Congreso, 2000. 18 p.

-------. Ley 603. (27, julio, 2000). Bogotá, D.C: El Congreso, 2000. 21 p.

-------. Ley 719. (24, Febrero, 2001). Bogotá, D.C: El Congreso, 1999. 187 p.

-------. Resolución 26930. (26, octubre, 2000). Bogotá, D.C: El Congreso, 2000. 69 p.

COLOMBIA. MINISTERIO DEL INTERIOR. Ley 545 de 1999. por medio de la cual se apreueba el tratado de la OMPI sobre interpretación o ejecución y fonogramas. Bogotá, D.C: El Ministerio, 1999. 15 p.

INTERNATIONAL STANDARD ISO/IEC 17799. (En línea) (Citado el 16 de Mayo del 2005). Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf.

MARTINEZ, Sergio. Normas de uso común para proyectos de TI (ISO). (En línea) (Citado el 27 de junio del 2014). Disponible en: https://checomart.wordpress.com/2014/01/

NORMA TÉCNICA COLOMBIANA. Administración De Riesgos. AS/NZS 4360. (En línea) (Citado el 13 de Octubre del 2014). Disponible en: http://auditoriauc20102mivi.wikispaces.com/file/view/Resumen_NTCAS436020101700422184.pdf.

-------. Gestión de riesgo. (En línea) (Citado el 23 de Enero del 2016). Disponible en: https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_riesgos.

NORMA TÉCNICA COLOMBIANA. Sistema de Gestión de la Seguridad de la Información, ¿Qué es un SGSI? (En línea) (Citado el 27 de junio del 2018). Disponible en: Disponible en: http://www.iso27000.es/sgsi.html.

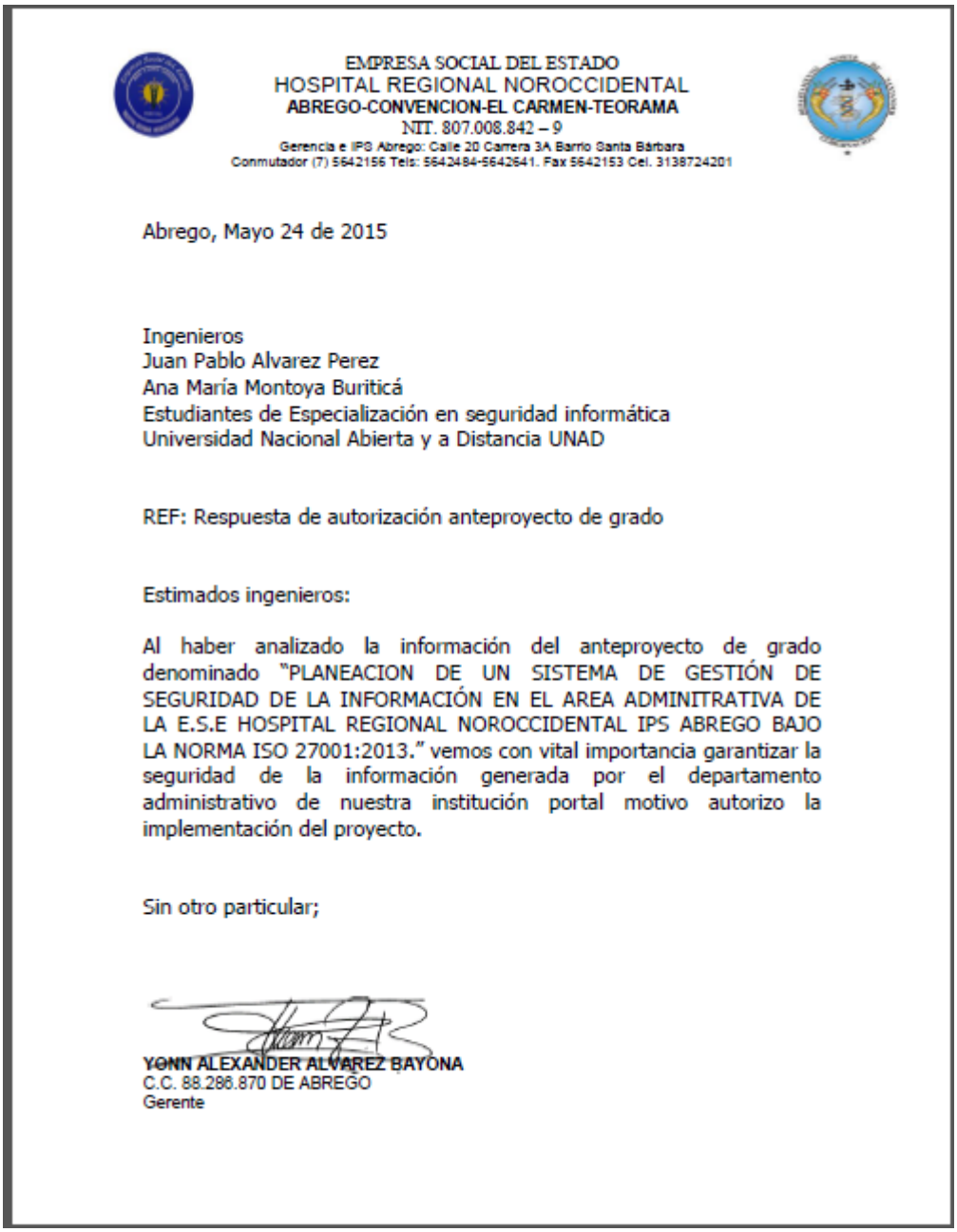
REYNOLDS, Jean y HOLBROOK, Paul. RFC 1244: Site Security Handbook. 1 ed. New York: McGraw-Hill, 1991. 102 p.

SUAREZ, Sandra. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & Cía. Ltda, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Trabajo de grado Especialista en Seguridad Informática. Bogota. D.C.: Universidad Nacional Abierta y a Distancia, Escuela de Tecnología e Ingeniería. Especialización en seguridad informática, 2015. 135 p.

TRUJILLLO, Freddy. C.E Soft Colombia. (En línea) (Citado el 15 de septiembre del 2010). Disponible en: http://cesoftco.net/2cmc/PAPER.htm.

ANEXOS

Anexo A. Carta de aceptación de la propuesta



EMPRESA SOCIAL DEL ESTADO
HOSPITAL REGIONAL NOROCCIDENTAL
ABREGO-CONVENCION-EL CARMEN-TEORAMA
NIT. 807.008.842 – 9
Gerencia e IPS Abrego: Calle 20 Carrera 3A Barrio Santa Bárbara
Conmutador (7) 5642156 Tels: 5642484-5642641. Fax 5642153 Cel. 3138724201

Abrego, Mayo 24 de 2015

Ingenieros
Juan Pablo Alvarez Perez
Ana María Montoya Buriticá
Estudiantes de Especialización en seguridad informática
Universidad Nacional Abierta y a Distancia UNAD

REF: Respuesta de autorización anteproyecto de grado

Estimados ingenieros:

Al haber analizado la información del anteproyecto de grado denominado "PLANEACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL AREA ADMINITRATIVA DE LA E.S.E HOSPITAL REGIONAL NOROCCIDENTAL IPS ABREGO BAJO LA NORMA ISO 27001:2013." vemos con vital importancia garantizar la seguridad de la información generada por el departamento administrativo de nuestra institución portal motivo autorizo la implementación del proyecto.

Sin otro particular;

YONN ALEXANDER ALVAREZ BAYONA
C.C. 88.286.870 DE ABREGO
Gerente

Anexo B. Acta 05 Socializaciones PAMEC

	EMPRESA SOCIAL DEL ESTADO HOSPITAL REGIONAL NOROCCIDENTAL ABREGO-CONVENCION-EL CARMEN-TEORAMA MACROPROCESO: INFORMACION , COMUNICACIÓN Y TIC	
CODIGO MA-PR-GICT16-01	PROCESO: Comunicaciones Internas y Externas	VERSION: 1.0 Enero/2015

ACTA 001
ESE HRNO

TEMA A TRATAR	LUGAR	FECHA DE REUNION	PROCESO
SOCIALIZACION PAMEC	ANTHOC	17 de Mayo de 2.015	PAMEC, IPS Abrego

PARTICIPANTES

Los enunciados en la lista de asistencia

RESUMEN DEL TEMA TRATADO

- Nos reunimos en el salón de ANTHOC, de la IPS de Abrego a las 7 de la mañana, los abajo firmantes por comunicado interno de la oficina de auditoría de calidad de la ESE HRNO, con el fin de retroalimentar la socialización del PROGRAMA DE AUDITORIA PARA EL MEJORAMIENTO DE LA CALIDAD 2.015 – 2.016.

- Inicialmente se tomó lista a la convocatoria y se realizó la recomendación por parte de la auditora de los inasistentes a la socialización pues la Gerencia manifiesto que todo el personal de la IPS debe ser capacitado sin falta.

- Se inició la capacitación mencionando el Decreto 1011 de 2.006, decreto que enmarca el sistema obligatorio de garantía de la calidad y las resoluciones que ayudan al cumplimiento del mismo y enuncia los estándares exigidos por la norma.

- Se hablo del estándar de habilitación resolución 2003 DE 2.014, en la cual se contemplan los requisitos mínimos que se debe contar en las IPS según los servicios habilitados en el Departamento.

- Se hablaron de los sistemas de información requeridos por la norma y los que se manejan en el programa de seguridad de paciente para mejorar y mantener la calidad de los servicios en la IPS.

- Se relacionó el PAMEC (PROGRAMA DE AUDITORIA PARA EL MEJORAMIENTO DE LA CALDIAD 2.015-2.016), que se ejecutara en el año en curso y los lideres encargados en el proceso.

- Se explicó el estándar de acreditación y los lineamientos del Ministerio para nosotros que somos IPS públicas.

- Se trató el tema de seguridad de la información se determinó que esta seguridad es limitada e insuficiente, por esto se determinó que debería realizarse un análisis de la situación actual de la empresa en cuanto a la seguridad informática.

Se da por terminada la capacitación con las respuestas a las inquietudes de los asistentes.

Se informa a los empleados que asistieron que deben informar a los que no asistieron a la convocatoria que se comuniquen con la oficina de auditoría de calidad, para entregar información dada en la misma para que queden todos socializados sobre el tema.

COMPROMISOS

- Se reunirán los equipos auto evaluadores para realizar un ejercicio de autoevaluación con uno de los estándares contemplados en la resolución 0123 de 2.012 y de una manera pedagógica aprender la metodología

CONCLUSIONES

- Se concluye que trabajaremos en Equipo para el desarrollo de las actividades que conllevan a la buena prestación del servicio y cumplimiento con lo exigido en la normatividad vigente.

Constancia de firma de los participantes a la capacitación.

Anexo C. Entrevista al personal del área de contabilidad

El siguiente cuestionario permite recaudar la información necesaria para complementar el diseño del sistema de seguridad de la información.

Empresa:		NIT:		
Cuestionario de control seguridad e informática		A1		
Proceso	Seguridad de la información			
Objetivo	Seguridad de la información			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Existen metodologías de respaldo de información?				
¿Se realizan respaldos de información periódicamente?				
¿existen respaldos de la información por fuera del edificio?				
¿Existe un administrador de sistemas que controle las cuentas de los usuarios?				
¿Existe algún estándar para la creación de contraseñas?				
¿Las contraseñas cuentan con letras, números y símbolos?				
¿cada cuánto tiempo se cambia la contraseña?				
¿La I.P.S cuenta con un proceso para dar mantenimiento preventivo y correctivo a los equipos?				
¿Se tienen *software* antivirus instalados en los equipos de cómputo?				
¿La actualización del *software* es automático?				
¿Cuenta con licencias de *software*?				
¿Existe un procedimiento para la actualización de *software*?				
¿Existe un proceso para adquirir nuevas licencias?				
¿Se sanciona al integrante del departamento si instala *software* no permitido?				

Empresa:			NIT:	
Cuestionario de control seguridad e informática			A2	
Proceso	Seguridad de la información			
Objetivo	Seguridad de la Información Bases de Datos			
Cuestionario				
Pregunta			**SI**	**NO**	**N/A**
¿Se encuentra un administrador de sistemas en la empresa que lleve un control de los usuarios?					
Son gestionados los perfiles de estos usuarios por el administrador?					
¿Se renuevan las claves de los usuarios de la Base de Datos?					
¿Se obliga el cambio de la contraseña de forma automática?					
¿Se realiza copias de seguridad?					
¿Las copias de seguridad se efectúan diariamente?					
¿Las copias de seguridad son encriptados?					
¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?					
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?					
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?					
¿Hay algún procedimiento para dar de alta a un usuario?					
¿Hay algún procedimiento para dar de baja a un usuario?					
¿Es eliminada la cuenta del usuario en dicho procedimiento?					
TOTAL					

Empresa:		NIT:		
Cuestionario de control seguridad e informática		A3		
Proceso	Adquirir y mantener la arquitectura tecnológica			
Objetivo	*Hardware* Compra y Garantía			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se cuenta con un inventario de todos los equipos que integran el centro de cómputo?				
¿Con cuanta frecuencia se revisa el inventario?				
¿Existen hojas de vida de los equipos?				
¿Existe cronograma de mantenimiento preventivo?				
¿Existe hoja de servicio de mantenimiento preventivo y o correctivo?				
¿La hoja de servicio señala fecha de detección de la falla?				
¿La hoja de servicio señala fecha de corrección de la falla?				
¿Se lleva un control de los equipos en garantía?				
¿Se cuenta con servicio de mantenimiento para todos los equipos?				
¿Existe cronograma de mantenimiento de los equipos?				
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?				
¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos a adquirir y así elegir el mejor?				
TOTAL				

Empresa:		NIT:		
Cuestionario de control seguridad e informática		A4		
Proceso	Redes y comunicaciones			
Objetivo	Infraestructura de redes de comunicación			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Los enlaces de la red se testean frecuentemente?				
¿La longitud de los tramos de cableado no excede de los 90 metros?				
¿El armado del patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B?				
¿La E.S.S Cuenta con un plano de la red LAN?				
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?				
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?				
¿Las direcciones IP´S de los equipos de cómputo son implementadas de forma fija?				
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?				
Cuenta con dispositivos para la regulación del voltaje?				
Cuenta con dispositivos de bakup de energía?				
TOTAL				

Empresa:		NIT:		
Cuestionario de control seguridad e informática		A5		
Proceso	Instalaciones			
Objetivo	Instalaciones, adecuaciones y seguridad			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Existe suficiente espacio dentro de las oficinas de forma que permita una circulación fluida?				
¿Existen lugares de acceso restringido?				
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?				
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?				
¿Se tienen medios adecuados para extinción de fuego en las oficinas?				
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?				
TOTAL				
Empresa:		NIT:		
Cuestionario de control seguridad e informática		A6		
Proceso	Instalaciones			
Objetivo	Suministro de Energía			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se cuenta con instalación con tierra física para todos los equipos?				
¿La Instalación es independiente para el los equipos de cómputo?				
¿La iluminación está alimentada de la misma acometida que los equipos?				
¿Se tienen los interruptores rotulados adecuadamente?				
¿Se tienen protecciones contra corto circuito?				
¿Se cuenta con Planta de emergencia?				
TOTAL				

Anexo D. Tabulación de la encuesta

PREGUNTA	RESPUESTA		
Seguridad de la información	si	no	n/a
¿Existen metodologías de respaldo de información?	0.00%	100.00%	0.00%
¿Se realizan respaldos de información periódicamente?	0.00%	100.00%	0.00%
¿existen respaldos de la información por fuera del edificio?	0.00%	100.00%	0.00%
¿Existe un administrador de sistemas que controle las cuentas de los usuarios?	0.00%	100.00%	0.00%
¿Existe algún estándar para la creación de contraseñas?	0.00%	100.00%	0.00%
¿Las contraseñas cuentan con letras, números y símbolos?	0.00%	100.00%	0.00%
¿cada cuánto tiempo se cambia la contraseña?			100.00%
¿La I.P.S cuenta con un proceso para dar mantenimiento preventivo y correctivo a los equipos?	100.00%	0.00%	0.00%
¿Se tienen *software* antivirus instalados en los equipos de cómputo?	100.00%	0.00%	0.00%
¿La actualización del *software* es automático?	100.00%	0.00%	0.00%
¿Cuenta con licencias de *software*?	100.00%	0.00%	0.00%
¿Existe un procedimiento para la actualización de *software*?	0.00%	100.00%	0.00%
¿Existe un proceso para adquirir nuevas licencias?	0.00%	25.00%	75.00%
¿Se sanciona al integrante del departamento si instala *software* no permitido?	0.00%	100.00%	0.00%
Información Bases de Datos			
¿Se encuentra un administrador de sistemas en la empresa que lleve un control de los usuarios?	100.00%	0.00%	0.00%
Son gestionados los perfiles de estos usuarios por el administrador?	100.00%	0.00%	0.00%
¿Se renuevan las claves de los usuarios de la Base de Datos?	0.00%	100.00%	0.00%
¿Se obliga el cambio de la contraseña de	0.00%	100.00%	0.00%

PREGUNTA	RESPUESTA		
Seguridad de la información	si	no	n/a
forma automática?			
¿Se realiza copias de seguridad?	12.50%	87.50%	0.00%
¿Las copias de seguridad se efectúan diariamente?	12.50%	87.50%	0.00%
¿Las copias de seguridad son encriptados?	0.00%	100.00%	0.00%
¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?	0.00%	100.00%	0.00%
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa ?	0.00%	25.00%	75.00%
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?	0.00%	100.00%	0.00%
¿Hay algún procedimiento para dar de alta a un usuario?	12.50%	12.50%	75.00%
¿Hay algún procedimiento para dar de baja a un usuario?	12.50%	12.50%	75.00%
¿Es eliminada la cuenta del usuario en dicho procedimiento?	12.50%	12.50%	75.00%
***Hardware* Compra y Garantía**			
¿Se cuenta con un inventario de todos los equipos que integran el centro de cómputo?	25.00%	0.00%	75.00%
¿Con cuanta frecuencia se revisa el inventario?	0.00%	25.00%	75.00%
¿Existen hojas de vida de los equipos?	100.00%	0.00%	0.00%
¿Existe cronograma de mantenimiento preventivo?	100.00%	0.00%	0.00%
¿Existe hoja de servicio de mantenimiento preventivo y o correctivo?	100.00%	0.00%	0.00%
¿La hoja de servicio señala fecha de detección de la falla?	100.00%	0.00%	0.00%
¿La hoja de servicio señala fecha de corrección de la falla?	100.00%	0.00%	0.00%
¿Se lleva un control de los equipos en garantía?	0.00%	25.00%	75.00%
¿Se cuenta con servicio de mantenimiento para todos los equipos?	100.00%	0.00%	0.00%
¿Existe cronograma de mantenimiento de los equipos?	100.00%	0.00%	0.00%

PREGUNTA	RESPUESTA		
Seguridad de la información	si	no	n/a
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?	0.00%	25.00%	75.00%
¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos a adquirir y así elegir el mejor?	0.00%	25.00%	75.00%
Infraestructura de redes de comunicación	0.00%	0.00%	0.00%
¿Los enlaces de la red se testean frecuentemente?	0.00%	12.50%	87.50%
¿La longitud de los tramos de cableado no excede de los 90 metros?	0.00%	12.50%	87.50%
¿ El armado del patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B?	12.50%	0.00%	87.50%
¿La E.S.S Cuenta con un plano de la red LAN?	12.50%	0.00%	87.50%
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?	12.50%	0.00%	87.50%
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?	0.00%	12.50%	87.50%
¿Las direcciones IP´S de los equipos de cómputo son implementadas de forma fija?	12.50%	0.00%	87.50%
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?	12.50%	0.00%	87.50%
Cuenta con dispositivos para la regulación del voltaje?	25.00%	0.00%	0.00%
Cuenta con dispositivos de bakup de energía?	100.00%	0.00%	0.00%
Instalaciones, adecuaciones y seguridad			
¿Existe suficiente espacio dentro de las oficinas de forma que permita una circulación fluida?	100.00%	0.00%	0.00%
¿Existen lugares de acceso restringido?	0.00%	100.00%	0.00%
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?	0.00%	100.00%	0.00%
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?	0.00%	100.00%	0.00%
¿Se tienen medios adecuados para	12.50%	87.50%	0.00%

PREGUNTA	RESPUESTA		
Seguridad de la información	si	no	n/a
extinción de fuego en las oficinas?			
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?	12.50%	12.50%	75.00%
Suministro de Energía			
¿Se cuenta con instalación con tierra física para todos los equipos?	12.50%	0.00%	87.50%
¿La Instalación es independiente para el los equipos de cómputo?	0.00%	12.50%	87.50%
¿La iluminación está alimentada de la misma acometida que los equipos?	0.00%	12.50%	87.50%
¿Se tienen los interruptores rotulados adecuadamente?	0.00%	100.00%	0.00%
¿Se tienen protecciones contra corto circuito?	12.50%	0.00%	87.50%
¿Se cuenta con Planta de emergencia?	100.00%	0.00%	0.00%

Anexo E. Resumen analítico educativo RAE

Título del Texto	DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA ADMINISTRATIVA DE LA E.S.E HOSPITAL REGIONAL NOROCCIDENTAL IPS ABREGO BAJO LA NORMA ISO 27001:2013
Nombres y apellidos del autor	JUAN PABLO ÁLVAREZ PEREZ
Año de la publicación	2019
Director	Esp. DANIEL FELIPE PALOMO LUNA

Referencias

Baldecchi, R. Implementación efectiva de un SGSI ISO 27001, 14 de septiembre de 2015 [En línea]
http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

Buitrago, J. Bonilla, D. Murillo, C. Diseño de una metodología para la Implementación del Sistema de Gestión de Seguridad de la Información - SGSI, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001, 14 de Septiembre de 2015 [En línea]
http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

Frayssinet, M. Taller de implementación de la norma ISO 27001, 15 de Septiembre de 2015 [En línea]
http://es.slideshare.net/mfrayssinet/taller-de-implementacin-de-la-norma-iso-27001

Fundación Wikipedia, Inc. Círculo de Deming, 22 de Octubre de 2015 [En línea]
https://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming

Universidad de la República. Metodologías para Implantación de SGSI, 22 de Octubre de 2015 [En línea]
http://www.fing.edu.uy/grupo-de-seguridad-inform%C3%A1tica/i-i/metodolog%C3%ADas-para-implantaci%C3%B3n-de-sgsi

Resumen del texto:

El desarrollo de este proyecto permite conocer la situación actual de la Empresa Social del Estado hospital regional noroccidental IPS Abrego, en cuanto a su objetivo de diseñar un sistema de seguridad de la información que sirva como respaldo de las actividades realizadas en el área administrativa, agilizando el análisis de riesgos, confiabilidad y disponibilidad a los que se ve expuesta la información en el caso particular del área de contabilidad, la cual busca poder minimizar y controlar las amenazas que pueden estar presentes en el flujo, almacenamiento y ejecución de la

información. Este sistema se realizó bajo un proceso sistemático, documentado y conocido por toda la organización para ser revisado y actualizado constantemente, con el uso de una metodología que permitiera indagar como era su funcionamiento y la incidencia directa e indirecta sobre el medio operativo de la empresa, ya que la información contable es de vital importancia para la toma de decisiones en el funcionamiento de esta.

El desarrollo del proyecto está basado en la norma de gestión de seguridad ISO/IEC 27001:2013 la cual proporciona las directrices, practicas, selección, implementación y gestión de los controles, teniendo en cuenta el medio ambiente, riesgo y seguridad de la información para su diseño. La metodología empleada se basó en el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) la cual ofrece una opción que permite mantener la competitividad de los servicios, mejorar la calidad, reduce los costos, mejora la productividad, la confiabilidad de la información, la toma de decisiones, supervivencia de la empresa y aumenta la rentabilidad de esta.

El Diseño del Sistema de Gestión de Seguridad Informática fue concebido para suministrar un conjunto de actividades que deben realizarse mediante procesos sistemáticos enfocados en el proceso contable de la Empresa Social del Estado hospital regional noroccidental IPS Abrego, la cual genera un impacto en la continuidad del negocio y del funcionamiento de los demás procesos dentro de la empresa. Su objetivo está orientado a generar políticas y controles de seguridad para que los riesgos sean conocidos, asumidos, gestionados y minimizados, de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la misma.

Palabras claves	Políticas, SGSI, Alcance, *Magerit*, Activos, Riesgos, Impacto, Amenaza, vulnerabilidad, *bakup,* salvaguarda.

Descripción del problema: Al analizar la infraestructura tecnológica del Área Administrativa de la E.S.E Hospital Regional Noroccidental I.P.S Abrego, es notable el crecimiento experimentado con el paso de los años, este hecho ha provocado que los controles a nivel de seguridad de la información que se encuentran vigentes, no sean los adecuados para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información, razón por la cual es necesario que sean revisados y mejorados.

En caso de no remediarse la situación anteriormente expuesta, se eleva exponencialmente el riesgo de ocurrencia de incidentes de seguridad, pérdida de información o disponibilidad de los servicios y sistemas que sustentan la operación del Área Administrativa del Hospital, esto redundaría en pérdidas económicas y podría generar desconfianza sobre la imagen que mantiene la E.S.E Hospital Regional Noroccidental I.P.S Abrego en el medio de la salud.

Objetivos

General:

Diseñar un Sistema de Gestión de Seguridad de la Información para el área administrativa E.S.E Hospital Regional Noroccidental IPS Abrego bajo la norma ISO 27001:2013

Específicos:

•Definir el alcance y límites del SGSI para el área administrativa de la E.S.E Hospital Regional Noroccidental IPS Abrego.

•Realizar inventario de los activos tecnológicos.

•Elaborar la política del SGSI.

•Elaborar la definición del SOA (Aplicabilidad).

•Identificar, evaluar y ejecutar el análisis de riesgos de los activos informáticos.

Diseño metodológico	El diseño metodológico de este trabajo se basa en la metodología PHVA (Planear, Hacer, Verificar y Actuar) de la norma ISO 27001 para los SGSI.
Referentes teóricos y conceptuales	El referente principal teórico se basó en la norma ISO/IEC 2700, estándares de seguridad, metodologías y análisis de evaluación de riesgos (MAGERIT).

Resultados

Se documentó el estado actual de la seguridad de la información para así determinar que políticas de seguridad y controles más adecuados para la ESE. Se determinó que la implementación del SGSI propuesto en el diseño para protegerá de forma eficiente los activos de la información que allí se encuentra.

Se levantó el inventario de activos del área de contabilidad de la empresa quedando actualizada a la fecha.

El área de calidad se encuentra implementando procesos para mejorar el nivel de seguridad de la información, se determinó que no existe documentación referente a estos procesos.

Se determinó que el estado actual de la seguridad de la información, se encuentra en estado medio, ya que el personal lleva a cabo el trabajo, acatando buenas practicas, pero no existen procesos claros que permitan establecer roles y responsabilidades en los empleados de la entidad.

La entidad no se realizan campañas internas, donde se oriente a los usuarios al buen uso de los recursos tecnológicos, tampoco existe divulgación de riesgos a los que se están expuestos, uso de contraseñas

fuertes y temas de ingeniería social, se hace necesario llevar a cabo estas campañas de sensibilización y estrategias que permitan aumentar el nivel de seguridad, tratamiento y niveles de confidencialidad, disponibilidad y autenticidad de la información.

Conclusiones

La realización de este proyecto permitió el diseño de un sistema de gestión de seguridad de la información para el área administrativa E.S.E Hospital regional Noroccidental IPS Abrego bajo la norma ISO 27001: 2013, lo cual sirvió como base estructural que dio el sustento necesario para la creación del sistema y el medio tecnológico indispensable para la creación de los diferentes componentes del sistema de información del referido hospital.

Además, Se implementó un conjunto de medidas encaminadas a realizar un inventario fidedigno de los activos tecnológicos, equipos, aplicativos, hardware software, archivos, implementos de seguridad informática e incluso infraestructura requerida. Tomando en consideración, la enorme cantidad de activos que se involucraron en esta faena es resaltante que el hospital requiere con urgencia desarrollar las medidas apropiadas para mantener la seguridad informática, sobre todo a nivel de procedimientos adecuados para tal fin.

Seguidamente, se elaboró la política de SGSI necearía para la implementación de los dispositivos y mecanismos destinados para corregir las fallas que se evidenciaron en el sistema.

También, se definió y estructuro la aplicabilidad de los mecanismos del SOA. Para ello, fue necesario un marco conceptual que sirviera como base para este punto.

Finalmente, al identificarse el nivel de riesgo de los activos informáticos. Se evaluaron, ejecutaron y analizaron estos riesgos para la toma de medidas preventivas encaminadas a la protección de estos.